iS5 Communications

RAPTOR iMX950 CLI Reference
iMX950

Document Version: 1.12.05-2-EN
April 18, 2022

© 2022 iS5 Communications Inc.
All Rights Reserved

Copyright Notice

© 2022 iS5 Communications Inc. All rights reserved.

No Part of this publication may be reproduced in any form without the prior written consent of iS5 Communications Inc. (iS5).

Trademarks

iS5Com is a registered trademark of iS5. All other trademarks belong to their respective owners.

Regulatory Compliance Statement

Product(s) associated with this publication complies/comply with all applicable regulations. For more details, refer to the Technical Specifications.

Warranty

iS5 warrants that all products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). iS5 will repair or replace products found to be defective within this warranty period including shipping costs. This warranty does not cover product modifications or repairs done by persons other than iS5-approved personnel, and this warranty does not apply to products that are misused, abused, improperly installed, or damaged by accident. Refer to the Technical Specifications for the actual warranty period(s) of the product(s) associated with this publication. Warranty certificate available at: https://is5com.com/warranty

Disclaimer

Information in this publication is intended to be accurate. iS5 shall not be responsible for its use or infringements on third-parties because of the use of this publication. There may occasionally be unintentional errors on this publication. iS5 reserves the right to revise the contents of this publication without notice.

Contact Information

iS5 Communications Inc. 5895 Ambler Dr., Mississauga, Ontario, L4W 5B7 Tel: 1+ 905-670-0004 // Fax: 1+ 289-401-5206 Website: http://www.is5com.com/ Technical Support: E-mail: support@is5com.com Sales Contact: E-mail: sales@is5com.com

End User License Agreement (EULA)

TERMS AND CONDITIONS FOR SOFTWARE PROGRAMS AND EMBEDDED SOFTWARE IN PRODUCTS

1) **EULA**

*All products which consist of or include software (including operating software for hardware supplied by Supplier and software in object code format that is embedded in any hardware) and/or any documentation shall be subject to the End User License Agreement ("**EULA**") attached hereto as Exhibit A. Buyer shall be deemed to have agreed to be bound by all of the terms, conditions and obligations therein and shall ensure that all subsequent purchasers and licensees of such products shall be further bound by all of the terms, conditions and obligations therein. For software and/or documentation delivered in connection with these Terms and Conditions, that is not produced by Supplier and which is separately licensed by a third party, Buyer's rights and responsibilities with respect to such software or documentation shall be governed in accordance with such third party's applicable software license. Buyer shall, on request, enter into one or more separate "click-accept" license agreements or third party license agreements in respect thereto. Supplier shall have no further obligations with respect to such products beyond delivery thereof. Where Buyer is approved by Supplier to resell products, Buyer shall provide a copy of the EULA and applicable third party license agreements to each end user with delivery of such products and prior to installation of any software. Buyer shall notify Supplier promptly of any breach or suspected breach of the EULA or third party license agreements and shall assist Supplier in efforts to preserve Supplier's or its supplier's intellectual property rights including pursuing an action against any breaching third parties. For purposes of these terms and conditions: "software" shall mean scripts, programs, macros, computer programs, application programming and other interfaces, tools and other instructions and sets of instructions for hardware to follow, including SQL and other query languages, hypertext markup language ("**html**") and other computer mark-up languages; "**hardware**" shall mean mainframes, personal computers, servers, client/server stations, network equipment, routers, semi-conductor chips, communication lines and other equipment; and "**documentation**" shall mean documentation supplied by Supplier relating to the development, use, installation, implementation, integration, configuration, operation, modification, maintenance or support of any software.*

2) **INTELLECTUAL PROPERTY**

*Buyer shall not alter, obscure, remove, cancel or otherwise interfere with any markings (including without limitation any trademarks, logos, trade names, or labelling applied by Supplier). Buyer acknowledges that Supplier is the sole owner of the trademarks used in association with the products and that Buyer has no right, title or interest whatsoever in such trademarks and any goodwill associated therewith and that all goodwill associated with such trademarks is owned by and shall enure exclusively to and for the benefit of Supplier. Further, Buyer shall not represent in any manner that it has acquired any ownership rights in such trademarks or other intellectual property of Supplier. Supplier will defend any claim against Buyer that any iS5Com branded product supplied under these Terms and Conditions infringes third party patents or copyrights (a "**Patent Claim**") and will indemnify Buyer against the final judgment entered by a court of competent jurisdiction or any settlements arising out of a Patent Claim, provided that Buyer: (1) promptly notifies Supplier in writing of the Patent Claim; and (2) cooperates with Supplier in the defence of the Patent Claim, and grants Supplier full and exclusive control of the defence and settlement of the Patent Claim and any subse-*

quent appeal. If a Patent Claim is made or appears likely, Buyer agrees to permit Supplier to procure for Buyer the right to continue using the affected product, or to replace or modify the product with one that is at least functionally equivalent. If Supplier determines that none of those alternatives is reasonably available, then Buyer will return the product and Supplier will refund Buyer's remaining net book value of the product calculated according to generally accepted accounting principles. Supplier has no obligation for any Patent Claim related to: (1) compliance with any designs, specifications, or instructions provided by Buyer or a third party on Buyer's behalf; (2) modification of a product by Buyer or a third party; (3) the amount or duration of use which Buyer makes of the product, revenue earned by Buyer from services it provides that use the product, or services offered by Buyer to external or internal Buyers; (4) combination, operation or use of a product with non-Supplier products, software or business processes; or (5) use of any product in any country other than the country or countries specifically authorized by Supplier.

3) **EXPORT CONTROLS AND SANCTIONS**

a) In these Term and Conditions, "***Export Controls and Sanctions***" means the export control and sanctions laws of each of Canada, the US and any other applicable country, territory or jurisdiction including the United Nations, European Union and the United Kingdom, and any regulations, orders, guides, rules, policies, notices, determinations or judgements issued thereunder or imposed thereby.

b) Supplier products, documentation and services provided under these Terms and Conditions may be subject to Canadian, U.S. and other country Export Controls and Sanctions. Buyer shall accept and comply with all applicable Export Control and Sanctions in effect and as amended from time to time pertaining to the export, re-export and transfer of Supplier's products, documentation and services. Buyer also acknowledges and agrees that the export, re-export or transfer of Supplier products, documentation and services contrary to applicable Export Controls and Sanctions may be a criminal offence.

c) For greater certainty, Buyer agrees that (i) it will not directly or indirectly export, re-export or transfer Supplier products, documentation and services provided under these Terms and Conditions to any individual or entity in violation of any aforementioned Export Controls and Sanctions; (ii) it will not directly or indirectly export, re-export or transfer any such products, documentation and services to any country or region of any country that is prohibited by any applicable Export Controls and Sanctions or for any of the following end-uses, or in any of the following forms unless expressly authorized by any applicable government permit issued under or otherwise expressly permitted by applicable Export Controls and Sanctions:

   i) For use that is directly or indirectly related to the research, design, handling, storage, operation, detection, identification, maintenance, development, manufacture, production or dissemination of chemical, biological or nuclear weapons, or any missile or other delivery systems for such weapons, space launch vehicles, sounding rockets or unmanned air vehicle systems;

   ii) Technical information relating to the design, development or implementation of the cryptographic components, modules, interfaces, or architecture of any software; or

   iii) Source code or pseudo-code, in any form, of any of the cryptographic components, modules, or interfaces of any software.

d) Buyer confirms that it is not (i) listed as a sanctioned person or entity under any Export Controls and Sanctions list of designated persons, denied persons or specially designated

nationals maintained by the Canadian Department of Foreign Affairs, Trade and Development, the Canadian Department of Public Safety and Emergency Preparedness, the U.S. Office of Foreign Assets Control of the U.S. Department of the Treasury, the U.S. Department of State, the U.S. Department of Commerce, United Nations Security Council, the European Union or any EU member state, HM's Treasury, or any other department or agency of any of the aforementioned countries or territories, or the United Nations or any other country's sanctions-related list; (ii) owned or controlled by such person or entity; or (iii) acting in any capacity on behalf of or for the benefit of such person or entity. Buyer also confirms that this applies equally to any of its affiliates, joint venture partners, subsidiaries and to the best of Buyer's knowledge, any of its agents or representatives.

Exhibit A: End User License Agreement

IMPORTANT – READ CAREFULLY: iS5 Communications Inc. ("**iS5Com**") licenses the iS5Com Materials (as defined below) subject to the terms and conditions of this end user license agreement (the "**EULA**"). BY SELECTING "ACCEPT" OR OTHERWISE EXPRESSLY AGREEING TO THIS EULA, BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE, OR BY USING THE HARDWARE (AS DEFINED BELOW), ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS EULA BECOME LEGALLY BINDING ON THE CUSTOMER.This End User License Agreement (the "**EULA**") supplements the Terms and Conditions or such other terms and conditions between iS5Com or, if applicable, a reseller for iS5Com, and the Customer (as defined below) (in either case, the "**Contract**").

1) **DEFINITIONS**

*"**Confidential Information**" means all data and information relating to the business and management of iS5Com, including iS5Com Materials, trade secrets, technology and records to which access is obtained hereunder by the Customer, and any materials provided by iS5Com to the Customer, but does not include any data or information which: (a) is or becomes publicly available through no fault of the Customer; (b) is already in the rightful possession of the Customer prior to its receipt from iS5Com; (c) is already known to the Customer at the time of its disclosure to the Customer by iS5Com and is not the subject of an obligation of confidence of any kind; (d) is independently developed by the Customer; (e) is rightfully obtained by the Customer from a third party; (e) is disclosed with the written consent of iS5Com; or (f) is disclosed pursuant to court order or other legal compulsion.*

- "***Customer***" means the licensee of the iS5Com Software pursuant to the Contract.
- "**iS5Com Documentation**" means Documentation supplied by or on behalf of iS5Com under the Contract relating to the development, use, installation, implementation, integration, configuration, operation, modification, maintenance or support of iS5Com Software, or iS5Com Firmware.
- "**iS5Com Firmware**" means iS5Com Software in object code format that is embedded in iS5Com Hardware.
- "**iS5Com Hardware**" means Hardware supplied by or on behalf of iS5Com under the Contract.
- "**iS5Com Materials**" means, collectively, the iS5Com Software and the iS5Com Documentation.

- "**iS5Com Software**" means Software supplied by or on behalf of iS5Com under the Contract. For greater certainty, iS5Com Software shall include all operating Software for iS5Com Hardware, and iS5Com Firmware.
- "**Documentation**" means written instructions and manuals of a technical nature.
- "**EULA**" means this End User License Agreement.
- "**Hardware**" means hardware, mainframes, personal computers, servers, client/server stations, network equipment, routers, semi-conductor chips, communication lines and other equipment.
- "**Intellectual Property Rights**" means any and all proprietary rights provided under: (i) patent law; (ii) copyright law (including moral rights); (iii) trade-mark law; (iv) design patent or industrial design law; (v) semi-conductor chip or mask work law; or (vi) any other statutory provision or common law principle applicable to this EULA, including trade secret law, which may provide a right in either Hardware, Software, Documentation, Confidential Information, ideas, formulae, algorithms, concepts, inventions, processes or know-how generally, or the expression or use of such Hardware, Software, Documentation, Confidential Information, ideas, formulae, algorithms, concepts, inventions, processes or know-how trade secret law; any and all applications, registrations, licenses, sub-licenses, franchises, agreements or any other evidence of a right in any of the foregoing; and all licenses and waivers and benefits of waivers of the intellectual property rights set out herein, all future income and proceeds from the intellectual property rights set out herein, and all rights to damages and profits by reason of the infringement of any of the intellectual property rights set out herein.
- "**Software**" means scripts, programs, macros, computer programs, application programming and other interfaces, tools and other instructions and sets of instructions for hardware to follow, including SQL and other query languages, hypertext markup language ("html") and other computer mark-up languages.
- "**Third Party License Terms**" means additional terms and conditions that are applicable to Third Party Software.
- "**Third Party Software**" means Software owned by any third party, licensed to iS5Com and sublicensed to the Customer.
- "**Update**" means a supplemented or revised version of iS5Com Software which rectifies bugs or makes minor changes or additions to the functionality of iS5Com Software and is designated by iS5Com as a higher release number from, for example, 6.06 to 6.07 or 6.1 to 6.2.

2) **LICENSE**

- **2.1 License Grant**

  The iS5Com hereby grants to the Customer, subject to any Third Party License Terms, a non-exclusive, non-transferable, non-sublicensable right and licence to use iS5Com Materials solely in object code format, solely for the Customer's own business purposes, solely in accordance with this EULA (including, for greater certainty, subject to Section 6.1 of this EULA) and the applicable iS5Com Documentation, and, in the case of iS5Com Firmware, solely on iS5Com Hardware on which iS5Com Firmware was installed, provided that Customer may only install iS5Com Software on such number of nodes expressly set out in the Contract.

- **2.2 License Restrictions**

Except as otherwise provided in Section 2.1 above, the Customer shall not: (a) copy iS5Com Materials for any purpose, except for the sole purpose of making an archival or back-up copy; (b) modify, translate or adapt the iS5Com Materials, or create derivative works based upon all or part of such iS5Com Materials; (c) assign, transfer, loan, lease, distribute, export, transmit, or sublicense iS5Com Materials to any other party; (d) use iS5Com Materials for service bureau, rent, timeshare or similar purposes; (e) decompile, disassemble, decrypt, extract, or otherwise reverse engineer, as applicable, iS5Com Software or iS5Com Hardware; (f) use iS5Com Materials in a manner that uses or discloses the Confidential Information of iS5Com or a third party without the authorization of such person; (g) permit third parties to use iS5Com Materials in any way that would constitute breach of this EULA; or (h) otherwise use iS5Com Materials except as expressly authorized herein.

- **2.3 Updates and Upgrades**

  The license granted hereunder shall apply to the latest version of iS5Com Materials provided to the Customer as of the effective date of this EULA, and shall apply to any Updates and Upgrades subsequently provided to the Customer by iS5Com pursuant to the terms of this EULA. Customer shall only be provided with Updates and/or Upgrades if expressly set out in the Contract.

- **2.4 Versions**

  In the event any Update or Upgrade includes an amended version of this EULA, Customer will be required to agree to such amended version in order to use the applicable iS5Com Materials and such amended EULA shall be deemed to amend the previously effective version of the EULA.

- **2.5 Third Party Software**

  Customer shall comply with any Third Party License Terms.

3) **OWNERSHIP**

- **3.1 Intellectual Property**

  Notwithstanding any other provision of the Contract, iS5Com and the Customer agree that iS5Com is and shall be the owner of all Intellectual Property Rights in iS5Com Materials and all related modifications, enhancements, improvements and upgrades thereto, and that no proprietary interests or title in or to the intellectual property in iS5Com Materials is transferred to the Customer by this EULA. iS5Com reserves all rights not expressly granted to the Customer under Section 2.1.

- **3.2 Firmware**

  iS5Com and the Customer agree that any and all iS5Com Firmware in or forming a part of iS5Com Hardware is being licensed and not sold, and that the words "purchase," "sell" or similar or derivative words are understood and agreed to mean "license," and that the word "Customer" as used herein are understood and agreed to mean "licensee," in each case in connection with iS5Com Firmware.

- **3.3 Third Party Software**

  Certain of iS5Com Software provided by iS5Com may be Third Party Software owned by one or more third parties and sublicensed to the Customer. Such third parties retain ownership of and title to such Third Party Software, and may directly enforce the Customer's obligations hereunder in order to protect their respective interests in such Third Party Software.

4) **CONFIDENTIALITY**

– **4.1 Confidentiality**

The Customer acknowledges that iS5Com Materials contain Confidential Information of iS5Com and that disclosure of such Confidential Information to any third party could cause great loss to iS5Com. The Customer agrees to limit access to iS5Com Materials to those employees or officers of the Customer who require access to use iS5Com Materials as permitted by the Contract and this EULA and shall ensure that such employees or officers keep the Confidential Information confidential and do not use it otherwise than in accordance with the Contract and this EULA. The obligations set out in this Section 4 shall continue notwithstanding the termination of the Contract or this EULA and shall only cease to apply with respect to such part of the Confidential Information as is in, or passes into, the public domain (other than in connection with the Customer's breach of this EULA) or as the Customer can demonstrate was disclosed to it by a third person who did not obtain such information directly or indirectly from iS5Com.

– **4.2 Irreparable Harm**

Without limiting any other rights or remedies available to iS5Com in law or in equity, the Customer acknowledges and agrees that the breach by Customer of any of the provisions of this EULA would cause serious and irreparable harm to iS5Com which could not adequately be compensated for in damages and, in the event of a breach by the Customer of any of such provisions, the Customer hereby consents to an injunction against it restraining it from any further breach of such provisions.

– **4.3 Security**

*Any usernames, passwords and/or license keys ("**Credentials**") provided to you by iS5Com shall be maintained by the Customer and its representatives in strict confidence and shall not be communicated to or used by any other persons. THE CUSTOMER SHALL BE RESPONSIBLE FOR ALL USE OF CREDENTIALS, REGARDLESS OF THE IDENTITY OF THE PERSON(S) MAKING SUCH USE, AND WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, IS5COM SHALL HAVE NO RESPONSIBILITY OR LIABILITY IN CONNECTION WITH ANY UNAUTHORIZED USE OF CREDENTIALS.*

5) **LIMITATION OF LIABILITY**

– **5.1 Disclaimer**

EXCEPT FOR THE EXPRESS WARRANTIES MADE BY IS5COM IN THE CONTRACT, (A) IS5COM MAKES NO AND HEREBY EXPRESSLY DISCLAIMS, AND THE PARTIES HERETO HEREBY EXPRESSLY WAIVE AND EXCLUDE TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAWS, AND THE CUSTOMER AGREES NOT TO SEEK OR CLAIM ANY BENEFIT THEREOF, IN EACH CASE, ALL WARRANTIES, CONDITIONS, REPRESENTATIONS OR INDUCEMENTS (AND THERE ARE NO OTHER WARRANTIES, CONDITIONS, REPRESENTATIONS OR INDUCEMENTS, ORAL OR WRITTEN, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, OF ANY KIND WHATSOEVER SET OUT HEREIN) WITH RESPECT TO THE IS5COM MATERIALS, INCLUDING AS TO THEIR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, DESIGN OR CONDITION, COMPLIANCE WITH THE REQUIREMENTS OF ANY APPLICABLE LAWS, CONTRACT OR SPECIFICATION, NON- INFRINGEMENT OF THE RIGHTS OF OTHERS, ABSENCE OF LATENT DEFECTS, OR AS TO THE ABILITY OF THE IS5COM MATERIALS TO MEET CUSTOMER'S REQUIREMENTS OR TO OPERATE OF ERROR

*FREE; AND (B) THE IS5COM MATERIALS ARE PROVIDED "**AS IS**" WITHOUT WARRANTY OR CONDITION OF ANY KIND.*

– **5.2 Limitation of Liability**

EXCEPT AS EXPRESSLY PROVIDED IN THE CONTRACT, IN NO EVENT SHALL IS5COM BE LIABLE TO THE CUSTOMER OR ANY THIRD PARTY FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING UNDER OR IN CONNECTION WITH THIS EULA EVEN IF ADVISE OF THE POSSIBILITY THEREOF. THIS LIMITATION SHALL APPLY IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND OR CLAIM, INCLUDING BREACH OF CONTRACT, NEGLIGENCE, TORT OR ANY OTHER LEGAL THEORY, AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES AND/OR FAILURE OF THE ESSENTIAL PURPOSE OF THIS EULA.

6) **TERM**

– **6.1 Term**

Customer's right to use iS5Com Materials shall terminate at such time as set out in the Contract or upon termination or expiration of the Contract, in each case at which time this EULA shall be deemed to terminate.

– **6.2 Survival**

Each of Sections 1, 2.4, 3, 4, 5, 6.2, and 7 shall survive termination of the EULA.

7) **MISCELLANEOUS**

– **7.1 Miscellaneous**

This EULA is (together with, as applicable, any click-wrap license agreement or Third Party License Terms pertaining to the use of iS5Com Materials) the entire agreement between the Customer and iS5Com pertaining to the Customer's right to access and use iS5Com Materials, and supersedes all prior or collateral oral or written representations or agreements related thereto. Notwithstanding anything to the contrary contained in the Contract, to the extent of any inconsistency between this EULA and the Contract, or any such applicable click-wrap agreement, this EULA shall take precedence over the Contract and such click- wrap agreement. In the event that one or more of the provisions is found to be illegal or unenforceable, this EULA shall not be rendered inoperative but the remaining provisions shall continue in full force and effect. The parties expressly disclaim the application of the United Nations Convention for the International Sale of Goods. This EULA shall be governed by the laws of the Province of Ontario, Canada, and federal laws of Canada applicable therein. In giving effect to this EULA, neither party will be or be deemed an agent of the other for any purpose and their relationship in law to the other will be that of independent contractors. Any waiver of any terms or conditions of this EULA: (a) will be effective only if in writing and signed by the party granting such waiver, and (b) shall be effective only in the specific instance and for the specific purpose for which it has been given and shall not be deemed or constitute a waiver of any other provisions (whether or not similar) nor shall such waiver constitute a continuing waiver unless otherwise expressly provided. The failure of either party to exercise, and any delay in exercising, any of its rights hereunder, in whole or in part, shall not constitute or be deemed a waiver or forfeiture of such rights, neither in the specific instance nor on a continuing basis. No single or partial exercise of any such right shall preclude any other or further exercise of such right or the exercise of any other right. Customer shall not assign or transfer this EULA or any of its rights or obligations hereunder, in whole or in part, without the prior written consent of

iS5Com. The division of this EULA into sections and the insertion of headings are for convenience of reference only and shall not affect the construction or interpretation of this EULA. References herein to Sections are to sections of this Agreement. Where the word "include", "includes" or "including" is used in this EULA, it means "include", "includes" or "including", in each case, "without limitation". All remedies provided for iS5Com under this EULA are non-exclusive and are in addition, and without prejudice, to any other rights as may be available to of iS5Com, whether in law or equity. By electing to pursue a remedy, of iS5Com does not waive its right to pursue any other available remedies. The parties acknowledge that they have required this Agreement to be written in English. Les parties aux présentes reconnaissent qu'elles ont exigé que la présente entente soit rédigée en anglais.

– **7.2 Subject to Change**

Terms and Conditions are subject to change. For the latest information please visit: https://is5com.com/terms-and-conditions/

GLOSSARY ENTRIES

802.1D

IEEE 802.1D is the Ethernet MAC bridges standard which includes Bridging, Spanning Tree and others. It is standardized by the IEEE 802.1 working group. It includes details specific to linking many of the other 802 projects including the widely deployed 802.3 (Ethernet), 802.11 (Wireless LAN) and 802.16 (WiMax) standards.
Bridges using virtual LANs (VLANs) have never been part of 802.1D, but were instead specified in separate standard, 802.1Q originally published in 1998.
By 2014, all the functionality defined by IEEE 802.1D has been incorporated into either IEEE 802.1Q (Bridges and Bridged Networks) or IEEE 802.1AC (MAC Service Definition).

802.1Q

IEEE 802.1Q, often referred to as DOT1Q or 1Q, is the networking standard that supports virtual LANs (VLANs) on an IEEE 802.3 Ethernet network. It is the most widely used encapsulation method for VLAN tagging.

802.1X

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). 802.1X authentication requires a client, an authenticator, and an authentication server. The client is a device that wants to connect to the network.

802.1W

IEEE 802.1W feature provides rapid traffic reconvergence for point-to-point links within a few milliseconds (0-500 milliseconds), following the failure of bridge or bridge point. This reconvergence occurs more rapidly than the reconvergence provided by the 802.1F spanning Tree Protocol (STP) or by RSTP.

AAA

Authentication, Authorization and Accounting (AAA) functionalities. AAA are provided by TACACS+. TACACS+ is used because it provides independently separate and modular authentication, authorization, and accounting (AAA) facilities achieved by a single access control server (the TACACS+ daemon).

AARP

AppleTalk Address Resolution Protocol (AARP). The AARP maps computers' physical hardware addresses to their temporarily assigned AppleTalk network addresses. AARP is functionally equivalent to Address Resolution Protocol (ARP). The AARP table permits management of the address mapping table on the managed device. This protocol allows Apple computers' AppleTalk hosts to generate their own network addresses

ABR

Area Border Router (ABR)

ACK

ACK stands for acknowledgment. ACK is one of the TCP flags.

TCP flags are various types of flag bits present in the TCP header. Each of them has its own significance. They initiate connections, carry data, and tear down connections. The commonly used TCP flags are SYN, ACK, RST, FIN, URG, PSH.

- SYN (synchronize): Packets that are used to initiate a connection.
- ACK (acknowledgment): Packets that are used to confirm that the data packets have been received, also used to confirm the initiation request and tear down requests.
- RST (reset): Signify the connection is down or maybe the service is not accepting the requests.
- FIN (finish): Indicate that the connection is being torn down. Both the sender and receiver send the FIN packets to gracefully terminate the connection.
- PSH (push): Indicate that the incoming data should be passed on directly to the application instead of getting buffered.
- URG (urgent): Indicate that the data that the packet is carrying should be processed immediately by the TCP stack

ACL

An access-control list (ACL) is a list of permissions associated with a system resource (object). An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation. For instance, if a file object has an ACL that contains (Admin: read, write; guest 1: read), this would give Admin permission to read and write the file, and only give guest 1 permission to read it.

AES

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption.

AH

The Authentication Header (AH) protocol provides data origin authentication, data integrity, and replay protection. However, AH does not provide data confidentiality, which means that all of your data is sent in the clear.

AH ensures data integrity with the checksum that a message authentication code, like MD5, generates. To ensure data origin authentication, AH includes a secret shared key in the algorithm that it uses for authentication. To ensure replay protection, AH uses a sequence number field within the AH header. It is worth noting here, that these three distinct functions are often lumped together and referred to as authentication. In the simplest terms, AH ensures that your data has not been tampered with en route to its final destination.

Although AH authenticates as much of the IP datagram as possible, the values of certain fields in the IP header cannot be predicted by the receiver. AH does not protect these fields, known as mutable fields. However, AH always protects the payload of the IP packet.

The Internet Engineering Task Force (IETF) formally defines AH in Request for Comment (RFC) 4302, IP Authentication Header.

AO

Authentication Option (AO). TCP-AO specifies the use of stronger Message Authentication Codes (MACs), protects against replays even for long-lived TCP connections, and provides more details on the association of security with TCP connections than TCP MD5. TCP-AO is compatible with either a static Master Key Tuple (MKT) configuration or an external, out-of-band MKT management mechanism; in either case, TCP-AO also protects connections when using the same MKT across repeated

instances of a connection, using traffic keys derived from the MKT, and coordinates MKT changes between endpoints.

ARAP

Apple Remote Access Protocol (ARAP); the Apple Remote Access Protocol (ARAP) sends traffic based on the AppleTalk protocol across PPP links and ISDN switched-circuit networks. ARAP is still pervasive in the Apple market, although the company is attempting to transition into an Apple-specific TCP stack for use over a PPP link.

ARP

ARP (Address Resolution Protocol). The ARP is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given Internet layer address, typically an IPv4 address.

AS

Autonomous System (AS)

ASBR

Autonomous Border System Router (ASBR)

Asdot

Asdot format is used when the 4-byte ASN are represented by their decimal value e.g. 100.1. BGP uses AS numbers as a fundamental part of its routing process. Because conventional 2-byte public AS numbers were becoming exhausted, the IANA increased the AS numbers by introducing a 4-byte AS numbers. The Asdot notation to represent these AS numbers is as follows.
For values between 0 and 65535, Asdot notation is simply the decimal value of the AS number. These values take up to 16 bits to express in binary. Examples include:

- 5
- 25
- 196
- 65000
- 65535

For values above 65536, Asdot notation splits the 32 bit binary value into two 16 bit values. These values are represented as two decimal numbers separated by a dot. Examples include:

- 0.65536
- 15.418
- 65535.8520
- 65535.65535

You will notice that for values of up to 65535, the Asdot is the same as the Asplain notation, and for values of 65536 and above, the Asdot is the same as the Asdot+ notation.

ASN

Autonomous System Number (ASN)

BDR

BDR stands for Backup Designated Router.

BFD

Bidirectional Forwarding Detection (BFD) is a super fast protocol that is able to detect link failures within milliseconds or even microseconds. BFD runs independent from any other (routing) protocols. Once it's up and running, you can configure protocols like OSPF, EIGRP, BGP, HSRP, MPLS LDP etc. to use BFD for link failure detection instead of their own mechanisms. When the link fails, BFD will inform the protocol

BGP

BGP (Border Gateway Protocol) is an Inter AS (Autonomous Systems) Routing Protocol that manages the distribution of Network Layer Reachability Information (NLRI) across AS. It is used to build an AS connectivity graph that is used to prune routing loops and enforce policies at AS level

BGP

BGP-4 is an extension of BGP-3 (BGP version 3),and it is the current version of BGP. BGP4 was published as RFC 4271 in 2006. Its major enhancement is the support for Classless Inter-Domain Routing (CIDR) and use of route aggregation to decrease the size of routing tables. The new RFC allows BGP4 to carry a wide range of IPv4 and IPv6 "address families".

BIDIR-PIM

Bi-directional Sparse Mode (PIM-SM); Derived from PIM-SM, BIDIR-PIM builds and maintains a bidirectional RPT, which is rooted at the RP and connects the multicast sources and the receivers. Along the bidirectional RPT, the multicast sources send multicast data to the RP, and the RP forwards the data to the receivers. Each router along the bidirectional RPT needs to maintain only one (*, G) entry, saving system resources.

Another difference between PIM sparse mode and PIM bidirectional mode is that with sparse mode traffic only flows down the shared tree. Using PIM bidirectional mode, traffic will flow up and down the shared tree. When the multicast packets arrive at the RP, they will be forwarded down the shared tree (if there are receivers) or dropped (when we don't have receivers).

BMS

Best Master Clock (BMS); The ordinary clock executes the port state machine and BMC (Best Master Clock) algorithm to select the *PTP* port state.

BOOTP

The Bootstrap Protocol (BOOTP) is a computer networking protocol used in Internet Protocol networks to automatically assign an IP address to network devices from a configuration server. The BOOTP was originally defined in RFC 951.

BPDU

Bridge Protocol Data Units (BPDUs) are frames that contain information about the spanning tree protocol (STP). A switch sends BPDUs using a unique source MAC address from its origin port to a multicast address.

There are two kinds of BPDUs for 802.1D Spanning Tree:[

- Configuration BPDU, sent by root bridges to provide information to all switches.
- TCN (Topology Change Notification), sent by bridges towards the root bridge to notify changes in the topology, such as port up or port down.

BPS

BPS (Bits-per-second)

BR

Border Router (BR)

BSD

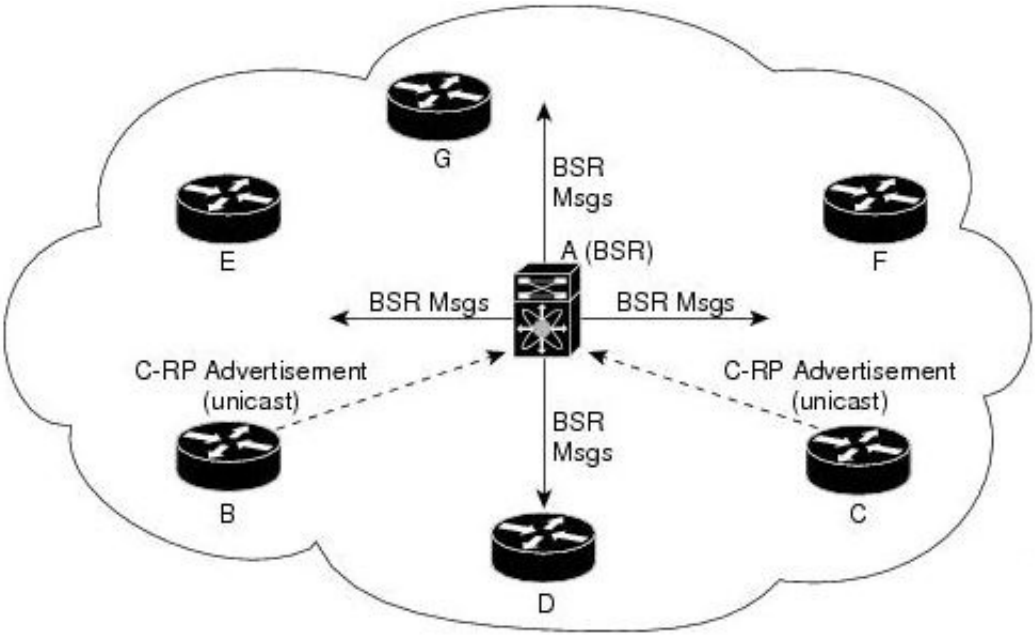
Berkeley Software Distribution (BSD)

BSR

The bootstrap router (BSR) ensures that all routers in the PIM domain have the same RP cache as the BSR. You can configure the BSR to help you select an RP set from BSR candidate RPs. The function of the BSR is to broadcast the RP set to all routers in the domain. You select one or more candidate BSRs to manage the RPs in the domain. Only one candidate BSR is elected as the BSR for the domain.

This figure shows the BSR mechanism. Router A, the software-elected BSR, sends BSR messages out all enabled interfaces (shown by the solid lines in the figure). The messages, which contain the RP set, are flooded hop by hop to all routers in the network. Routers B and C are candidate RPs that send their candidate-RP advertisements directly to the elected BSR (shown by the dashed lines in the figure).

The elected BSR receives candidate-RP messages from all the candidate RPs in the domain. The bootstrap message sent by the BSR includes information about all of the candidate RPs. Each router uses a common algorithm to select the same RP address for a given multicast group.



CA

Certificate Authorization (CA)

CBP

Customer Backbone Port (CBP)

CBS

Committed burst size (CBS). During periods of average traffic rates below the Committed information rate (CIR), any unused bandwidth capacity accumulates up to a maximum amount defined by the CBS. Short periods of bursting traffic (back-to-back traffic at averages rates that exceed the CIR) are also categorized as green provided that unused bandwidth capacity is available.

CEP

Customer Edge Port (CEP). The Customer Edge Port (CEP) and each Provider Edge Port are treated as separate Bridge Ports by the spanning tree protocol. If the C-VLAN component connects to the S-VLAN component with a single Provider Edge Port, and the associated service instance supports no more than two customer interfaces, then all frames (including Spanning Tree BPDUs) addressed to the Bridge Group Address may be relayed between the two Ports of the C-VLAN component without modification. Otherwise, the Spanning Tree Protocol Entity shall execute the Rapid Spanning Tree Protocol (RSTP, Clause 17 of IEEE Std 802.1D), as modified by the provisions of this subclause.

CFI

Canonical Format Identifier (CFI). If Drop Eligible Indicator (DEI) bit is enabled in 802.1ad header or has Canonical Format Identifier (CFI) bit enabled in 802.1q header on an arriving packet, such packets will be dropped using QoS.

MS-CHAP

CHAP stands for Challenge Handshake Authentication Protocol. MS-CHAP is the Microsoft version of the Challenge-Handshake Authentication Protocol, CHAP. The protocol exists in two versions, MS-CHAPv1 (defined in RFC 2433) and MS-CHAPv2 (defined in RFC 2759). MS-CHAPv2 provides mutual authentication between peers by piggybacking a peer challenge on the Response packet and an authenticator response on the Success packet.

CIDR

Classless Inter Domain Routing (CIDR).

CIR

Committed information rate (CIR) is defines the guaranteed bandwidth for traffic arriving at or departing from the interface under normal line conditions.

CIST

The Common and Internal Spanning Tree (CIST) is a collection of the ISTs in each MST region.

CLI

Command line interface (CLI) is a text-based interface that is used to operate software and operating systems while allowing the user to respond to visual prompts by typing single commands into the interface and receiving a reply in the same way

CLKIWF

CLKIWF is short for Clock InterWorking Function.

CoS

Output queue scheduling defines the class-of-service (CoS) properties of output queues. Based on certain types of traffic are preferred. The level of service is determined by the egress port queue to which the traffic is assigned. When traffic is queued for transmission, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in other queues for that port.

Some traffic is classified for service (i.e., packet marking) before it arrives at the switch. If you decide to use these classifications, you can map this traffic to egress queues by setting the CoS in the Queue table.

CPLD

A Complex Programmable logic device (CPLD) is a logic device with completely programmable AND/OR arrays and macrocells. Macrocells are the main building blocks of a CPLD, which contain complex logic operations and logic for implementing disjunctive normal form expressions. AND/OR arrays are completely reprogrammable and responsible for performing various logic functions.

CPU

The central processing unit (CPU) is the primary component of a computer that processes instructions. It runs the operating system and applications, constantly receiving input from the user or active software programs. It processes the data and produces output.

CRT

CRT stands for "Internet security certificate.

CSR

Certificate Signing Request (CSR)

CST

common spanning tree (CST); The common spanning tree (CST) that interconnects the MST regions and single spanning trees

CTS

CTS stands for Clear to Send. Request to Send (RTS)/CTS Flow Control is another flow control mechanism that is part of the RS232 standard.

CVID

The C-VID registration table is as follows:

Table 1: C-VID registration table

C-VID Registration Table	Description
Cvid value	The value of the Customer VLAN id on the Customer edge port. (Table key)
Svid Value	The S-VLAN tag. Auto creates an S-VLAN component and the CNP and PNP and links the PEP of the C-VLAN component to the CNP.
Untagged-pep	A boolean indicating frames for this C-VLAN should be forwarded untagged through the Provider Edge Port (PEP).
Untagged-cep	A boolean indicating frames for this C-VLAN should be forwarded untagged through the Customer Edge Port (CEP).

CVLAN

Set of ports & inner VLANs (CVLAN); or C-VLAN or Customer Bridge (CB)

DB9

DB9 refers to a common connector type from the D-Subminiatures (D-Sub) connector family, which when introduced, was among the smallest connectors used on computer systems. DB9 houses 9 pins (for the male connector) or 9 holes (for the female connector). DB9 connectors were once very

common on PCs and servers. Today, the DB9 has mostly been replaced by more modern interfaces such as USB, PS/2, Firewire, and others.

DB25

The DB25 connector is an analog socket, with 25 pins, from the D-Subminiatures (D-Sub) connector family. The prefix “D” represents the D-shape of the connector shell. The DB25 connector is mainly used in serial and parallel ports, allowing asynchronous data transmission according to the RS-232 standard (RS-232C).

DCD

DCD stands Data Carrier Detect. The description is modem connected to another.

DEC

Digital Equipment Corporation (DEC)

DEI

Drop Eligible Indicator (DEI). If DEI bit is enabled in 802.1ad header or has Canonical Format Identifier (CFI) bit enabled in 802.1q header on an arriving packet, such packets will be dropped using QoS.

DES

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption.

DF

Designated Forwarder (DF).

DH

Diffie and Hellman (*DH*) describe a method for two parties to agree upon a shared secret number, called ZZ, in such a way that the secret will be unavailable to eavesdroppers. This method requires that both the sender and recipient of a message have key pairs (private and public). By combining one's private key and the other party's public key, both parties can compute the same shared secret number ZZ

DHCP

Dynamic Host Configuration Protocol (DHCP)

DITA

Darwin Information Typing Architecture (DITA); the DITA specification defines a set of document types for authoring and organizing topic-oriented information, as well as a set of mechanisms for combining, extending, and constraining document types.

D-LAG

Distributed Link Aggregation (D-LAG or DLAG)

DLF

The Destination Lookup Failure (DLF). When a packet arrives at the device and the device doesn't have an entry for the destination MAC address in its MAC address table, the packet is classified as a Destination Lookup Failure (DLF)

DM

DM stands for Dense Mode. Protocol-Independent Multicast Dense Mode (PIM-DM) uses dense multicast routing.

DNAT

Destination network address translation (DNAT) is a technique for transparently changing the destination IP address of an end route packet and performing the inverse function for any replies.

DNS

Domain Name System

DOT1Q

IEEE 802.1Q, often referred to as DOT1Q or 1Q, is the networking standard that supports virtual LANs (VLANs) on an IEEE 802.3 Ethernet network. It is the most widely used encapsulation method for VLAN tagging.

Dot1x

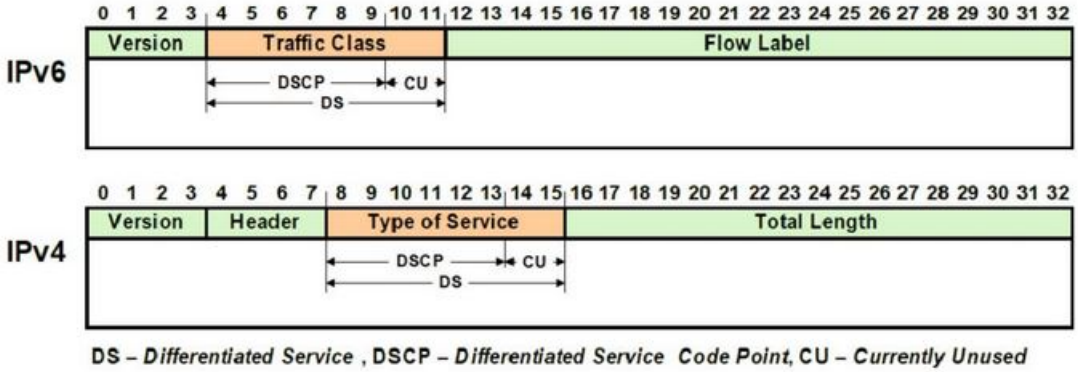
Dot1x Authentication is enabled when dot1x system-auth-control is enabled, and aaa authentication dot1x default is local. If you enable authentication on a port by using the default setting of dot1x port-control, which is force-authorized, it disables 802.1X authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client

DR

The Designated Router (DR) is the router that will forward the PIM join message from the receiver to the RP (rendezvous point).

DS

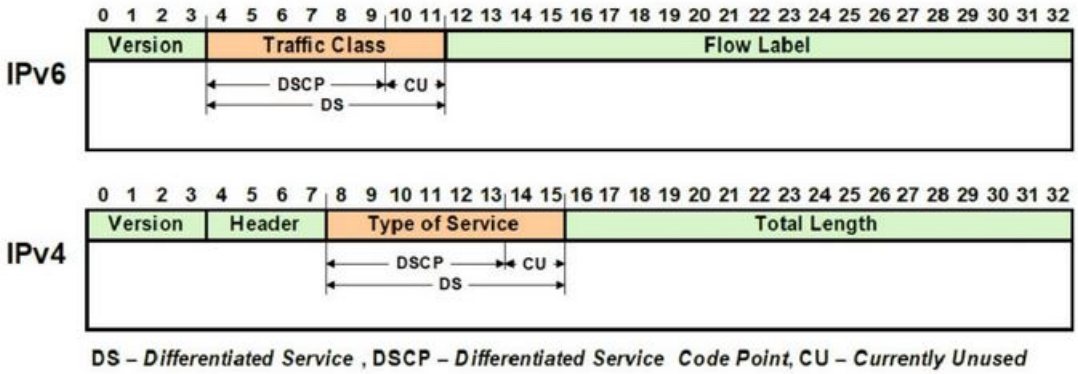
Differentiated Services (DS).



DS – *Differentiated Service* , DSCP – *Differentiated Service Code Point*, CU – *Currently Unused*

DSCP

A Differentiated Services Code Point (DSCP) is a packet header value that can be used to request (for example) high priority or best effort delivery for traffic.



DS – *Differentiated Service* , DSCP – *Differentiated Service Code Point*, CU – *Currently Unused*

DSR

DSR stands Data Set Ready. The description is ready to communicate.

DST

Daylight Saving Time (DST) is a system of setting clocks ahead so that both sunrise and sunset occur at a later hour. The effect is additional daylight in the evening. Many countries observe DST, although most have their own rules and regulations for when it begins and ends. The dates of DST may change from year to year

DTR

DTR stands Data Terminal Ready. The description is ready to communicate.

DUT

Device under Test (DUT)

DVMRP

Distance Vector Multicast Routing Protocol (DVMRP)

E2E

End-to-end (E2E) transparent clock for Precision Time Protocol (PTP). With an E2Etransparent clock, only the residence time is included in the timestamp in the packet.

EAP

Extensible Authentication Protocol (EAP) is an authentication framework frequently used in network and Internet connections. EAP is usually tunnelled over RADIUS between the Authenticator and the Authentication Server. 802.1x uses EAP.

EAP is an authentication framework, not a specific authentication mechanism. Commonly used modern methods capable of operating in wireless networks include EAP-TLS, EAP-SIM, EAP-AKA, LEAP and EAP-TTLS. Requirements for EAP methods used in wireless LAN authentication are described in RFC 4017.

The Lightweight Extensible Authentication Protocol (LEAP) method was developed by Cisco Systems prior to the IEEE ratification of the 802.11i security standard.

EAPOL

Extensible Authentication Protocol (EAP) over LAN (EAPoL) is used between the Supplicant (software on your laptop) and the Authenticator (switch)

EBGP

External *BGP* (EBGP); EBGP runs between two BGP routers in different Autonomous System (AS).

EBS

The Excess Burst size (EBS) specifies how much data above the committed burst size (CBS) a user can transmit. The EBS is the size up to which the traffic is allowed to burst without being discarded. EBS allows for moderate periods of bursting traffic that exceeds both the committed information rate (CIR) and the committed burst size (CBS).

ECN

Explicit Congestion Notification (ECN)

EGP

Exterior Gateway Protocol (EGP) is a defunct routing protocol used in autonomous systems to exchange data between surrounding gateway sites. Border Gateway Protocol (BGP) supplanted EGP, widely utilized by research institutes, universities, government agencies, and commercial

companies (BGP). EGP is built on poll instructions to request update answers and periodic message exchange polling for neighbor reachability.

EIR

The excess information rate (EIR) specifies the rate above the CIR (committed information rate) at which traffic is allowed into the network and that may get delivered if the network is not congested. The EIR has an additional parameter associated with it called the excess burst size (EBS). The EBS is the size up to which the traffic is allowed to burst without being discarded.

ESD

ElectroStatic Discharge (ESD) is the sudden flow of electricity between two electrically charged objects caused by contact, an electrical short or dielectric breakdown. A buildup of static electricity can be caused by tribocharging or by electrostatic induction. The ESD occurs when differently-charged objects are brought close together or when the dielectric between them breaks down, often creating a visible spark.

EXEC

exec: Protocol
Commands that are invoked using the exec: protocol must be executable as standalone commands. Commands that are built into a command interpreter or other program cannot be executed directly, but must be executed (if possible) within the context of the application that provides them. For example, the following seed URL would not work on Microsoft Windows systems because the dir command is built into the Windows command interpreter (cmd.exe):
exec: dir e:\data
To use the exec protocol with commands that are built into the Windows command interpreter, you must do something as the following:
exec: cmd /c dir 'e:\data'

ESP

Encapsulation Security Protocol (ESP); the ESP protocol provides data confidentiality, and also optionally provides data origin authentication, data integrity checking, and replay protection. The difference between ESP and the Authentication Header (AH) protocol is that ESP provides encryption, while both protocols provide authentication, integrity checking, and replay protection. With ESP, both communicating systems use a shared key for encrypting and decrypting the data they exchange.

EVB

Edge Virtual Bridge (EVB) is an IEEE standard that involves the interaction between virtual switching environments in a hypervisor and the first layer of the physical switching infrastructure. The EVB enhancements are following 2 different paths – 802.1qbg and 802.1qbh.

EVC

Ethernet Virtual Connection (EVC).

FCS

A frame check sequence (FCS) is an error-detecting code added to a frame in a communication protocol. Frames are used to send payload data from a source to a destination.

FDB

Forwarding Database (FDB)

FID

Filtering ID (FID)

FHRP

First Hop Redundancy Protocol (FHRP)

FPGA

The Field Programmable Gate Array (FPGA) is a programmable logic device that can have its internal configuration set by the firmware.

FTP

The File Transfer Protocol (FTP) is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture using separate control and data connections between the client and the server.[1] FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP).

GARP

GARP (Generic Attribute Registration Protocol) is a local area network (LAN) protocol that defines procedures by which end stations and switches can register and deregister attributes, such as network identifiers or addresses, with each other. Every end station and switch thus has a record, or list, of all the other end stations and switches that can be reached at any given time.
When an attribute for an end station or switch is registered or deregistered according to GARP, the set of reachable end stations and switches, called participants, is modified according to specific rules. The defined set of participants at any given time, along with their attributes, is a subset of the network topology called the reachability tree. Data frames are propagated only to registered end stations. This prevents attempts to send data to end stations that are not reachable.

GGP

Gateway-to-Gateway Protocol (GGP) is an obsolete protocol defined for routing datagrams between Internet gateways. It was first outlined in 1982. The GGP was designed as an IP datagram service similar to the TCP and the UDP.

GMRP

GARP Multicast Registration Protocol (GMRP) is a Generic Attribute Registration Protocol (GARP) application that provides a constrained multicast flooding facility similar to IGMP snooping.

GND

Ground

GPS

Global Positioning System

GR

Graceful Restart (GR)

GRE

Generic routing encapsulation (GRE) is an IP encapsulation protocol which is used to transport IP packets over a network. In GRE, an IP datagram is tunnelled (encapsulated) within another IP datagram.One great advantage of GRE is that it allows routing of IP packets between private IPv4

networks which are separated over public IPv4 Internet. GRE also supports encapsulating IPv4 broadcast and multicast traffic.

GVRP

GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frame s with VLAN configuration data

HA

High Availability (HA)

HDMI

HDMI (High-Definition Multimedia Interface) is digital interface capable of transmitting high-quality and high-bandwidth streams of audio and video between devices

HOL

Head-Of-Line (HOL) blocking should be prevented on a port. HOL blocking happens when HOL packet of a buffer cannot be switched to an output port (i.e. HOL occurs when a line of packets is held up by the first packet).

HSR

High-availability Seamless Redundancy (HSR) is a network protocol for Ethernet that provides seamless failover against failure of any single network component. PRP and HSR are standardized by the IEC 62439-3:20 and are suited for applications that request high availability and short switchover time.

HTTP

Hyper Text Transfer Protocol (HTTP)

HTTPS

Hyper Text Transfer Protocol Secure (HTTPS)

IANA

Internet Assigned Numbers Authority (IANA)

IBGP

Internal BGP (iBGP) is the protocol used between the routers in the same autonomous system (AS). iBGP is used to provide information to your internal routers. iBGP requires all the devices in same AS to form full mesh neighborship or either of Route reflectors and Confederation for prefix learning.

ICMP

Internet Control Message Protocol

IDPR

Inter-domain Routing Protocol (IDPR). The objective of IDPR is to construct and maintain routes, between source and destination administrative domains, that provide user traffic with the requested services within the constraints stipulated for the domains transited.

IETF

Internet Engineering Task Force (IETF) is an open standards organization, which develops and promotes voluntary Internet standards, in particular the technical standards that comprise the Internet protocol suite (TCP/IP).

IGMP

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast and allows the network to direct multicast transmissions only to hosts that have requested them.

IGP

Interior Gateway Protocol (IGP) is a type of routing protocol used for exchanging routing table information between gateways (commonly routers) within an autonomous system (for example, a system of corporate local area networks). This routing information can then be used to route network-layer protocols like IP.

IGRP

Interior Gateway Routing Protocol (IGRP) is a proprietary distance vector routing protocol that manages the flow of routing information within connected routers in the host network or autonomous system. The protocol ensures that every router has routing tables updated with the best available path. IGRP also avoids routing loops by updating itself with the changes occurring over the network and by error management.

IGS

The Internet Group Management Protocol (IGMP) Snooping (IGS) is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. It provides switches with a mechanism to prune multicast traffic from links that do not contain a multicast listener (an IGMP client). Essentially, IGS is a layer 2 optimization for the Layer 3 IGMP.

IKE

Internet Key Exchange (IKE)

IP

Internet Protocol (IP).

IPSec

IPSec (Internet Protocol Security) is a suite of protocols that provides security to Internet communications at the IP layer. The most common current use of IPSec is to provide a Virtual Private Network (VPN), either between two locations (gateway-to-gateway) or between a remote user and an enterprise network (host-to-gateway); it can also provide end-to-end, or host-to-host, security.

IPv4

IPv4 and IPv6 are Internet protocol version 4 and Internet protocol version 6. IPv4 supports:

- IPv4 has a 32-bit address length
- IPv4 binary bits are separated by a dot(.) whereas IPv6 binary bits are separated by a colon(:).
- IPv4 is a numeric addressing method whereas IPv6 is an alphanumeric addressing method
- It Supports Manual and DHCP address configuration
- In IPv4 end to end, connection integrity is Unachievable
- It can generate 4.29×109 address space
- Fragmentation performed by Sender and forwarding routers
- In IPv4 Packet flow identification is not available
- In IPv4 checksum field is available
- It has broadcast Message Transmission Scheme

- In IPv4 Encryption and Authentication facility not provided
- IPv4 has a header of 20-60 bytes.

IPv6

IPv6 stands for Internet protocol version 6. An IPv6 address consists of eight groups of four hexa-decimal digits. Anexample of IPv6 address is as follows
3001:0da8:75a3:0000:0000:8a2e:0370:7334
there are different ypes of IPv6 addresses:

- Unicast addresses—it identifies a unique node on a network and usually refers to a single sender or a single receiver.
- Multicast addresses—it represents a group of IP devices and can only be used as the destination of a datagram.
- Anycast addresses—it is assigned to a set of interfaces that typically belong to different nodes.

IRTP

Internet Reliable Transaction Protocol (IRTP) is a transport level host to host protocol designed for an Internet environment. It provides reliable, sequenced delivery of packets of data between hosts and multiplexes / demultiplexes streams of packets from/to user processes representing ports.

ISAKMP

Internet Security Association and Key Management Protocol (ISAKMP)

ISDN

Integrated Services Digital Network (ISDN)

ISL

ISL stands for Inter-Switch Link which is one of the VLAN protocols. The ISL is proprietary of Cisco and is used only between Cisco switches. It operates in a point-to-point VLAN environment and supports up to 1000 VLANs and can be used over Fast Ethernet and Gigabit Ethernet links only.

ISP

Internet service provider (ISP)

ISS

Intelligent Switch Solution (ISS).

IST

The Internal Spanning Tree (IST) instance receives and sends BPDUs to the CST. The IST can repre-sent the entire MST region as a CST virtual bridge to the outside world.

IVL

Independent VLAN Learning (IVL)

IVR

Inter VLAN Routing (IVR)

IWF

InterWorking Function (IWF).

KDF

Key Derivation Functions (KDFs); TCP-AO's Traffic_Keys are derived using KDFs. As per RFC5926, when invoked, a KDF generates a string of length Output_Length bit based on the Master_Key and

context value. This result may then be used as a cryptographic key for any algorithm that takes anOutput_Length length key. A KDF MAY specify a maximum Output_Length parameter.

L2GP

Layer 2 Gateway Port (L2GP)

LA

Link Aggregation

LACP

Link Aggregation Control Protocol

LAG

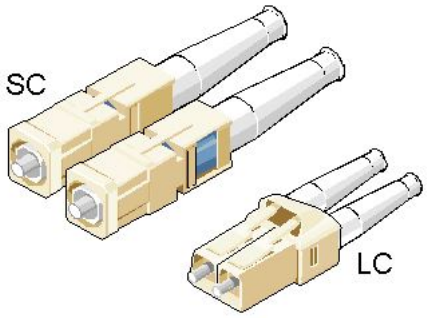
Link Aggregation Group

LAN

Local Area Network

LC

LC (Lucent Connector) is a miniaturized version of the fiber-optic SC (Standard Connector) connector. It looks somewhat like the SC, but is half the size with a 1.25mm ferrule instead of 2.5mm.



SC and LC Connectors

LED

Light-emitting diode (LED) is a widely used standard source of light in electrical equipment.

LLDP

Link Layer Discovery Protocol (LLDP)

LM

Line Module (LM)

LRE

Link Redundancy Entity (LRE); Each redundant switch or LRE (Link Redundancy Entity) must be represented by a logical interface (a.k.a redundant interface or Red X) in ISS. This logical interface will be used to configure the port A and B of the redundant switch

LSA

Link State Advertisement (LSA)

LSDB

link state database (LSDB)

LSR

link state routing (LSR)

MAC

Media access control (MAC) is a sublayer of the data link layer in the seven-layer OSI network reference model. MAC is responsible for the transmission of data packets to and from the network-interface card, and to and from another remotely shared channel.

MAU

Medium Attachment Unit (MAU)

MD5

Message Digest Algorithm 5 (MD5) is a cryptographic hash algorithm that can be used to create a 128-bit string value from an arbitrary length string.

A hash function provides encryption using an algorithm and no key. A variable-length plaintext is "hashed" into a (typically) fixed-length hash value (often called a "message digest" or simply a "hash"). Hash functions are primarily used to provide integrity; if the hash of a plaintext changes, the plaintext itself has changed.

Common older hash functions include Secure Hash Algorithm 1 (SHA-1), which creates a 160-bit hash and Message Digest 5 (MD5), which creates a 128-bit hash.

Although there has been insecurities identified with MD5, it is still widely used, and its most common use is to verify the integrity of files.

MDI

Media Independent Interface (MDI) and Media Independent Interface with Crossover (MDIX) are basically ports on a computer and a network switch, router, or hub, respectively.

MDIX

Media Independent Interface with Crossover (MDIX) and Media Independent Interface (MDI) are basically ports on a computer and a network switch, router, or hub, respectively.

MED

1) Media Endpoint Discovery (MED); LLDP does not contain the capability of negotiating additional information such as PoE management and VLAN assignments. This capability was added as an enhancement known as Media Endpoint Discovery or MED, resulting in the enhanced protocol LLDP-MED.The MED enhancement has been standardized by the Telecommunications Industry Association in standard number ANSI/TIA-1057.
2) Multi Exit Discriminator (MED) for routes received from different autonomous systems; MED is one of the parameters considered for selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED.

MHRP

Multipath Hybrid Routing Protocol (MHRP) is a multipath routing protocol for hybrid Wireless Mesh Network (WMN), which provides security and uses technique to find alternate path in case of route failure.

MIB

Management Information Base (MIB) is the hierarchical database used by the simple network management protocol (SNMP) to describe the particular device being monitored.

MIB OID

Management Information Base (MIB) is the hierarchical database used by the simple network management protocol (SNMP) to describe the particular device being monitored.
MIB Object IDentifier (OID), as known as a MIB object identifier in the SNMP, is a number assigned to devices in a network for identification purposes. OID numbering is hierarchical. Using the IETF notation of digits and dots, resembling very long IP addresses, various registries such as ANSI assign high-level numbers to vendors and organizations. They, in turn, append digits to the number to identify individual devices or software processes.

MIC

Media redundancy Interconnection Client (MIC) is a member node of a MRP Interconnect ring.

MIM

Media redundancy Interconnection Manager (MIM) is a node in a MRP Interconnect ring which acts a redundancy manager.

MLDS

Multicast Listener Discovery Snooping (MLDS) constrains the flooding of IPv6 multicast traffic on VLANs. When MLDS is enabled on a VLAN, adevice examines MLD messages between hosts and multicast routers and learns which hosts are interested in receiving traffic for a multicast group. On the basis of what it learns, the device then forwards multicast traffic only to those interfaces in the VLAN that are connected to interested receivers instead of flooding the traffic to all interfaces.

MKT

Master Key Tuple (MKT). TCP-AO uses cryptographic algorithms to convert MKTs, which can be shared across connections, into unique traffic keys for each connection.

MM

MultiMode (MM) Mode is in optical fiber with a larger core than singlemode fiber. Typically, MM has a core diameter of 50 or 62.5 μm and a cladding diameter of 125 μ.

MIC

Media redundancy Interconnection Client (MIC) is a member node of a MRP Interconnect ring.

MPLS

Multiprotocol Label Switching (MPLS) is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols, hence the "multiprotocol" reference on its name.

MRA

Media Redundancy Automanager (MRA). To configure a Media Redundancy Automanager (MRA), the node or nodes elect an MRM by a configured priority value.

MRC

Media Redundancy Client (MRC) is a member node of a MRP ring.

MRM

Media Redundancy Manager (MRM) is a node in the network which acts a redundancy manager.

MRP

Media Redundancy Protocol (MRP) is a networking protocol designed to implement redundancy and recovery in a ring topology.

MSR

1) MSR (MIB Save and Restore).
2) Model-Specific Register (*MSR*)

MST

MST (Multiple Spanning Tree) is the version of STP that allows multiple VLANs to a single instance. It is the standard based protocol defined with IEEE 802.1s. Unlike other spanning tree protocols, in which all the spanning tree instances are independent, MST establishes and maintains IST, CIST, and CST spanning trees.

MSTI

Multiple spanning trees, called MSTIs; inside an MST region, multiple spanning trees, called MSTIs, are calculated. Among these MSTIs, MSTI 0 is the IST.

MSTP

Multiple Spanning-Tree Protocol

MTU

Maximum Transmission Unit (MTU)

MVLAN

Multicast VLANs (MVLAN)

NAP

Network Access Protection (NAP)

NAPT

Network address port translation (NAPT) is a variation of the traditional *NAT*. NAPT extends the notion of translation one step further by also translating transport identifiers (e.g., TCP and UDP port numbers, ICMP query identifiers).

NAS

The Network Access Server (NAS) is the front line of authentication – it's the first server that fields network authentication requests before they pass through to the RADIUS. The NAS Identifier (NAS-ID) is a feature that allows the RADIUS server to confirm information about the sender of the authentication request.

NAT

Network address translation (NAT) is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

NBMA

NBMA (Non Broadcast Multi Access)

NBNS

NetBIOS Name Server where NetBIOS stands for Network Basic Input / Output System.

NC

NC (normally closed) is a closed (short) circuit creating a path for the current.

ND

Neighbor Discovery (ND); the Virtual Router Redundancy Protocol (*VRRP*) for IPv6 provides a much faster switchover to an alternate default router than can be obtained using standard neighbor discovery (ND) procedures.

NETBIOS

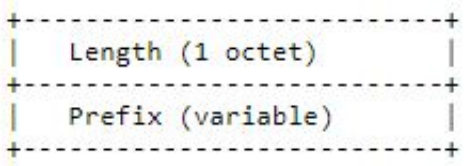
Network Basic Input / Output System (NETBIOS)

NIP

This set of fields are a vector of N IP unicast addresses, where the value N corresponds to the Number or Sources (N) field.

NLRI

Network Layer Reachability Information (NLRI). The Network Layer Reachability information is encoded as one or more 2-tuples of the form <length, prefix>, whose fields are described below.



NMS

Network Management System (NMS)

NO

NO (normally open) is an open circuit not creating a path for the current.

NPS

Network Policy Server (NPS)

NSSA

Not-so-stubby Area (NSSA)

NTP

Network Time Protocol (NTP)

NVP

Network Voice Protocol (NVP) was a pioneering computer network protocol for transporting human speech over packetized communications networks. It was an early example of Voice over Internet Protocol technology.

NVRAM

Non-volatile random-access memory (NVRAM) is random-access memory that retains data without applied power. This is in contrast to dynamic random-access memory (DRAM) and static random-access memory (SRAM), which both maintain data only for as long as power is applied, or such forms of memory as magnetic tape, which cannot be randomly accessed but which retains data indefinitely without electric power.

OID

Object IDentifier

ORF

Outbound Route Filter (ORF); the BGP Prefix-Based ORF feature uses BGP ORF send and receive capabilities for minimizing the number of BGP updates that are sent between BGP peers. Configuring this feature can help reduce the amount of system resources required for generating and processing routing updates by filtering out unwanted routing updates at the source.

OSPF

Open Shortest Path First routing protocol

OUI

organization unique identifiers (OUI)s. LLDP enables defining optional *TLV* units by using organization unique identifiers (OUIs) or organizationally-specific TLVs. An OUI identifies the category for a *TLV* unit depending on whether the OUI follows the IEEE 802.1 or IEEE 802.3 standard.

P2P

Peer-to-peer (P2P) transparent clock for Precision Time Protocol (PTP).

PAE

Port Access Entity (PAE). 802.1X-2001 defines two logical port entities for an authenticated port—the "controlled port" and the "uncontrolled port". The controlled port is manipulated by the 802.1X PAE (Port Access Entity) to allow (in the authorized state) or prevent (in the unauthorized state) network traffic ingress and egress to/from the controlled port. The uncontrolled port is used by the 802.1X PAE to transmit and receive EAPOL frames.

PAP

Password Authentication Protocol (PAP) is a password-based authentication protocol used by Point to Point Protocol (PPP) to validate users. PAP stops working after establishing the authentication; thus, it can lead to attacks on the network.

PC

Personal Computer

PCB

Provider Core Bridge (PCB) or S-VLAN Bridge; PCB integrates only one S-VLAN component. It is capable of providing single service on a port.

PDU

A Protocol Data Unit (PDU) is a single unit of information transmitted among peer entities of a computer network. A PDU is composed of protocol-specific control information and user data.

P/E

Program/Erase (P/E). Writing a byte to flash memory involves two steps: Program and Erase (P/E). P/E cycles can serve as a criterion for quantifying the endurance of a flash storage device.

PEB

Provider Edge Bridge (PEB); Provider Edge Bridge integrates one S-VLAN component with zero or many C-VLAN components as well as integrates each C-VLAN (up to 4094 C-VLANs) individually with a different S-VLAN (up to 4094 S-VLANs).

PEM

PEM (originally “Privacy Enhanced Mail”) is the most common format for X.509 certificates, CSRs, and cryptographic keys. A PEM file is a text file containing one or more items in Base64 ASCII encoding, each with plain-text headers and footers (e.g. -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----). A single PEM file could contain an end-entity certificate, a private key, or multiple certificates forming a complete chain of trust. Most certificate files downloaded from SSL.com will be in PEM format

PEP

Provider Edge Port (PEP). The Customer Edge Port and each Provider Edge Port are treated as separate Bridge Ports by the spanning tree protocol. If the C-VLAN component connects to the S-VLAN component with a single Provider Edge Port, and the associated service instance supports no more than two customer interfaces, then all frames (including Spanning Tree BPDUs) addressed to the

Bridge Group Address may be relayed between the two Ports of the C-VLAN component without modification. Otherwise, the Spanning Tree Protocol Entity shall execute the Rapid Spanning Tree Protocol (RSTP, Clause 17 of IEEE Std 802.1D), as modified by the provisions of this subclause.

PFS

Perfect Forward Secrecy (PFS) means that a piece of an encryption system automatically and frequently changes the keys it uses to encrypt and decrypt information, such that if the latest key is compromised, it exposes only a small portion of the user's sensitive data.
If PFS is specified in the IPSec policy, a new Diffie-Hellman exchange is performed with each quick mode, providing keying material that has greater entropy (key material life) and thereby greater resistance to cryptographic attacks. Each Diffie-Hellman exchange requires large exponentiations, thereby increasing CPU use and exacting a performance cost.

PHB

PHB (Per Hop Behavior) is a term used in differentiated services (DiffServ) or multiprotocol label switching (MPLS). It defines the policy and priority applied to a packet when traversing a hop (such as a router) in a DiffServ network.

PHY

A PHY, an abbreviation for "physical layer", is an electronic circuit, usually implemented as an integrated circuit, required to implement physical layer functions of the OSI model in a network interface controller.A PHY connects a link layer device (often called MAC as an acronym for medium access control) to a physical medium such as an optical fiber or copper cable. A PHY device typically includes both physical coding sublayer (PCS) and physical medium dependent (PMD) layer functionality. -PHY may also be used as a suffix to form a short name referencing a specific physical layer protocol, for example M-PHY..

PIM

Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other routing protocols. PIM is not dependent on a specific unicast routing protocol; it can make use of any unicast routing protocol in use on the network. PIM does not build its own routing tables. PIM uses the unicast routing table for reverse-path forwarding.
There are four variants of PIM:

- PIM Sparse Mode (PIM-SM) explicitly builds unidirectional shared trees rooted at a rendezvous point (RP) per group, and optionally creates shortest-path trees per source. PIM-SM generally scales fairly well for wide-area usage.
- PIM Dense Mode (PIM-DM) uses dense multicast routing. It implicitly builds shortest-path trees by flooding multicast traffic domain wide, and then pruning back branches of the tree where no receivers are present. PIM-DM is straightforward to implement but generally has poor scaling properties. The first multicast routing protocol, DVMRP used dense-mode multicast routing. See the PIM Internet Standard RFC 3973.
- Bidirectional PIM (Bidir-PIM) explicitly builds shared bi-directional trees. It never builds a shortest path tree, so may have longer end-to-end delays than PIM-SM, but scales well because it needs no source-specific state. See Bidirectional PIM Internet Standard RFC 5015, 70–73 .

- PIM Source-Specific Multicast (PIM-SSM) builds trees that are rooted in just one source, offering a more secure and scalable model for a limited number of applications (mostly broadcasting of content). In SSM, an IP datagram is transmitted by a source S to an SSM destination address G, and receivers can receive this datagram by subscribing to channel (S,G). See informational RFC 3569

Bidirectional (Bidir) *PIM*

Bidirectional PIM (Bidir-PIM) explicitly builds shared bi-directional trees. It never builds a shortest path tree, so may have longer end-to-end delays than PIM-SM, but scales well because it needs no source-specific state. See Bidirectional PIM Internet Standard RFC 5015, 70–73.

PIM-DM

Protocol-Independent Multicast Dense Mode PIM-DM) uses dense multicast routing. It implicitly builds shortest-path trees by flooding multicast traffic domain wide, and then pruning back branches of the tree where no receivers are present. PIM-DM is straightforward to implement but generally has poor scaling properties.

PIM-SM

Protocol-Independent Multicast Sparse Mode (PIM-SM) explicitly builds unidirectional shared trees rooted at a rendezvous point (RP) per group, and optionally creates shortest-path trees per source. PIM-SM generally scales fairly well for wide-area usage.

PING

Packet INternet Groper (PING or Ping)

PIP

Provider Instance Port (PIP)

PIR

Peak Information Rate (PIR) is a burstable rate set on routers and/or switches that allows throughput overhead. Related to committed information rate (CIR) which is a committed rate speed guaranteed/capped.

PMBR

PIM Multicast Border Router (PMBR)

PMTU

Path Maximum Transmission Unit (PMTU)

PNAC

Port Based Network Access Control (PNAC), or 802.1X, authentication requires a client, an authenticator, and an authentication server. The client is a device that wants to connect to the network.

PNP

Provider Network Ports (PNP)

PoE

Power over Ethernet (PoE) is distributing power over an Ethernet network. Because the power and signal are on the same cable, PoE enables remote network devices such as ceiling-mounted access points, surveillance cameras and LED lighting to be installed far away from AC power sources.

PPP

- Point-to-Point Protocol (PPP); The user or machine sends a request to a Network Access Server (NAS) to gain access to a particular network resource using access credentials. The credentials are

passed to the NAS device via the data link layer (L2) protocol—for example, Point-to-Point Protocol (PPP) in the case of many dial up or DSL providers or posted in an HTTPS secure web form.

- Protocol Packet Processing (PPP)

PPVID

Port and Protocol *VLAN* ID (PPVID)

PRP

Parallel Redundancy Protocol (PRP) is a network protocol standard for Ethernet that provides seamless failover against failure of any network component. This redundancy is invisible to the application.PRP nodes have two ports and are attached to two separated networks of similar topology. PRP can be implemented entirely in software, i.e. integrated in the network driver. Nodes with single attachment can be attached to one network only. This is in contrast to the companion standard HSR (IEC 62439-3 Clause 5), with which PRP shares the operating principle.

PS

Power Supply

PTP

Precision Timing Protocol

PVID

Port *VLAN* ID (PVID)

PVLAN

Private VLAN (PVLAN); Private VLAN, also known as port isolation, is a technique in computer networking where a VLAN contains switch ports that are restricted such that they can only communicate with a given uplink. The restricted ports are called private ports

PVRST

Per VLAN Rapid Spanning-Tree

PVRSTP

Per VLAN Rapid Spanning-Tree Protocol

PW

An Ethernet pseudowire (PW) is used to carry Ethernet/802.3 Protocol Data Units (PDUs) over an MPLS network. See RFC 4448 for details.

Q-in-Q

802.1Q tunneling (Q-in-Q) is a technique often used by Ethernet providers as a layer 2 VPN for customers. During 802.1Q (or dot1q) tunneling, the provider will put an 802.1Q tag on all the frames that it receives from a customer with a unique VLAN tag. By using a different VLAN tag for each customer we can separate the traffic from different customers and also transparently transfer it throughout the service provider network.

QoS

Quality of Service (QoS) refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. QoS defines the ability to provide different priorities to different applications, users, or data flows or the ability to guarantee a certain level of performance to a data flow.

QRV

Querier’s Robustness Variable (QRV).

RADIUS

Remote Authentication Dial-In User Service

RAM

Random-access memory (RAM) is a form of computer memory that can be read and changed in any order, and typically is used to store working data and machine code.

RARP

The Reverse Address Resolution Protocol (RARP) is an obsolete computer communication protocol used by a client computer to request its Internet Protocol (IPv4) address from a computer network, when all it has available is its link layer or hardware address, such as a MAC address.

RBAC

Role Based Authentication (RBAC)

RED

1) Random early detection (RED) is where a single queue may have several different sets of queue thresholds.
2) Redundant interface (RED) (e.g. RED 1 or RED 2).

RFD

A flapping route is an unstable route that is advertised and withdrawn over and over again. Every time a flap occurs, a BGP UPDATE message is sent. When routers have to process many BGP UPDATE messages, their CPU load increases.
BGP route dampening can be used to prevent installing flapping BGP routes and forwarding them to other BGP routers. This decreases the CPU load of routers and increases network stability. Nowadays, routers are powerful enough to process BGP updates so dampening isn't considered a best practice anymore
RFP has 5 attributes - the default values are shown

- Penalty
- Suppress-Limit - 2000
- Half-Life - 900 secs
- Reuse limit - 750
- Maximum Suppress-Limit -3600 secs (60 min)

When the route exceeds the suppress limit, the route is dampened.Once the route is dampened, the router won't install the route in the routing table nor advertise it to other BGP neighbor.
If for example the penalty is 4000 and the half-life time is 15 minutes. After 15 minutes the penalty will be 2000, after another 15 minutes, the penalty is 1000, and after another 15 minute, the penalty is 500. Once the penalty is below the reuse limit of 750, the route can be used again and advertised to other BGP routers. When the penalty is below 50% of the reuse limit, the penalty is removed from the route.
The maximum suppress limit ensures that a route won't be dampened forever. The maximum suppress time is 3600 secs or 60 minutes by default.

RFL

Route Reflector Client (RFL); The route reflector allows all IBGP speakers within your autonomous network to learn about the available routes without introducing loops

RIB

Routing Information Base (RIB); Routing and routing functions in enterprise and carrier networks are typically performed by network devices (routers and switches) using an RIB. Protocols and configuration push data into the RIB and the RIB manager installs state into the hardware for packet forwarding.

RIP

RIP (Routing Information Protocol) sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers about the change. These updates are sent independently of the regularly scheduled updates that RIP routers send. RIP uses a hop count as a way to determine network distance. Each host with a router in the network uses the routing table information to determine the next host to route a packet for a specified destination.

RMON

Remote network monitoring (RMON) is the process of monitoring network traffic on a remote Ethernet segment for detectingnetwork issues such as dropped packets, network collisions, and traffic congestion

RP

Rendezvous point (RP)

RPF

RPF stands for Reverse Path Forwarding. PIM uses reverse-path forwarding (RPF) to prevent multicast routing loops by leveraging the unicast routing table on the virtual router. When the virtual router receives a multicast packet, it looks up the source of the multicast packet in its unicast routing table to see if the outgoing interface associated with that source IP address is the interface on which that packet arrived. If the interfaces match, the virtual router duplicates the packet and forwards it out the interfaces toward the multicast receivers in the group. If the interfaces don't match, the virtual router drops the packet. *This is called a RPF failure.*

RPT

Root Part Tree (RPT)

RRD

Route Redistribution (RRD)

RSVP

Resource Reservation Protocol (RSVP) is a transport layer protocol designed to reserve resources across a network using the integrated services model. RSVP operates over an IPv4 or IPv6 and provides receiver-initiated setup of resource reservations for multicast or unicast data flows.

RS-232

RS-232 is a short range connection between a single host and a single device (such as a PC to a modem) or another host (such as a PC to another PC). The standard uses a single TX line, a single RX line, numerous modem handshaking lines and a ground line with the option of DB9 and DB25 connectors. A minimal 3-wire RS-232 connection consists only the TX, RX, and ground lines, but if flow control is required a minimal 5-wire RS-232 is used adding the RTS and CTS lines. The RS-232

standard has been commonly used in computer serial ports and is still widely used in industrial communication devices.

RS-422

RS-422 was meant as a replacement for RS-232 as it offered much higher speeds, better immunity to noise and allow for longer cable lengths making it better suited to industrial environments. The standard uses the same signals as the RS-232 standard, but used differential twisted pair so requires double the number of wires as RS-232. Connectors are not specified in the standard so block or DB connectors are commonly used. RS-422 cannot implement a true multi-point communications network since there can be only one driver on each pair of wires. However, one driver can fan-out to up to ten receivers.

RS-485

RS-485 standard addresses some short coming of the RS-422 standard. The standard supports inexpensive local networks and multidrop communication links, using the same differential signalling over twisted pairs as RS-422. The main difference being that in RS-485 drivers use three-state logic allowing the individual transmitters to deactivate while not transmitting, while RS-422 the transmitter is always active therefore holding the differential lines. Up to 32 devices can be connected, but with repeaters a network with up to 256 devices can be achieved. RS-485 can be used in a full-duplex 4-wire mode or half-duplex 2-wire mode. With long wires and high baud-rates it is recommended that termination resistors are used at the far ends of the network for signal integrity

RST

RST stands for reset. RST is one of the TCP flags.
TCP flags are various types of flag bits present in the TCP header. Each of them has its own significance. They initiate connections, carry data, and tear down connections. The commonly used TCP flags are SYN, ACK, RST, FIN, URG, PSH.

- SYN (synchronize): Packets that are used to initiate a connection.
- ACK (acknowledgment): Packets that are used to confirm that the data packets have been received, also used to confirm the initiation request and tear down requests.
- RST (reset): Signify the connection is down or maybe the service is not accepting the requests.
- FIN (finish): Indicate that the connection is being torn down. Both the sender and receiver send the FIN packets to gracefully terminate the connection.
- PSH (push): Indicate that the incoming data should be passed on directly to the application instead of getting buffered.
- URG (urgent): Indicate that the data that the packet is carrying should be processed immediately by the TCP stack.

RSTP

Rapid Spanning-Tree Protocol

RT

Route Target (RT) value; RT can be used to share routes among them. We can apply route targets to a VRF to control the import and export of routes among it and other VRFs. When you configure RT import, it imports all prefixes that match the configured RT value as one of the attributes in the BGP update. So in any-any VRF, it is common to see all PE configured with same RT value

RTM

routing table manager (RTM). The RTM is the central repository of routing information for all routing protocols that operate under the routing and remote access service (RRAS). It provides routing information to all interested clients, such as routing protocols, management programs, and monitoring programs. The RTM also determines the best route to each destination network that is known to the routing protocols. The determination of this route is based on routing protocol priorities and on the metrics associated with the routes.

RTS

Request to Send (RTS)/CTS Flow Control is another flow control mechanism that is part of the RS232 standard.

RX

Receive

SA

Security Associations (SA). A SA is a relationship between two or more entities that describes how the entities will utilize security services to communicate securely. In endpoint-to-endpoint Transport Mode, both end points of the IP connection implement IPSec.

SAN

Singly attached nodes (SAN); singly attached nodes don't have the same redundancy as the doubly attached nodes since they still have just one connection that could fail.

SEM

State Event Machines (SEM)

SFP

SFP (Small Form-factor Pluggable) is a small transceiver that plugs into the SFP port of a network switch and connects to fibre channel and gigabit Ethernet (GbE) optical fiber cables at the other end. The SFP converts the serial electrical signals to serial optical signals and vice versa. SFP modules are hot swappable and contain ID and system information for the switch.

SFTP

SSH File Transfer Protocol (SFTP)

SHA

Secure Hash Algorithm is the name of a series of hash algorithms.
A hash function provides encryption using an algorithm and no key. A variable-length plaintext is “hashed” into a (typically) fixed-length hash value (often called a “message digest” or simply a “hash”). Hash functions are primarily used to provide integrity; the hash of a plaintext changes, the plaintext itself has changed.
Common older hash functions include Secure Hash Algorithm 1 (SHA-1), which creates a 160-bit hash and Message Digest 5 (MD5), which creates a 128-bit hash.

SIP

Session Initiation Protocol (SIP) is mostly well known for establishing voice and video calls over the Internet. To initiate such sessions, SIP uses simple request and response messages. For example, the INVITE request message is used to invite a user to begin a session and ACK confirms the user has received the request. The response code 180 (Ringing) means the user is being alerted of the call and 200 (OK) indicates the request was successful. Once a session has been established, BYE is used to end the communication.

SISP

Switch Instance Shared Port (SISP)

SLA

Service-level agreements (SLA).

SLIP

Serial Line Internet Protocol (SLIP); SLIP is the predecessor protocol of Point-to-Point Protocol (PPP). SLIP does not provide authentication, is a static IP addressing assignment, and data is transferred in synchronous form.

SM

State Machine

SNAT

Static Network Address Translation (SAT, SNAT) performs one-to-one translation of internal IP addresses to external ones.

SNMP

Simple Network Management Protocol

SNTP

Simple Network Time Protocol (SNTP)

SPT

Shortest path tree (SPT) is used for multicast transmission of packets with the shortest path from sender to recipients.

SR

State Refresh (SR) message. For a given (S,G) tree, SR messages will be originated byall routers that use an interface directly connected to the source as the RPF interface for the source. Ref: IETF “State Refresh in PIM-DM”

SRM

State Refresh Message (SRM). For a given (S,G) tree, SRM will be originated byall routers that use an interface directly connected to the source as the RPF interface for the source. Ref: IETF “State Refresh in PIM-DM”

SSD

SSD (Solid State Drive) is an all-electronic, non-volatile random access storage drive.

SSH

(Secure SHell) is a security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs on all platforms. Also serving as a secure client/server connection for applications such as database access and email, SSH supports a variety of authentication methods.

SSL

Secure Sockets Layer

SSM

Source-Specific Multicast (SSM)

SST

Single Spanning Tree (SST); SST is formed in either of the following situations:

- A switch running STP or RSTP belongs to only one spanning tree.

- An MST region has only one switch.

STP

Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on bridges and switches. The specification for STP is IEEE 802.1D. The main purpose of STP is provide path redundancy while preventing undesirable loops in the network.

SVL

Shared VLAN Learning (SVL)

S-VLAN

Stacked VLAN (S-VLAN)

TAC

Taxonomy Access Control (TAC) allows the user administrator to control access to nodes indirectly by controlling which roles can access which categories.

TACACS

Terminal Access Controller Access-Control System

TAI

International Atomic Time (TAI); if the port is in the master state, the local clock is synchronized to an external source of time traceable to TAI (International Atomic Time) and UTC (Universal Coordinated Time) such as GPS (Global Positioning System) system.

TB

Token Bucket (TB). The TB algorithm is based on an analogy of a fixed capacity bucket into which tokens, normally representing a unit of bytes or a single packet of predetermined size, are added at a fixed rate. When a packet is to be checked for conformance to the defined limits, the bucket is inspected to see if it contains sufficient tokens at that time. If so, the appropriate number of tokens, e.g. equivalent to the length of the packet in bytes, are removed ("cashed in"), and the packet is passed, e.g., for transmission. The packet does not conform if there are insufficient tokens in the bucket, and the contents of the bucket are not changed.

TC

TC (Topology Change); once the Root Bridge is aware of a change in the topology of the network, it sets the Topology Change (TC) flag on the sent BPDs.

TCN

TCN (Topology Change Notification), a kind of BPDU, is sent by bridges towards the root bridge to notify changes in the topology, such as port up or port down.

TCP

Transmission Control Protocol

TCP-AO

TCP-AO MKT (Transmission Control Protocol Authentication Option). TCP-AO uses cryptographic algorithms to convert MKTs, which can be shared across connections, into unique traffic keys for each connection.

TCP-AO MKT

TCP-AO MKT (Transmission Control Protocol Authentication Option Master Key Tuple). TCP-AO uses cryptographic algorithms to convert MKTs, which can be shared across connections, into unique traffic keys for each connection.

TLS

Transport Layer Security (TLS), the successor of the now-deprecated Secure Sockets Layer (SSL), is a cryptographic protocol designed to provide communications security over a computer network.

TLV

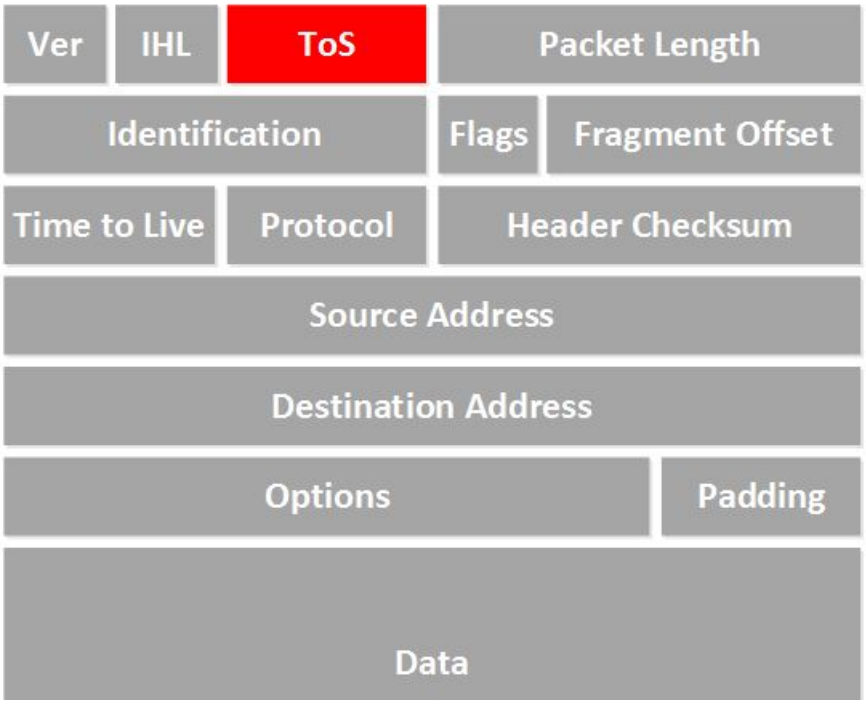
type, length, and value (TLV) traces

TN

Telnet (TN) is a networking protocol and software program used to access remote computers and terminals over the Internet or a TCP/IP computer network. Upon providing correct login and sign-in credentials, a user may access a remote system's privileged functionality. Telnet sends all messages in clear text and has no specific security mechanisms.

TOS

Type of Service (TOS). IP packets have a field called the Type of Service field (also known as the TOS byte).



TPID

Tag Protocol Identifier (TPID)

TTL

TTL (time to live). Under IP, TTL is an 8-bit field. In the IPv4 header, TTL is the 9th octet of 20. In the IPv6 header, it is the 8th octet of 40. The maximum TTL value is 255, the maximum value of a single octet. A recommended initial value is 64.

TX

Transmit

UAP

Uplink Access Port (UAP); when a tagged LLDP is enabled, the LLDP packets with destination address as 'nearest bridge address (01-80-c2-00-00-0E)' will be replicated for all S-Channels emulated over that UAP.

UART

UART (Universal Asynchronous Transmitter Receiver) is the most common protocol used for full-duplex serial communication.It is a single LSI (large scale integration) chip designed to perform asynchronous communication. This device sends and receives data from one system to another system.

UDP

User Datagram Protocol

UFD

Uplink failure detection (UFD)

URM

Unified Route Map (URM)

USM

USM stands for User based Security Model; USM (User based Security Model) and VACM (View-based Access Control Model) are the main features added as a part of the SNMPv3 specification. USM provides both encryption and authentication of the SNMP PDUs, while VACM specifies a mechanism for defining access policies for different users with different MIB trees.

UTC

Coordinated Universal Time (UTC); If the port is in the master state, the local clock is synchronized to an external source of time traceable to TAI (International Atomic Time) and UTC (Universal Coordinated Time) such as GPS (Global Positioning System) system.

UTP

Unshielded Twisted Pair (UTP) is a pair of wires that are twisted around each other to minimize interference. Ethernet cables are common example of UTP wires.

UUID

A Universally Unique IDentifier (UUID) is a 128-bit domain UUID unique to a MRP domain/ring. All MRP instances belonging to the same ring must have the same domain ID.

VACM

VACM stands for View-based Access Control Model); USM (User based Security Model) and VACM (View-based Access Control Model) are the main features added as a part of the SNMPv3 specification. USM provides both encryption and authentication of the SNMP PDUs, while VACM specifies a mechanism for defining access policies for different users with different MIB trees.

Varbind

A Variable Binding (Varbind) represents a set of Oid/Value pairs. Individual Variable Bindings are stored in the Vb class. Individual Variable Bindings are stored in the Vb class.
Create a variable binding and add the Object identifier in string format:
Vb vb = new Vb("1.3.6.1.2.1.1.1.0")
Create a variable binding and add the Object identifier in Oid format:
Oid oid = new Oid("1.3.6.1.2.1.1.1.0");
Vb vb = new Vb(oid);

VFI

Virtual Forwarding Interface (VFI)

VID

Management VLAN ID (VID)

VINES

Virtual Integrated Network Service (VINES)

VLAN

Virtual Local Area Network (VLAN) is a logical subgroup within a local area network that is created via software rather than manually moving cables in the wiring closet.

VPN

Virtual Private Network (*VPN*)

VRF

Virtual Routing and Forwarding (VRF). In IP-based computer networks, VRF is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time. One or more logical or physical interfaces may have a VRF and these VRFs do not share routes; therefore, the packets are only forwarded between interfaces on the same VRF. VRFs are the TCP/IP layer 3 equivalent of a VLAN. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other.

VRRP

VRRP (Virtual Router Redundancy Protocol) is an election protocol that dynamically assigns responsibility for one or more virtual router(s) to the VRRP router(s) on a LAN, allowing several routers on a multi-access link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP setup, one router is elected as the virtual router master, and the other routers are acting as backups in case of the failure of the virtual router master. VRRP is designed to eliminate the single point of failure inherent in the static default routed environment

VSA

Vendor Specific Attribute (VSA)

WAN

A wide area network is a telecommunications network that extends over a large geographic area for the primary purpose of computer networking.

Web UI

Web User Interface (Web UI) is a control panel in a device presented to the user via the Web browser. Network devices such as gateways, routers, and switches typically have such control panel that is accessed by entering the IP address of the device into a Web browser in a computer on the same local network.

WRED

WRED (Weighted Random Early Detection) is a queueing discipline for a network scheduler suited for congestion avoidance. It is an extension to random early detection (RED) where a single queue may have several different sets of queue thresholds.

WRR

Weighted Round Robin (WRR) is one of the scheduling algorithms used by the device. In WRR, there is a number of queues and to every queue is assigned weight (*w*). In a classical WRR, the scheduler cycles over the queues, and when a queue with weight *w* is visited, the scheduler can send consequently a burst of up *to w* packets. This works well for packets with the same size.

XNS

Xerox Network Systems (XNS)

Contents

Copyright Notice i

End User License Agreement (EULA) ii

Chapter: 1 Introduction 1

Scope 1
CLI Document Convention 1
Keyboard Conventions and Shortcuts 2

Chapter: 2 Command Line Interface 3

Context-Sensitive Help 3
CLI Command Modes 4
User Exec Mode 6
Privileged Exec Mode 6
Global Configuration Mode 6
Interface Configuration Mode 6
Port Channel Interface Configuration 7
VLAN Interface Configuration Mode 7
UFD Configuration Mode 7
Privilege Levels and Command Access 7
Configuration Terminal Access 12
Stopping Long Running Commands 12

Chapter: 3 System Commands 14

help 14
Parameters 14
Mode 14
Examples 14
clear screen 15
Mode 15
configure terminal 15

Mode 15
Examples 15
listuser 16
Mode 16
Examples 16
lock 16
Mode 16
Examples 16
username 16
Parameters 18
Mode 19
Prerequisites 19
Examples 19
enable password 19
Parameters 20
Mode 20
Prerequisites 20
Examples 20
alias 20
Parameters 21
Mode 21
Examples 21
access-list 21
Parameters 22
Mode 22
Examples 23
exec-timeout 23
Parameters 23
Mode 23
Default 23
Examples 23
logout 24
Mode 24
Examples 24
end 24
Mode 24
Examples 24
exit 25
Mode 25
Examples 25
enableuser 25
Parameters 25
Mode 25
Examples 25
clear line vty 26
Parameters 26

Mode 26
Examples 26
password 26
Parameters 27
Mode 27
Examples 28
set minimum password length 28
Parameters 28
Mode 28
Examples 28
set cli pagination 28
Parameters 29
Mode 29
Examples 29
set banner-name 29
Parameters 30
Mode 30
Examples 30
set prompt-name 30
Parameters 30
Mode 30
Examples 30
factory reset 31
Parameters 31
Mode 31
Examples 31
show privilege 31
Mode 31
Examples 32
show line 32
Parameters 32
Mode 32
Examples 32
show aliases 33
Mode 33
Examples 33
show history 33
Mode 33
Examples 33
show eula 34
Mode 34
Examples 34
set cli-console access 34
Parameters 34
Mode 34
Examples 35

Related Commands 35
set mgmt-port access 35
Parameters 35
Mode 35
Examples 35
Related Commands 35
set external-storage access 35
Parameters 36
Mode 36
Examples 36
Related Commands 36

Chapter: 4 System Features 37

ip address 37
Parameters 38
Mode 41
Default 41
Prerequisites 41
Examples 41
switchport 42
Mode 42
Default 42
Prerequisites 42
Examples 42
default ip address allocation protocol 42
Parameters 43
Mode 43
Default 43
Prerequisites 43
Examples 43
ip http 43
Parameters 45
Mode 46
Default 46
Prerequisites 46
Examples 46
login authentication 47
Parameters 48
Mode 48
Default 48
Examples 48
set ip http 48
Parameters 49
Mode 49
Default 49
Examples 49

authorized-manager ip-source 49
Parameters 50
Mode 51
Default 51
Examples 52
mtu 52
Parameters 52
Mode 52
Default 52
Examples 52
loopback local 52
Mode 53
Examples 53
archive download-sw 53
Parameters 54
Mode 54
Prerequisites 54
Examples 54
interface 55
Parameters 56
Mode 57
Prerequisites 57
Examples 58
mac-addr 58
Mode 58
Default 58
Prerequisites 58
Examples 58
system 58
Parameters 59
Mode 59
Examples 59
snmp trap link-status 59
Mode 60
Default 60
Prerequisites 60
Examples 60
bridge port-type 60
Parameters 61
Mode 62
Default 62
Prerequisites 62
Examples 63
monitor session 63
Parameters 64
Mode 64

Examples 64
show monitor 64
Parameters 65
Mode 65
Examples 65
mirror cpu-port 66
Parameters 66
Mode 66
Examples 67
show cpu-mirroring 67
Mode 67
Examples 67
write 67
Parameters 68
Mode 68
Prerequisites 68
Examples 68
copy 69
Parameters 70
Mode 71
Prerequisites 71
Examples 71
set linkup-delay 71
Parameters 72
Mode 72
Prerequisites 72
Examples 72
linkup-delay 72
Parameters 73
Mode 73
Prerequisites 73
Examples 73
show linkup-delay 73
Parameters 74
Mode 74
Examples 74
firmware switch 74
Mode 74
Examples 75
firmware upgrade 75
Parameters 75
Mode 75
Prerequisites 76
Examples 76
clock set 76
Parameters 77

Mode 77
Examples 77
erase 78
Parameters 78
Mode 78
Examples 78
cli console 78
Mode 78
Default 79
Examples 79
flowcontrol 79
Parameters 80
Mode 80
Prerequisites 80
Default 80
Examples 80
shutdown 81
Mode 81
Prerequisites 81
Default 81
Examples 81
debug interface 81
Parameters 83
Mode 83
Examples 84
debug-logging 84
Parameters 84
Mode 84
Default 84
Examples 84
rollback 85
Parameters 85
Mode 85
Default 85
Examples 85
shutdown 85
Parameters 86
Mode 86
Prerequisites 86
Examples 87
start 87
Parameters 87
Mode 87
Examples 87
set switch 87
Parameters 89

Mode 90
Default 90
Examples 90
hostname 91
Parameters 91
Mode 91
Examples 91
set designated-uplink 91
Parameters 92
Mode 92
Prerequisites 92
Examples 92
mac-learn-rate 93
Parameters 94
Mode 94
Default 94
Examples 94
ports 95
Parameters 95
Mode 95
Prerequisites 96
Examples 96
set port-role 96
Parameters 96
Mode 96
Examples 96
clear interfaces 96
Parameters 97
Mode 97
Examples 97
clear counters 98
Parameters 98
Mode 98
Examples 99
show ip interface 99
Parameters 100
Mode 100
Examples 100
show authorized-managers 101
Parameters 101
Mode 101
Examples 101
show interfaces 101
Parameters 103
Mode 105
Examples 105

show system-specific port-id 107
Mode 107
Examples 107
set custom-param 107
Parameters 108
Mode 108
Default 108
Examples 108
show custom-param 108
Mode 109
Examples 109
show env 109
Parameters 110
Mode 110
Examples 110
show system 111
Parameters 111
Mode 111
Examples 111
show flow-control 113
Parameters 113
Mode 113
Examples 114
show debug-logging 114
Parameters 114
Mode 114
Examples 114
show debugging 114
Mode 115
Examples 115
show clock 115
Mode 115
Examples 115
show running-config 115
Mode 115
Examples 115
show health status 119
Mode 119
Examples 119
show mac-learn-rate 119
Mode 120
Examples 120
set timer speed 120
Parameters 120
Mode 120
Examples 120

audit-logging . . . 120
Parameters . . . 121
Mode . . . 121
Examples . . . 121
Remote Logging Example . . . 122
Disabling Audit-Logging . . . 122
Seeing all available local files including current . . . 122
Seeing content of the local file . . . 123
Viewing the audit logging configuration . . . 123
show audit-logging . . . 123
Parameters . . . 124
Mode . . . 124
Examples . . . 124
shutdown ufd . . . 124
Mode . . . 124
Examples . . . 125
set ufd . . . 125
Parameters . . . 125
Mode . . . 125
Examples . . . 125
ufd group . . . 125
Parameters . . . 126
Mode . . . 126
Examples . . . 126
internal-lan . . . 126
Parameters . . . 127
Mode . . . 127
Prerequisites . . . 127
Examples . . . 127
show internal-lan . . . 127
Parameters . . . 128
Mode . . . 128
Prerequisites . . . 128
Examples . . . 128
show iftype protocol deny table . . . 128
Parameters . . . 128
Mode . . . 128
Prerequisites . . . 129
Examples . . . 129
login block-for . . . 129
Parameters . . . 129
Mode . . . 129
Defaults . . . 130
Examples . . . 130
show ufd . . . 130
Parameters . . . 130

Mode . . . 130
Examples . . . 130
feature telnet . . . 131
Mode . . . 131
Default . . . 131
Examples . . . 131
show telnet server . . . 131
Mode . . . 131
Examples . . . 131
set http . . . 132
Parameters . . . 132
Mode . . . 132
Default . . . 132
Examples . . . 132
show http . . . 133
Parameters . . . 133
Mode . . . 133
Examples . . . 133
http redirect . . . 134
Parameters . . . 134
Mode . . . 134
Default . . . 134
Examples . . . 135
set split-horizon . . . 135
Parameters . . . 135
Mode . . . 135
Prerequisites . . . 135
Examples . . . 135
shutdown split-horizon . . . 135
Mode . . . 136
Examples . . . 136
show split-horizon . . . 136
Parameters . . . 136
Mode . . . 136
Examples . . . 137
speed . . . 137
Parameters . . . 137
Mode . . . 137
Prerequisites . . . 137
Examples . . . 138
port-type providerInstancePort . . . 138
Parameters . . . 138
Mode . . . 138
Prerequisites . . . 138
Examples . . . 138
sleep . . . 138

Parameters . . . 139
Mode . . . 139
Examples . . . 139
rate-limit pause . . . 139
Parameters . . . 139
Mode . . . 139
Examples . . . 139
cpu controlled learning . . . 140
Mode . . . 140
Examples . . . 140
traffic-separation control . . . 140
Parameters . . . 141
Mode . . . 141
Examples . . . 141
mdix auto . . . 141
Mode . . . 142
Default . . . 142
Examples . . . 142
set port . . . 142
Parameters . . . 142
Mode . . . 142
Examples . . . 143
config-restore . . . 143
Parameters . . . 143
Mode . . . 143
Default . . . 143
Examples . . . 143
set mgmt-port routing . . . 144
Parameters . . . 144
Mode . . . 144
Default . . . 144
Examples . . . 144
set switch-name . . . 144
Parameters . . . 145
Mode . . . 145
Examples . . . 145
packet . . . 145
Parameters . . . 146
Mode . . . 146
Examples . . . 147
show packet . . . 147
Parameters . . . 147
Mode . . . 147
Examples . . . 147
alias . . . 148
Parameters . . . 148

Mode . . . 148
Examples . . . 148
port-security-state . . . 148
Parameters . . . 149
Mode . . . 149
Default . . . 149
Examples . . . 149
default-value save . . . 149
Parameters . . . 149
Mode . . . 149
Default . . . 150
Examples . . . 150
set mirroring . . . 150
Parameters . . . 150
Mode . . . 150
Examples . . . 150
default exec-timeout . . . 150
Parameters . . . 151
Mode . . . 151
Examples . . . 151
port . . . 151
Parameters . . . 152
Mode . . . 152
Examples . . . 152
web-session timeout . . . 152
Parameters . . . 153
Mode . . . 153
Prerequisites . . . 153
Examples . . . 153
clear http server statistics . . . 153
Mode . . . 153
Examples . . . 153
show web-session timeout . . . 153
Mode . . . 154
Examples . . . 154
show config-restore status . . . 154
Mode . . . 154
Default . . . 154
Examples . . . 154
clear protocol counters . . . 155
Parameters . . . 155
Mode . . . 155
Examples . . . 155
dump core-file . . . 155
Mode . . . 155
Examples . . . 156

dump 156
Parameters 156
Mode 156
Examples 157
debug iss 157
Parameters 158
Mode 158
Examples 158
show nvram 158
Mode 159
Examples 159
debug np module 160
Parameters 160
Mode 162
Examples 162
description 162
Parameters 163
Mode 163
Examples 163
counters 163
Parameters 163
Mode 163
Examples 164
show l3vlan interfaces counters 164
Parameters 164
Mode 164
Examples 165
set entity physical-index 165
Parameters 166
Mode 166
Default 166
Prerequisites 167
Examples 167
show entity 167
Parameters 168
Mode 168
Examples 168
gratuitous arp 170
Parameters 170
Mode 170
Example: Enabling Gratuitous ARP 170
Example: Disabling Gratuitous ARP 171
show grat-arp 171
Parameters 172
Mode 172
Example: Show Gratuitous ARP 172

Chapter: 5 **RADIUS 174**
radius-server host 174
Parameters 175
Mode 176
Default 176
Prerequisites 176
Examples 176
set radius 176
Parameters 177
Mode 177
Examples 177
show radius 177
Parameters 178
Mode 178
Prerequisites 178
Examples 178
debug radius 178
Parameters 179
Mode 179
Default 179
Examples 179

Chapter: 6 **TACACS 180**
tacacs-server 180
Parameters 181
Mode 182
Default 182
Prerequisites 182
Examples 182
show tacacs 183
Mode 183
Prerequisites 183
Examples 183
debug tacacs 184
Parameters 185
Mode 185
Default 185
Examples 185

Chapter: 7 **SSH 186**
ssh 186
Parameters 187
Mode 187
Default 187
Examples 187

show ssh 187
Mode 187
Examples 188
show ssh-configurations 188
Mode 188
Examples 188
show ip ssh 188
Mode 188
Examples 188
ip ssh 189
Parameters 190
Mode 190
Default 190
Examples 190
ip ssh pubkey-chain 191
Mode 191
Examples 191
debug ssh 191
Parameters 192
Mode 192
Default 192
Examples 192

Chapter: 8 SSL 193

show ssl server-cert 193
Mode 193
Examples 193
show ip http 194
Mode 195
Examples 195
ip http 195
Parameters 196
Mode 197
Default 197
Prerequisites 197
Examples 197
crypto pki keygen 198
Parameters 198
Mode 198
Examples 199
Related Commands 199
crypto pki csrgen 199
Parameters 199
Mode 199
Examples 200
crypto pki import 200

Parameters . . . 200
Mode . . . 200
Examples . . . 201
ip http secure crypto key . . . 201
Parameters . . . 201
Mode . . . 201
Examples . . . 202
no crypto pki . . . 202
show crypto PKI . . . 203
Parameters . . . 203
Mode . . . 203
Examples . . . 203

Chapter: 9 SNTP . . . 205

sntp . . . 205
Mode . . . 205
Examples . . . 205
set sntp . . . 205
Parameters . . . 207
Mode . . . 212
Examples . . . 212
show sntp . . . 213
Parameters . . . 214
Mode . . . 214
Examples . . . 214
debug sntp . . . 215
Parameters . . . 216
Mode . . . 216
Default . . . 216
Examples . . . 216

Chapter: 10 PTP . . . 217

ptp . . . 217
Mode . . . 218
Parameters . . . 219
Examples . . . 220
ptp (interfaces) . . . 221
Mode . . . 221
Parameters . . . 221
Examples . . . 221
show ptp . . . 221
Parameters . . . 222
Mode . . . 222
Examples . . . 222
debug ptp . . . 224

Parameters 224
Mode 224
Default 224
Examples 224

Chapter: 11 SNMPv3 225

SNMP Traps 225
Introduction 225
General SNMP configuration for TRAP Generation 225
Line Module Trap 226
Warm Start 227
Alarm Trap 228
Power Supply Trap 229
Cold Start Trap 230
Authentication Failure Trap 230
Link UP / DOWN Trap 231
Spanning Tree Trap 232
Temperature Trap 233
Port Security Traps 234
disable snmpagent 237
Parameters 237
Mode 237
Examples 237
enable snmpagent 237
Parameters 238
Mode 238
Default 238
Examples 238
show mib 238
Parameters 239
Mode 239
Examples 239
show snmp 239
Mode 239
Examples 239
show snmp-server 244
Mode 244
Examples 244
snmp 244
Parameters 247
Mode 258
Examples 259
snmpget mib 260
Parameters 260
Mode 260
Examples 260

snmpgetnext mib 260
Parameters 261
Mode 261
Examples 261
snmp-server 261
Parameters 262
Mode 262
Default 262
Examples 262
snmpset mib 263
Parameters 264
Mode 264
Examples 264
snmpwalk mib 264
Parameters 265
Mode 265
Examples 265

Chapter: 12 Syslog 266

Severity 266
Priority 267
Facility 267
Example of Valid Syslog Message 268
Factory Default Syslog Configuration Values 268
Logging Mechanisms Types and Default Configuration 268
Local Logging Mechanism 1 268
CLI Commands for Local Logging Method 1 269
Local Logging Mechanism 2 270
CLI Commands for Setting Flash Size and Threshold Limit 270
Logging to Flash Files CLI Commands 270
Flash Space Restriction Mechanisms 271
Warning Messages 271
Error Messages 272
USB Option for Copying Logs to External USB Flash Drive 272
CLI Command for Listing File Contents of Flash 273
Example configuration for Local (Flash) Logging 273
Remote Logging 273
Remote Logging Syslog CLI Command 274
Remote Logging Syslog Facility Level Configuration 275
Example 1 for Configuration for Remote Logging 275
Example 2 for Configuration for Remote Logging 276
Syslog List 276
logging 287
Parameters 289
Mode 291
Examples 291

syslog format . . . 291
Parameters . . . 291
Mode . . . 291
Examples . . . 291
secure logging crypto key . . . 292
Description . . . 292
Parameters . . . 292
Mode . . . 292
Examples . . . 292
Related Commands: . . . 292
mail-server . . . 293
Parameters . . . 294
Mode . . . 294
Examples . . . 294
sender . . . 295
Parameters . . . 295
Mode . . . 295
Default . . . 295
Prerequisites . . . 295
Examples . . . 295
cmdbuffs . . . 295
Parameters . . . 296
Mode . . . 296
Default . . . 296
Examples . . . 296
clear logs . . . 296
Mode . . . 296
Examples . . . 296
syslog . . . 297
Parameters . . . 298
Mode . . . 299
Examples . . . 299
show logging . . . 299
Mode . . . 299
Examples . . . 299
show flash logs . . . 300
Mode . . . 300
Examples . . . 300
show email alerts . . . 300
Mode . . . 300
Prerequisites . . . 301
Examples . . . 301
show syslog . . . 301
Parameters . . . 301
Mode . . . 301
Examples . . . 302

show logging-server . . . 302
Mode . . . 302
Examples . . . 303
show logging-file . . . 303
Mode . . . 303
Examples . . . 303
show mail-server . . . 303
Mode . . . 304
Examples . . . 304
smtp authentication . . . 304
Parameters . . . 305
Mode . . . 305
Examples . . . 305
logsize . . . 305
Parameters . . . 306
Mode . . . 306
Examples . . . 306

Chapter: 13 Serial . . . 307

CLI Serial Command Modes . . . 307
User Exec Mode . . . 309
Privileged Exec Mode . . . 309
Global Configuration Mode . . . 309
Serial Interface Configuration Mode . . . 309
Serial Profile Mode (Raw Socket) . . . 310
Serial Profile Mode (Preemptive-raw) . . . 310
Serial Profile Mode (UDP) . . . 310
Serial Profile Mode (TCP) . . . 311
Serial Profile Mode (Modbus) . . . 311
Transport Protocol TCP Mode . . . 311
Transport Protocol UDP Mode . . . 312
Direction (In) Mode (Raw) . . . 312
Direction (Out) Mode (Raw) . . . 312
Direction (IN-OUT) Mode (Raw) . . . 313
Role Mode (Modbus server) . . . 313
Role Mode (Modbus client) . . . 313
add slave-id . . . 313
Parameters . . . 314
add udp-host . . . 314
Parameters . . . 315
Mode . . . 315
Examples . . . 315
baud-rate . . . 315
Parameters . . . 316
Mode . . . 316
Examples . . . 316

clear serial config . . . 316
Parameters . . . 317
Mode . . . 317
Examples . . . 317
clear serial counters . . . 318
Parameters . . . 318
Mode . . . 318
Examples . . . 318
connection-map interface . . . 318
Parameters . . . 319
Mode . . . 319
Examples . . . 319
data-bits . . . 319
Parameters . . . 320
Mode . . . 320
Examples . . . 320
debug serial . . . 320
Parameters . . . 321
Mode . . . 321
Examples . . . 321
description . . . 321
Parameters . . . 322
Mode . . . 322
Examples . . . 322
direction . . . 322
Parameters . . . 322
Mode . . . 322
Examples . . . 323
DSCP . . . 323
Parameters . . . 324
Mode . . . 324
Examples . . . 324
dynamic idle-timeout . . . 324
Parameters . . . 325
Mode . . . 325
Examples . . . 325
dynamic packet timeout . . . 325
Prerequisites . . . 325
Parameters . . . 326
Mode . . . 326
Examples . . . 326
dynamic packet char . . . 326
Prerequisites . . . 326
Parameters . . . 327
Mode . . . 327
Examples . . . 327

flow-control . . . 327
Parameters . . . 328
Mode . . . 328
Examples . . . 328
force half-duplex . . . 328
Parameters . . . 329
Mode . . . 329
Examples . . . 329
forward-exception . . . 329
Parameters . . . 330
Mode . . . 330
Examples . . . 330
hold-time . . . 330
Parameters . . . 331
Mode . . . 331
Examples . . . 331
interface serial . . . 331
Parameters . . . 331
Mode . . . 331
Examples . . . 332
keep-alive . . . 333
Parameters . . . 333
Mode . . . 333
Examples . . . 334
local client port . . . 334
Parameters . . . 335
Mode . . . 335
Examples . . . 335
local server . . . 335
Parameters . . . 336
Mode . . . 336
Examples . . . 336
loopback local . . . 337
Mode . . . 337
Examples . . . 337
max client connections . . . 337
Parameters . . . 338
Mode . . . 338
Examples . . . 338
max connections . . . 338
Parameters . . . 338
Mode . . . 338
Examples . . . 339
max pending messages . . . 339
Parameters . . . 339
Mode . . . 339

Examples . . . 339
max udp connections . . . 340
Parameters . . . 340
Mode . . . 340
Examples . . . 340
mtu . . . 340
Parameters . . . 341
Mode . . . 341
Examples . . . 341
packet char . . . 341
Prerequisites . . . 341
Parameters . . . 342
Mode . . . 342
Examples . . . 342
packet size . . . 343
Prerequisites . . . 343
Parameters . . . 343
Mode . . . 343
Examples . . . 343
packet timeout . . . 344
Prerequisites . . . 344
Parameters . . . 344
Mode . . . 344
Examples . . . 344
packetizing . . . 345
Parameters . . . 346
Mode . . . 346
Examples . . . 346
parity . . . 346
Parameters . . . 347
Mode . . . 347
Examples . . . 347
permanent-client . . . 347
Parameters . . . 348
Mode . . . 348
Examples . . . 348
post-tx delay . . . 348
Parameters . . . 348
Mode . . . 348
Examples . . . 349
re-connect timeout . . . 349
Parameters . . . 349
Mode . . . 349
Examples . . . 349
remote ipv4 address . . . 350
Parameters . . . 351

Mode . . . 351
Examples . . . 351
remove slave-id . . . 352
Parameters . . . 352
Mode . . . 352
Examples . . . 352
remove udp-host . . . 353
Parameters . . . 353
Mode . . . 353
Examples . . . 353
response-timeout . . . 354
Parameters . . . 354
Mode . . . 354
Examples . . . 355
role . . . 355
Parameters . . . 355
Mode . . . 355
Examples . . . 355
rx-to-tx delay . . . 356
Parameters . . . 356
Mode . . . 356
Examples . . . 356
serial connection-type . . . 356
Parameters . . . 357
Mode . . . 357
Examples . . . 357
show interfaces serial . . . 357
Parameters . . . 358
Mode . . . 358
Examples . . . 358
show serial profile . . . 358
Parameters . . . 359
Mode . . . 359
Examples . . . 359
shutdown . . . 361
Mode . . . 362
Examples . . . 362
stop-bits . . . 362
Parameters . . . 362
Mode . . . 362
Examples . . . 362
tcp buffering . . . 363
Parameters . . . 363
Mode . . . 363
Examples . . . 363
transmit-exception . . . 364

Parameters . . . 364
Mode . . . 364
Examples . . . 364
transport protocol . . . 364
Parameters . . . 365
Mode . . . 365
Examples . . . 365
turnaround delay . . . 365
Parameters . . . 366
Mode . . . 366
Examples . . . 366

Chapter: 14 TCP . . . 367

tcp max retries . . . 367
Parameters . . . 367
Mode . . . 367
Examples . . . 367
show tcp . . . 368
Parameters . . . 368
Mode . . . 368
Examples . . . 368

Chapter: 15 UDP . . . 372

show udp . . . 372
Parameters . . . 372
Mode . . . 372
Examples . . . 372

Chapter: 16 STP . . . 374

clear spanning-tree detected protocols . . . 375
Parameters . . . 375
Mode . . . 375
Examples . . . 375
clear spanning-tree . . . 376
Parameters . . . 377
Mode . . . 377
Prerequisites . . . 377
Examples . . . 378
debug customer spanning-tree . . . 378
Parameters . . . 379
Mode . . . 381
Prerequisites . . . 381
Default . . . 381
Examples . . . 381
debug spanning-tree . . . 381

Parameters . . . 383
Mode . . . 385
Default . . . 385
Examples . . . 385
errordisable . . . 385
Parameters . . . 385
Mode . . . 385
Examples . . . 385
instance . . . 386
Parameters . . . 386
Mode . . . 386
Examples . . . 386
name . . . 387
Parameters . . . 387
Mode . . . 387
Examples . . . 387
revision . . . 387
Parameters . . . 388
Mode . . . 388
Examples . . . 388
set performance-data . . . 388
Parameters . . . 388
Mode . . . 388
Examples . . . 389
set performance-data-status . . . 389
Parameters . . . 389
Mode . . . 389
Examples . . . 389
show spanning-tree . . . 389
Parameters . . . 391
Mode . . . 398
Examples . . . 398
shutdown spanning-tree . . . 406
Mode . . . 406
Default . . . 406
Examples . . . 406
spanning-tree . . . 406
Parameters . . . 408
Mode . . . 413
Examples . . . 413
spanning-tree . . . 414
Parameters . . . 416
Mode . . . 421
Examples . . . 421

Chapter: 17 MRP CLI Commands . . . 423

Redundancy 423
Media Redundancy Protocol 424
MRP Function 424
Normal Operation: (Ring Closed) 425
Failure Detection: (Ring Open) 425
Alarms supported in MRP 426
MRP status changed: 427
MRM condition/detected 427
mrp 428
Parameters 428
Mode 428
Examples 428
mrp ringid 428
Parameters 429
Mode 429
Examples 429
mrp vid 429
Parameters 430
Mode 430
Examples 430
mode 430
Parameters 431
Mode 431
Examples 431
priority 431
Parameters 432
Mode 432
Examples 432
uuid 432
Parameters 432
Mode 432
Examples 432
show mrp 433
Parameters 433
Mode 433
Definitions of Errors 433
Examples 433

Chapter: 18 LA 435

channel-group 435
Parameters 436
Mode 436
Prerequisites 436
Examples 436
channel-protocol 436
Parameters 437

Mode . . . 437
Default . . . 437
Examples . . . 437
channel-protocol . . . 437
Parameters . . . 438
Mode . . . 438
Default . . . 438
Examples . . . 438
debug etherchannel . . . 438
Parameters . . . 439
Mode . . . 439
Examples . . . 439
debug lacp . . . 439
Parameters . . . 440
Mode . . . 440
Default . . . 440
Examples . . . 440
default port . . . 440
Parameters . . . 441
Mode . . . 441
Prerequisites . . . 441
Examples . . . 442
defaulted-state-threshold . . . 442
Parameters . . . 442
Mode . . . 442
Examples . . . 442
hw-failure recovery-threshold . . . 442
Parameters . . . 443
Mode . . . 443
Examples . . . 443
lacp admin-key . . . 443
Parameters . . . 444
Mode . . . 444
Prerequisites . . . 444
Examples . . . 444
lacp port-identifier . . . 444
Parameters . . . 445
Mode . . . 445
Prerequisites . . . 445
Examples . . . 445
lacp port-priority . . . 445
Parameters . . . 446
Mode . . . 446
Prerequisites . . . 446
Examples . . . 446
lacp rate . . . 446

Parameters . . . 447
Mode . . . 447
Prerequisites . . . 447
Examples . . . 447
lacp system-identifier . . . 447
Parameters . . . 448
Mode . . . 448
Prerequisites . . . 448
Examples . . . 448
lacp system-priority . . . 448
Parameters . . . 449
Mode . . . 449
Prerequisites . . . 449
Examples . . . 449
lacp timeout . . . 449
Parameters . . . 450
Mode . . . 450
Prerequisites . . . 450
Examples . . . 450
lacp wait-time . . . 450
Parameters . . . 451
Mode . . . 451
Prerequisites . . . 451
Examples . . . 451
port-channel max-ports . . . 451
Parameters . . . 452
Mode . . . 452
Prerequisites . . . 452
Examples . . . 452
port-channel . . . 452
Parameters . . . 454
Mode . . . 457
Default . . . 457
Prerequisites . . . 457
Examples . . . 457
same-state recovery-threshold . . . 457
Parameters . . . 458
Mode . . . 458
Examples . . . 458
set port-channel . . . 458
Parameters . . . 458
Mode . . . 458
Examples . . . 459
show etherchannel . . . 459
Parameters . . . 460
Mode . . . 460

Prerequisites 461
Examples 461
show interfaces etherchannel 464
Parameters 465
Mode 465
Prerequisites 465
Examples 465
show lacp 467
Parameters 468
Mode 468
Prerequisites 468
Examples 468
shutdown port-channel 469
Mode 469
Default 469
Prerequisites 469
Examples 469

Chapter: 19 LLDP 470

clear lldp 471
Parameters 471
Mode 471
Prerequisites 471
Examples 471
debug lldp 471
Parameters 473
Mode 474
Prerequisites 474
Examples 474
lldp 475
Parameters 476
Mode 478
Examples 478
lldp 478
Parameters 480
Mode 483
Examples 483
set lldp 484
Parameters 485
Mode 485
Examples 485
set lldp-med 485
Parameters 486
Mode 486
Examples 486
show lldp 486

Parameters 487
Mode 490
Examples 490

Chapter: 20 PNAC 494

aaa authentication dot1x default 494
Parameters 495
Mode 495
Default 495
Examples 495
dot1x 495
Parameters 497
Mode 499
Default 499
Examples 499
dot1x 499
Parameters 501
Mode 502
Default 502
Examples 502
dot1x 502
Parameters 504
Mode 508
Examples 508
debug dot1x 509
Parameters 509
Mode 509
Default 510
Examples 510
show dot1x 510
Parameters 511
Mode 513
Default 513
Examples 513
set nas-id 514
Parameters 515
Mode 515
Default 515
Prerequisites 515
Examples 515

Chapter: 21 VLAN 516

base 516
Parameters 517
Mode 517

Default . . . 517
Prerequisites . . . 517
Examples . . . 517
clear garp counters . . . 517
Parameters . . . 518
Examples . . . 518
clear mac-address-table . . . 518
Parameters . . . 519
Mode . . . 520
Examples . . . 520
clear vlan statistics . . . 520
Parameters . . . 521
Mode . . . 521
Prerequisites . . . 521
Examples . . . 521
debug garp . . . 522
Parameters . . . 523
Mode . . . 524
Default . . . 524
Prerequisites . . . 524
Examples . . . 524
debug vlan . . . 524
Parameters . . . 526
Mode . . . 526
Default . . . 527
Prerequisites . . . 527
Examples . . . 527
forward-all . . . 527
Parameters . . . 528
Mode . . . 529
Default . . . 530
Prerequisites . . . 530
Examples . . . 530
forward-unregistered . . . 530
Parameters . . . 531
Mode . . . 533
Default . . . 533
Prerequisites . . . 533
Examples . . . 533
group restricted . . . 533
Parameters . . . 534
Mode . . . 534
Default . . . 534
Prerequisites . . . 534
Examples . . . 534
interface range . . . 534

Parameters . . . 535
Mode . . . 535
Default . . . 535
Prerequisites . . . 536
Examples . . . 536
mac-address-table . . . 536
Parameters . . . 537
Mode . . . 539
Default . . . 539
Prerequisites . . . 539
Examples . . . 540
mac-map . . . 540
Parameters . . . 541
Mode . . . 541
Default . . . 542
Prerequisites . . . 542
Examples . . . 542
map protocol . . . 542
Parameters . . . 543
Mode . . . 545
Default . . . 545
Prerequisites . . . 545
Examples . . . 545
map subnet . . . 545
Parameters . . . 546
Mode . . . 546
Default . . . 547
Prerequisites . . . 547
Examples . . . 547
name . . . 547
Mode . . . 547
Parameters . . . 548
Examples . . . 548
port . . . 548
Parameters . . . 549
Mode . . . 549
Prerequisites . . . 549
Examples . . . 550
ports . . . 550
Parameters . . . 551
Mode . . . 553
Default . . . 554
Prerequisites . . . 554
Examples . . . 554
port-security trap-syslog . . . 554
Parameters . . . 554

Examples . . . 554
Syslogs . . . 555
port-security violation . . . 555
Parameters . . . 555
Examples . . . 555
protocol-vlan . . . 556
Mode . . . 556
Default . . . 556
Prerequisites . . . 556
Examples . . . 556
set filtering-utility-criteria . . . 556
Parameters . . . 557
Mode . . . 557
Default . . . 557
Examples . . . 557
set garp timer . . . 557
Parameters . . . 559
Mode . . . 560
Default . . . 560
Prerequisites . . . 560
Examples . . . 560
set gmrp . . . 560
Parameters . . . 561
Mode . . . 561
Default . . . 561
Prerequisites . . . 561
Examples . . . 561
set gvrp . . . 561
Parameters . . . 562
Mode . . . 562
Default . . . 562
Prerequisites . . . 562
Examples . . . 562
set mac-learning . . . 562
Parameters . . . 563
Mode . . . 563
Default . . . 563
Examples . . . 563
set packet-reflection . . . 563
Parameters . . . 563
Mode . . . 563
Default . . . 563
Examples . . . 564
set port . . . 564
Parameters . . . 565
Mode . . . 567

Default . . . 567
Examples . . . 567
set sw-stats . . . 567
Parameters . . . 568
Mode . . . 568
Default . . . 568
Examples . . . 568
set unicast-mac learning . . . 568
Parameters . . . 569
Mode . . . 569
Default . . . 569
Prerequisites . . . 569
Examples . . . 569
set vlan traffic-classes . . . 569
Parameters . . . 570
Mode . . . 570
Default . . . 570
Prerequisites . . . 570
Examples . . . 570
show forward-all . . . 570
Parameters . . . 571
Mode . . . 571
Prerequisites . . . 571
Examples . . . 571
show forward-unregistered . . . 571
Parameters . . . 572
Mode . . . 572
Prerequisites . . . 572
Examples . . . 572
show garp timer . . . 572
Parameters . . . 573
Mode . . . 573
Prerequisites . . . 573
Examples . . . 574
show gmrp statistics . . . 574
Parameters . . . 574
Mode . . . 574
Examples . . . 575
show gvrp statistics . . . 575
Parameters . . . 576
Mode . . . 576
Examples . . . 576
show mac-address-table . . . 577
Parameters . . . 578
Mode . . . 582
Prerequisites . . . 582

Examples . . . 583
show port-security . . . 584
Parameters . . . 585
Mode . . . 585
Examples . . . 585
show unicast port-security . . . 586
Parameters . . . 587
Mode . . . 587
Examples . . . 588
show vlan . . . 588
Parameters . . . 589
Mode . . . 592
Prerequisites . . . 592
Examples . . . 592
shutdown garp . . . 600
Mode . . . 600
Default . . . 600
Prerequisites . . . 601
Examples . . . 601
shutdown vlan . . . 601
Mode . . . 601
Default . . . 601
Prerequisites . . . 601
Examples . . . 601
switchport . . . 601
Parameters . . . 603
Mode . . . 612
Examples . . . 612
Enabling Port Security . . . 612
MAC learning . . . 613
Unicast . . . 613
unicast-mac learning limit . . . 613
Parameters . . . 614
Mode . . . 614
Default . . . 614
Prerequisites . . . 614
Examples . . . 614
user-defined TPID . . . 614
Parameters . . . 615
Mode . . . 615
Default . . . 615
Prerequisites . . . 615
Examples . . . 615
vlan . . . 616
Parameters . . . 617
Mode . . . 619

Default 619
Prerequisites 619
Examples 619
vlan 619
Parameters 621
Mode 622
Examples 622
vlan 622
Parameters 624
Mode 625
Default 625
Prerequisites 625
Examples 626

Chapter: 22 IP 627

arp 628
Parameters 630
Mode 632
Prerequisites 632
Examples 632
clear ip arp 632
Mode 632
Examples 632
ip aggregate-route 632
Parameters 633
Mode 633
Default 633
Examples 633
ip arp max-retries 633
Parameters 634
Mode 634
Default 634
Examples 634
ip default-distance 634
Parameters 634
Mode 634
Default 634
Examples 635
ip default-ttl 635
Parameters 635
Mode 635
Default 635
Examples 635
ip directed-broadcast 635
Mode 636
Default 636

Examples . . . 636
ip echo-reply . . . 636
Mode . . . 636
Default . . . 636
Examples . . . 637
ip mask-reply . . . 637
Mode . . . 637
Default . . . 637
Examples . . . 637
ip path . . . 637
Parameters . . . 638
Mode . . . 638
Default . . . 638
Prerequisites . . . 638
Examples . . . 638
ip proxy-arp . . . 638
Mode . . . 639
Default . . . 639
Examples . . . 639
ip proxyarp-subnetoption . . . 639
Mode . . . 639
Default . . . 639
Examples . . . 640
ip rarp client . . . 640
Mode . . . 640
Default . . . 640
Prerequisites . . . 640
Examples . . . 640
ip redirects . . . 640
Mode . . . 641
Default . . . 641
Examples . . . 641
ip unreachables . . . 641
Mode . . . 641
Default . . . 641
Examples . . . 642
ipv4 enable . . . 642
Mode . . . 642
Default . . . 642
Examples . . . 642
maximum-paths . . . 642
Parameters . . . 643
Mode . . . 643
Default . . . 643
Examples . . . 643
ping . . . 643

Parameters . . . 644
Mode . . . 644
Default . . . 644
Examples . . . 645
show ip default-distance . . . 645
Mode . . . 645
Examples . . . 645
show ip proxy-arp . . . 645
Mode . . . 645
Examples . . . 646
traffic-share . . . 646
Mode . . . 646
Default . . . 646
Examples . . . 646
debug ip arp . . . 646
Parameters . . . 647
Mode . . . 647
Default . . . 647
Examples . . . 647
ip route . . . 648
Parameters . . . 649
Mode . . . 650
Prerequisites . . . 651
Examples . . . 651
ip routing . . . 651
Mode . . . 651
Default . . . 651
Examples . . . 651
show ip arp . . . 651
Parameters . . . 653
Mode . . . 654
Examples . . . 654
show ip information . . . 654
Mode . . . 654
Examples . . . 654
show ip pmtu . . . 655
Mode . . . 655
Examples . . . 655
show ip proxy-arp . . . 655
Mode . . . 655
Examples . . . 655
show ip rarp . . . 656
Mode . . . 656
Examples . . . 656
show ip route . . . 656
Parameters . . . 657

Mode . . . 657
Examples . . . 657
show ip traffic . . . 658
Parameters . . . 659
Mode . . . 660
Examples . . . 660
traceroute . . . 661
Parameters . . . 661
Mode . . . 661
Default . . . 661
Prerequisites . . . 661
Examples . . . 662

Chapter: 23 OSPF . . . 663

abr-type . . . 663
Parameters . . . 664
Mode . . . 664
Default . . . 664
Prerequisites . . . 664
Examples . . . 664
area . . . 664
Parameters . . . 666
Mode . . . 672
Examples . . . 673
ASBR Router . . . 673
Mode . . . 673
Examples . . . 673
bfd . . . 674
Parameters . . . 674
Mode . . . 674
Default . . . 675
Prerequisites . . . 675
Examples . . . 675
capability opaque . . . 675
Mode . . . 675
Default . . . 675
Examples . . . 675
compatible rfc1583 . . . 676
Mode . . . 676
Default . . . 676
Examples . . . 676
debug ip ospf . . . 676
Parameters . . . 677
Mode . . . 677
Examples . . . 677
disable bfd . . . 678

Mode . . . 678
Default . . . 678
Examples . . . 678
default-information . . . 678
Parameters . . . 679
Mode . . . 679
Default . . . 679
Examples . . . 679
distance . . . 680
Parameters . . . 680
Mode . . . 680
Default . . . 680
Prerequisites . . . 680
Examples . . . 680
distribute-list . . . 681
Parameters . . . 681
Mode . . . 681
Examples . . . 681
enable bfd . . . 681
Mode . . . 682
Default . . . 682
Examples . . . 682
ip ospf . . . 682
Parameters . . . 684
Mode . . . 690
Prerequisites . . . 690
Examples . . . 690
neighbor . . . 691
Parameters . . . 692
Mode . . . 692
Default . . . 692
Examples . . . 692
network . . . 693
Parameters . . . 694
Mode . . . 696
Prerequisites . . . 696
Examples . . . 696
nsf ietf . . . 696
Parameters . . . 698
Mode . . . 701
Default . . . 701
Prerequisites . . . 701
Examples . . . 701
passive-interface . . . 701
Parameters . . . 703
Mode . . . 704

Prerequisites . . . 704
Examples . . . 704
redist-config . . . 704
Parameters . . . 705
Mode . . . 705
Default . . . 706
Prerequisites . . . 706
Examples . . . 706
redistribute . . . 706
Parameters . . . 707
Mode . . . 708
Default . . . 708
Examples . . . 708
route-calculation . . . 708
Parameters . . . 709
Mode . . . 709
Default . . . 709
Prerequisites . . . 709
Examples . . . 709
router ospf . . . 709
Parameters . . . 710
Mode . . . 710
Examples . . . 710
router-id . . . 710
Parameters . . . 711
Mode . . . 711
Examples . . . 711
set nssa asbr-default-route . . . 711
Parameters . . . 712
Mode . . . 712
Default . . . 712
Examples . . . 712
show ip ospf . . . 712
Parameters . . . 714
Mode . . . 719
Examples . . . 719
summary-address . . . 723
Parameters . . . 724
Mode . . . 725
Default . . . 725
Examples . . . 725
timers spf . . . 725
Parameters . . . 726
Mode . . . 726
Default . . . 726
Examples . . . 726

Chapter: 24 **DHCP 727**
DHCP Client 727
DHCP Relay 727
DHCP Server 728
bootfile config-file 729
Parameters 729
Mode 729
Default 729
Examples 729
clear ip dhcp client statistics 729
Parameters 730
Mode 730
Examples 730
clear ip dhcp relay statistics 730
Mode 731
Examples 731
clear ip dhcp server statistics 731
Mode 731
Examples 731
debug ip dhcp 731
Parameters 733
Mode 734
Default 734
Examples 734
default-router 734
Parameters 735
Mode 735
Prerequisites 735
Examples 735
dns-server 735
Parameters 736
Mode 736
Prerequisites 736
Examples 736
domain-name 736
Parameters 737
Mode 737
Prerequisites 737
Examples 737
excluded-address 737
Parameters 738
Mode 738
Prerequisites 738
Examples 738
host hardware-type 738
Parameters 740

Mode . . . 741
Examples . . . 741
ip dhcp bootfile . . . 742
Parameters . . . 742
Mode . . . 742
Examples . . . 742
ip dhcp client . . . 742
Parameters . . . 744
Mode . . . 745
Prerequisites . . . 746
Examples . . . 746
ip dhcp client . . . 746
Parameters . . . 747
Mode . . . 747
Default . . . 747
Examples . . . 748
ip dhcp dns-server . . . 748
Parameters . . . 748
Mode . . . 748
Examples . . . 748
ip dhcp excluded-address . . . 749
Parameters . . . 749
Mode . . . 749
Prerequisites . . . 749
Examples . . . 750
ip dhcp next-server . . . 750
Parameters . . . 750
Mode . . . 750
Default . . . 750
Examples . . . 750
ip dhcp ntp-server . . . 750
Parameters . . . 751
Mode . . . 751
Examples . . . 751
ip dhcp option . . . 751
Parameters . . . 752
Mode . . . 752
Examples . . . 752
ip dhcp pool . . . 752
Parameters . . . 753
Mode . . . 753
Examples . . . 753
ip dhcp relay . . . 753
Parameters . . . 754
Mode . . . 754
Examples . . . 755

ip dhcp server 755
Parameters 755
Mode 755
Default 755
Prerequisites 756
Examples 756
ip dhcp sip-server 756
Parameters 756
Mode 756
Examples 757
ip dhcp snooping 757
Mode 757
Default 757
Examples 757
ip dhcp snooping trust 757
Mode 757
Default 758
Examples 758
ip dhcp snooping 758
Parameters 759
Mode 759
Default 759
Examples 759
lease 759
Parameters 760
Mode 760
Default 760
Prerequisites 760
Examples 760
netbios-name 761
Parameters 761
Mode 761
Prerequisites 761
Examples 761
netbios-node 762
Parameters 762
Mode 762
Prerequisites 762
Examples 763
netbios-node-type 763
Parameters 763
Mode 763
Prerequisites 764
Examples 764
network 764
Parameters 765

Mode . . . 765
Default . . . 765
Examples . . . 766
ntp-server . . . 766
Parameters . . . 766
Mode . . . 766
Examples . . . 766
option . . . 767
Parameters . . . 767
Mode . . . 767
Default . . . 767
Prerequisites . . . 768
Examples . . . 768
release dhcp . . . 768
Parameters . . . 769
Mode . . . 769
Prerequisites . . . 769
Examples . . . 769
renew dhcp . . . 769
Parameters . . . 770
Mode . . . 770
Prerequisites . . . 770
Examples . . . 771
service dhcp . . . 771
Mode . . . 771
Default . . . 771
Prerequisites . . . 771
Examples . . . 771
service dhcp-relay . . . 771
Mode . . . 772
Default . . . 772
Prerequisites . . . 772
Examples . . . 772
service dhcp-server . . . 772
Mode . . . 772
Default . . . 772
Prerequisites . . . 773
Examples . . . 773
set dhcp-client enable / disable . . . 773
Parameters . . . 773
Mode . . . 773
Examples . . . 773
show dhcp server . . . 773
Mode . . . 774
Examples . . . 774
show ip dhcp client . . . 774

Parameters . . . 774
Mode . . . 774
Examples . . . 775
show ip dhcp relay . . . 776
Parameters . . . 776
Mode . . . 776
Examples . . . 776
show ip dhcp server . . . 777
Parameters . . . 778
Mode . . . 778
Prerequisites . . . 778
Examples . . . 778
show ip dhcp snooping . . . 780
Parameters . . . 780
Mode . . . 780
Prerequisites . . . 781
Examples . . . 781
show dhcp-client module status . . . 781
Mode . . . 782
Examples . . . 782
sip-server . . . 782
Parameters . . . 782
Mode . . . 782
Examples . . . 783
utilization threshold . . . 783
Parameters . . . 783
Mode . . . 783
Default . . . 783
Prerequisites . . . 783
Examples . . . 783
vendor-specific . . . 784
Parameters . . . 784
Mode . . . 784
Examples . . . 784

Chapter: 25 RIP . . . 785

auto-summary . . . 785
Parameters . . . 786
Mode . . . 786
Prerequisites . . . 786
Examples . . . 786
debug ip rip . . . 786
Parameters . . . 787
Mode . . . 787
Prerequisites . . . 787
Examples . . . 787

default-information . . . 788
Parameters . . . 788
Mode . . . 788
Examples . . . 788
default-metric . . . 788
Parameters . . . 789
Mode . . . 789
Default . . . 789
Examples . . . 789
distance . . . 789
Parameters . . . 790
Mode . . . 790
Default . . . 790
Examples . . . 790
distribute-list . . . 790
Parameters . . . 791
Mode . . . 791
Prerequisites . . . 791
Examples . . . 791
ip rip . . . 791
Parameters . . . 793
Mode . . . 797
Prerequisites . . . 797
Examples . . . 797
ip rip . . . 798
Parameters . . . 799
Mode . . . 799
Examples . . . 799
ip split-horizon . . . 800
Parameters . . . 800
Mode . . . 800
Default . . . 800
Examples . . . 800
neighbor . . . 800
Parameters . . . 801
Mode . . . 801
Examples . . . 801
network . . . 801
Parameters . . . 802
Mode . . . 803
Examples . . . 803
output-delay . . . 803
Parameters . . . 804
Mode . . . 804
Default . . . 804
Examples . . . 804

passive-interface . . . 804
Parameters . . . 806
Mode . . . 807
Prerequisites . . . 807
Examples . . . 807
redistribute . . . 807
Parameters . . . 808
Mode . . . 808
Default . . . 808
Examples . . . 808
rip . . . 809
Parameters . . . 810
Mode . . . 810
Default . . . 810
Examples . . . 810
router rip . . . 810
Mode . . . 811
Default . . . 811
Examples . . . 811
show ip rip . . . 811
Parameters . . . 811
Mode . . . 811
Examples . . . 812
timers basic . . . 813
Parameters . . . 813
Mode . . . 813
Default . . . 814
Examples . . . 814
version . . . 814
Parameters . . . 814
Mode . . . 814
Default . . . 815
Prerequisites . . . 815
Examples . . . 815

Chapter: 26 BGP (Beta Version) . . . 816

address-family . . . 816
Parameters . . . 816
Mode . . . 816
Notes . . . 817
Examples . . . 817
aggregate-address . . . 817
Parameters . . . 818
Mode . . . 819
Notes . . . 819
Examples . . . 819

bgp 819
Parameters 822
Mode 834
Examples 834
clear bgp ipv6 835
Parameters 835
Mode 835
Examples 835
clear ip bgp 835
Parameters 837
Mode 837
Examples 838
debug ip bgp 838
Parameters 838
Mode 838
Examples 838
default-information 838
Parameters 839
Mode 839
Default 839
Examples 839
default-metric 839
Parameters 840
Mode 840
Default 840
Examples 840
distance 840
If Routemap is disabled 840
Parameters 841
Mode 841
Examples 841
distribute-list 841
Parameters 842
Mode 842
Examples 842
do shutdown ip bgp 842
Mode 842
Examples 842
ip bgp 843
Parameters 844
Mode 844
Default 844
Examples 845
label-allocation-mode 845
Parameters 845
Mode 845

Examples . . . 845
maximum-paths . . . 845
Parameters . . . 846
Default . . . 846
Note . . . 846
Mode . . . 846
Examples . . . 846
neighbor . . . 846
Parameters . . . 848
Mode . . . 856
Examples . . . 856
network . . . 857
Parameters . . . 858
Mode . . . 858
Notes . . . 858
Examples . . . 858
redistribute . . . 858
Parameters . . . 860
Mode . . . 860
Default . . . 860
Notes . . . 861
Examples . . . 861
restart-reason . . . 861
Parameters . . . 861
Mode . . . 861
Examples . . . 862
restart-support . . . 862
Parameters . . . 862
Mode . . . 862
Examples . . . 862
router bgp . . . 862
Parameters . . . 863
Mode . . . 863
Default . . . 863
Note . . . 863
Examples . . . 863
show bgp-version . . . 863
Mode . . . 864
Examples . . . 864
show ip bgp . . . 864
Mode . . . 865
Examples . . . 865
synchronization . . . 865
Mode . . . 865
Default . . . 865
Note . . . 866

Examples 866
tcp-ao mkt key-id 866
Parameters 867
Default 867
Mode 867
Examples 867

Chapter: 27 IGMP Snooping 868

debug ip igmp snooping 868
Parameters 869
Mode 870
Prerequisites 870
Examples 870
ip igmp snooping 870
Parameters 871
Mode 872
Default 872
Prerequisites 872
Examples 873
ip igmp snooping 873
Parameters 875
Mode 879
Examples 879
ip igmp snooping 880
Parameters 882
Mode 888
Examples 888
ip igmp 888
Parameters 889
Mode 889
Examples 889
ip igmp snooping clear counters 889
Parameters 890
Mode 890
Examples 890
mvr 890
Mode 891
Default 891
Examples 891
show ip igmp snooping 891
Parameters 893
Mode 897
Examples 897
shutdown snooping 901
Mode 901
Default 901

Prerequisites . . . 901
Examples . . . 901
snooping leave-process . . . 902
Parameters . . . 902
Mode . . . 902
Default . . . 902
Examples . . . 902
snooping report-process . . . 903
Parameters . . . 903
Mode . . . 903
Default . . . 903
Examples . . . 903

Chapter: 28 RMON . . . 904

rmon alarm . . . 904
Parameters . . . 905
Mode . . . 906
Default . . . 906
Prerequisites . . . 906
Examples . . . 906
rmon collection . . . 906
Parameters . . . 908
Mode . . . 908
Examples . . . 909
rmon event . . . 909
Parameters . . . 910
Mode . . . 910
Examples . . . 910
set rmon . . . 910
Parameters . . . 911
Mode . . . 911
Default . . . 911
Examples . . . 911
show rmon . . . 911
Parameters . . . 912
Mode . . . 912
Examples . . . 912

Chapter: 29 QoS . . . 916

class-map . . . 916
Parameters . . . 916
Mode . . . 916
Prerequisites . . . 917
Examples . . . 917
clear meter-stats . . . 917

Parameters . . . 917
Mode . . . 917
Prerequisites . . . 917
Examples . . . 917
debug qos . . . 918
Parameters . . . 918
Mode . . . 918
Examples . . . 918
map . . . 918
Parameters . . . 920
Mode . . . 921
Prerequisites . . . 921
Examples . . . 921
match access-group . . . 921
Parameters . . . 922
Mode . . . 922
Examples . . . 922
meter . . . 922
Parameters . . . 923
Mode . . . 923
Prerequisites . . . 923
Examples . . . 923
meter-type . . . 923
Parameters . . . 924
Mode . . . 924
Prerequisites . . . 925
Examples . . . 925
mls qos . . . 925
Parameters . . . 926
Mode . . . 926
Examples . . . 926
policy-map . . . 926
Parameters . . . 927
Mode . . . 927
Prerequisites . . . 927
Examples . . . 927
priority-map . . . 927
Parameters . . . 928
Mode . . . 928
Prerequisites . . . 928
Examples . . . 928
qos pbit-preference . . . 928
Parameters . . . 928
Mode . . . 928
Default . . . 929
Examples . . . 929

qos 929
Parameters 929
Mode 929
Default 929
Prerequisites 929
Examples 929
queue 930
Parameters 931
Mode 932
Prerequisites 932
Examples 932
queue-map 932
Parameters 933
Mode 933
Prerequisites 933
Examples 933
scheduler 933
Parameters 934
Mode 934
Examples 934
set class 934
Parameters 935
Mode 935
Examples 935
set meter 935
Parameters 937
Mode 941
Defaults 941
Prerequisites 941
Examples 941
set meter-stats 941
Parameters 942
Mode 942
Prerequisites 942
Examples 942
set policy 942
Parameters 943
Mode 944
Prerequisites 944
Examples 944
shape-template 944
Parameters 945
Mode 945
Examples 945
show class-map 945
Parameters 946

Mode 946
Examples 946
show meter 946
Parameters 947
Mode 947
Examples 947
show policy-map 948
Parameters 948
Mode 948
Examples 948
show qos 949
Parameters 950
Mode 951
Examples 951
show queue 953
Parameters 953
Mode 953
Examples 954
show queue-map 954
Parameters 955
Mode 955
Examples 955
show queue-template 956
Parameters 956
Mode 956
Examples 956
show scheduler 956
Parameters 957
Mode 957
Examples 957
show shape-template 957
Parameters 958
Mode 958
Examples 958

Chapter: 30 ACL 959

deny 959
Parameters 961
Mode 964
Default 964
Examples 965
deny 965
Parameters 966
Mode 968
Default 968
Examples 968

deny . . . 968
Parameters . . . 969
Mode . . . 969
Default . . . 970
Examples . . . 970
deny icmp . . . 970
Parameters . . . 971
Mode . . . 975
Default . . . 975
Examples . . . 975
deny tcp . . . 975
Parameters . . . 977
Mode . . . 980
Default . . . 980
Examples . . . 980
deny udp . . . 981
Parameters . . . 982
Mode . . . 985
Default . . . 985
Examples . . . 985
egress access-list . . . 985
Parameters . . . 986
Mode . . . 986
Default . . . 986
Examples . . . 986
ip access-group . . . 986
Parameters . . . 987
Mode . . . 987
Prerequisites . . . 987
Examples . . . 987
ip access-list . . . 987
Parameters . . . 988
Mode . . . 988
Examples . . . 988
mac access-group . . . 988
Parameters . . . 989
Mode . . . 989
Prerequisites . . . 989
Examples . . . 989
mac access-list . . . 989
Parameters . . . 990
Mode . . . 990
Examples . . . 990
permit . . . 990
Parameters . . . 992
Mode . . . 995

Default . . . 995
Examples . . . 996
permit . . . 996
Parameters . . . 997
Mode . . . 1002
Default . . . 1002
Examples . . . 1002
permit . . . 1002
Parameters . . . 1003
Mode . . . 1005
Default . . . 1005
Examples . . . 1005
permit icmp . . . 1005
Parameters . . . 1007
Mode . . . 1011
Default . . . 1011
Examples . . . 1011
permit tcp . . . 1012
Parameters . . . 1013
Mode . . . 1017
Default . . . 1017
Examples . . . 1018
permit udp . . . 1018
Parameters . . . 1020
Mode . . . 1024
Default . . . 1024
Examples . . . 1025
rate-limit . . . 1025
Parameters . . . 1026
Mode . . . 1026
Default . . . 1026
Examples . . . 1026
show access-lists . . . 1026
Parameters . . . 1027
Mode . . . 1027
Examples . . . 1027
show egress access-list mode . . . 1030
Mode . . . 1031
Examples . . . 1031
show interfaces rate-limit . . . 1031
Mode . . . 1031
Examples . . . 1031
show interfaces storm-control . . . 1031
Mode . . . 1032
Examples . . . 1032
storm-control . . . 1032

Parameters . . . 1033
Mode . . . 1033
Default . . . 1033
Prerequisites . . . 1033
Examples . . . 1033

Chapter: 31 VRRP . . . 1034

VRRP Definitions . . . 1034
Definitions . . . 1035
Reference . . . 1035
auth-deprecate . . . 1036
Parameters . . . 1036
Mode . . . 1036
Examples . . . 1036
interface . . . 1036
Parameters . . . 1037
Mode . . . 1037
Examples . . . 1037
router vrrp . . . 1037
Mode . . . 1037
Examples . . . 1038
track . . . 1038
Link-track and IP-track . . . 1038
Parameters . . . 1039
Mode . . . 1039
Examples . . . 1039
vrrp . . . 1040
Parameters . . . 1041
Mode . . . 1043
Examples . . . 1043
vrrp version . . . 1043
Parameters . . . 1044
Mode . . . 1044
Default . . . 1044
Examples . . . 1044
ip-tracking . . . 1044
Parameters . . . 1045
Mode . . . 1045
Prerequisites . . . 1046
Examples . . . 1046
show running vrrp . . . 1046
Mode . . . 1046
Examples . . . 1046
show track . . . 1047
Mode . . . 1047
Examples . . . 1047

show vrrp 1047
Parameters 1048
Mode 1048
Examples 1048

Chapter: 32 Alarms 1051

Example 1052
Alarm events covered – First phase 1052
Relay and LED for Alarms 1052
set alarm 1054
Parameters 1054
Mode 1054
Default 1054
Examples 1054
alarm buffered 1054
Parameters 1055
Mode 1055
Default 1055
Examples 1055
alarm config-type 1055
Parameters 1056
Mode 1056
Default 1056
Examples 1056
show active alarms 1056
Mode 1057
Examples 1057
show alarm history 1057
Parameters 1058
Mode 1058
Default 1058
Examples 1058
show alarm supported 1059
Parameters 1060
Mode 1060
Examples 1060

Chapter: 33 PoE 1062

set poe 1062
Parameters 1062
Mode 1062
Examples 1062
show power 1063
Parameters 1063
Mode 1063

Examples - Power Counters 1064
Example - Power Counters, single interface 1064
Example - Power Detail 1065
Example - Power Inline 1065
Example - Power Inline, single interface 1065
show poe state 1066
Parameters 1066
Mode 1066
Examples 1066
power inline 1066
Parameters 1067
Mode 1067
Examples 1067
power inline (interface) 1067
Parameters 1068
Mode 1068
Examples 1068

Chapter: 34 HSR-PRP 1070

redundancy 1070
Parameters 1070
Mode 1070
Examples 1071
redundancy 1071
Parameters 1071
Mode 1071
Examples 1071
mode 1071
Parameters 1072
Mode 1072
Examples 1072
hsr-operational-mode 1072
Parameters 1073
Mode 1073
Examples 1073
default 1073
Mode 1074
Examples 1074
no shutdown 1074
Mode 1074
Examples 1074
shutdown 1074
Mode 1074
Examples 1075
proxy-expire-time 1075
Parameters 1075

Mode . . . 1075
Examples . . . 1075
supervisory-expire-time . . . 1075
Parameters . . . 1076
Mode . . . 1076
Examples . . . 1076
port . . . 1076
Parameters . . . 1076
Mode . . . 1076
Examples . . . 1077
debug hst-prp . . . 1077
Parameters . . . 1077
Mode . . . 1077
Examples . . . 1077
clear counters redundant . . . 1077
Parameters . . . 1078
Mode . . . 1078
Examples . . . 1078
clear interfaces redundant . . . 1078
Parameters . . . 1078
Mode . . . 1078
Examples . . . 1079
show interfaces counters redundant . . . 1079
Parameters . . . 1079
Mode . . . 1079
Examples . . . 1079
show redundancy . . . 1079
Parameters . . . 1080
Mode . . . 1080
Examples . . . 1080

Chapter: 35 NAT . . . 1081

set ip nat . . . 1081
Parameters . . . 1082
Mode . . . 1082
Examples . . . 1082
ip nat . . . 1082
Parameters . . . 1084
Mode . . . 1085
Examples . . . 1085
clear ip connections . . . 1086
Parameters . . . 1086
Mode . . . 1086
Examples . . . 1086
clear ip nat rules . . . 1087
Mode . . . 1087

Examples 1087
show ip nat 1087
Parameters 1088
Mode 1089
Examples 1089
debug nat 1090
Parameters 1090
Mode 1090
Examples 1090

Chapter: 36 firewall 1091
Parameters 1091
Mode 1091
Examples 1091
enable 1091
Parameters 1091
Mode 1091
Examples 1092
disable 1092
Parameters 1092
Mode 1092
Examples 1092
access-group 1092
Parameters 1093
Mode 1093
Examples 1093
ip route 1094
Parameters 1095
Mode 1096
Prerequisites 1097
Examples 1097
clear screen 1097
Parameters 1097
Mode 1097
Examples 1097
help 1097
Parameters 1098
Mode 1098
Examples 1098
debug firewall 1098
Parameters 1098
Mode 1099
Examples 1099
show running-config firewall 1099
Parameters 1099
Mode 1099

Examples . . . 1099
Example of Firewall Configuration . . . 1100
Example . . . 1100
Static Route Requirements . . . 1100
rule . . . 1101
Parameters . . . 1102
Mode . . . 1103
Examples . . . 1103

Chapter: 37 VPN . . . 1104

How IPSec Works . . . 1104
ACK Packets . . . 1105
VPN Global Configuration . . . 1105
set vpn . . . 1105
Parameters . . . 1105
Mode . . . 1105
Examples . . . 1106
set tunnel . . . 1106
Parameters . . . 1106
Mode . . . 1106
Examples . . . 1106
crypto map . . . 1106
Parameters . . . 1107
Mode . . . 1107
Examples . . . 1107
wizard vpn . . . 1107
Parameters . . . 1107
Mode . . . 1107
Examples . . . 1107
show crypto . . . 1109
Parameters . . . 1109
Mode . . . 1109
Examples . . . 1109
IKE Phase 1 . . . 1110
Encryption Algorithms . . . 1111
Diffie and Hellman Key Exchange . . . 1111
Exchange Mode . . . 1112
IKE Phase 2 . . . 1113
IPSec Local and Peer End Points Configuration . . . 1114
isakmp local identity . . . 1114
Parameters . . . 1114
Mode . . . 1114
Examples . . . 1114
isakmp peer identity . . . 1115
Parameters . . . 1115
Mode . . . 1115

Examples 1115
IPSec Policy Configuration 1116
set ike version 1116
Parameters 1116
Mode 1116
Examples 1116
crypto policy encryption 1116
Parameters 1118
Mode 1119
Examples 1119
crypto key 1119
Parameters 1120
Mode 1121
Examples 1121
crypto map ipsec 1121
Parameters 1122
Mode 1122
Examples 1122
crypto ipsec mode 1123
Parameters 1123
Mode 1123
Examples 1123
access-list 1123
Parameters 1124
Mode 1124
Examples 1124
debug crypto ipsec level 1124
Parameters 1125
Mode 1126
Examples 1126
set ipv6 peer 1126
Parameters 1126
Mode 1126
Examples 1126
set local 1126
Parameters 1126
Mode 1126
Examples 1127
set peer 1127
Parameters 1127
Mode 1127
Examples 1127
copy crypto-pki 1127
Parameters 1128
Mode 1128
Examples 1128

show crypto ipsec secrets 1129
Parameters 1130
Mode 1130
Examples 1130
GRE 1130
tunnel mode 1130
Parameters 1131
Mode 1131
Examples 1131
CLI for Displaying Logs 1131
show file 1132
Parameters 1132
Mode 1132
Examples 1132
copy flash log file_name 1132
Parameters 1133
Mode 1133
Examples 1133

Index i

Introduction

1. Introduction

This document is designed to provide users with the web pages' information required to configure the switch through the *CLI*. All CLI configurations and statistics related pages are illustrated with field descriptions and additional information to help the end user.

This document is designed to provide users with the information required to configure the product through the *CLI*. All configurations and statistics related pages are illustrated with field descriptions and additional information to help the end user.

1.1. Scope

This document explains in detail all web screens and fields for the *CLI*.

This document explains in detail all commands and fields for the *CLI*. It does not include the details of the *HTTP* server architecture, backend processing of web screens, or the protocol details.

Convention	Usage	DESCRIPTION
Font as shown	Syntax of the *CLI* command	`configure terminal`

1.2. CLI Document Convention

This section describes the CLI document convention.

CLI commands presentation will follow this *CLI* Document Convention. To provide a consistent user experience, this *CLI* document convention adhere to the Industry Standard *CLI* syntax. The font & format is also updated to show DITA / Structured Framemaker 2019 layout.

Convention	Usage	DESCRIPTION
Font as shown	Syntax of the CLI command	`configure terminal`
< >	Parameter inside the brackets < > indicate the Input fields of syntax	`<integer (100-1000)>`

Convention	Usage	DESCRIPTION
[ ]	Parameter inside [ ] indicate optional fields of syntax	`show split-horizon [all]`
{ }	Grouping parameters in the syntax	`ip address <ip-address> [secondary {node0 | node1}]`
|	Separating grouped parameters in the syntax	`set http authentication-scheme {default| basic| digest}`

Font & format as shown	Example & CLI command outputs	iS5comm# show split-horizon interface 1
		`Ingress Port VlanId StorageType Egress List`
		`========== ====== ========== ==========`
		`Gi0/1 - Volatile Gi0/2,Gi0/3,Gi0/6`

Note	Notes	**NOTE:** All commands are case-sensitive

1.3. Keyboard Conventions and Shortcuts

Keyboard shortcuts are shown in this section.

Some Keyboard Conventions and Shortcuts are as shown below:

- **Up Arrow / Down Arrow**—displays the previously executed command.
- **Backspace / Ctrl + H**—removes a single character.
- **TAB**—completes a command without typing the full word.
- **Alt + V**—pastes content.
- **Alt + C**—copies content.
- **Left Arrow / Right Arrow**—traverses the current line.
- **q**—aborts long running text output.

Command Line Interface

2. Command Line Interface

This chapter explains how to access Command Line Interface (*CLI*) for Raptor and elaborates on the different *CLI* command modes. It also gives guidelines on context sensitive help.

The *CLI* can be used to configure switch from a console terminal connected to the serial port of the switch or from a remote terminal using TELNET.

The *CLI* supports a simple login authentication mechanism. The authentication is based on a username and password provided by the user during login. The user "admin" is created by default with password "admin".

NOTE: A new user can be created, or an existing user can be deleted, and the own password or password of the other users can be modified, only if login as a admin.

When login process is started, the username and password have to be given at the login prompt to access the *CLI* shell:

```
iS5Com Login: admin

Password: admin

iS5com
```

The Privileged Exec is now available for the user. The next section provides a detailed description of the various modes available for the switch.

CLI commands are also case sensitive.

CLI commands will be successful only if the dependencies are satisfied for a particular command that is issued. The general dependency is that the module specific commands are available only when the respective module is ‘enabled’ or they are used only in the suitable mode. Appropriate error messages will be displayed if the dependencies are not satisfied.

2.1. Context-Sensitive Help

The switch’s *CLI* framework offers context-sensitive help. The user can type a question mark (?) anytime during a session to get help. The help can be invoked in several ways. It is not displayed as a whole and is available only for the specific token from where it is invoked

Examples of possible scenarios are given below.

When a user types a character followed immediately by a question mark (?), this displays the current possible tokens without a help string.

iS5comm(config)# service?

```
dhcp            related configuration
dhcp-relay      DHCP relay related configuration
dhcp-server     DHCP server related configuration
```

Some of the basic concepts implemented for context-sensitive help are:

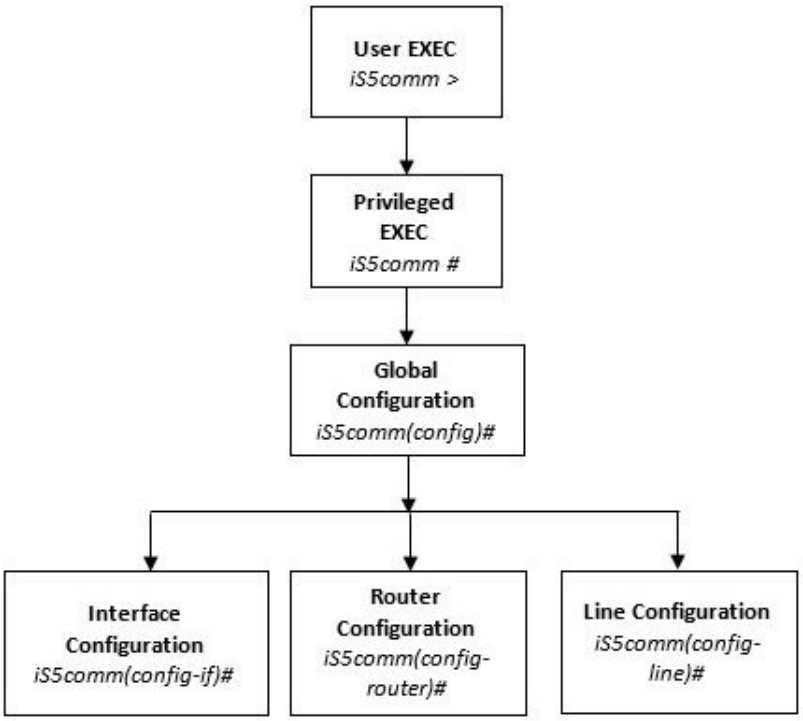
- The next possible tokens are listed only in the lexical order and not in the order as available in the syntax or command structure.
- All possible tokens are listed along with the help string, even though the command is ambiguous. Any ambiguous command and value range errors are taken care only during the execution of the command.
- The help tokens provided within <> brackets denote that the user should input values of specified format. For example, <string(32)> represents that the user should input a string of size varying from 1 to 32.
- The help tokens provided within () brackets denotes that the user should input only the values represented. For example, (1-4094) represents that the user should input value within the mentioned range alone.
- The format is directly provided as help token for some non-keyword such as IP address, IP mask, MAC address and so on. For example, aa:aa:aa:aa:aa:aa represents that a MAC address of this Format should be provided.
- Only the most commonly used format is provided as help token for some non-keywords such as IPv6 address. But the command supports most of the valid formats. For example, AAAA::BBBB represents the IPv6 address, but the command will accept the format AAAA:B::BBBB.
- The help token <CR> along with help string explaining the operation of the command is displayed if the command can be executed at that point (errors are handled only during the execution).

2.2. CLI Command Modes

Depending on the *CLI* mode, iS5comm prompt will be specific. This cannot be changed by the end user. For example, when the command mode is Global Configuration, the prompt display will be `iS5comm(config)#`.

The Hierarchical structure of the command modes is shown below. See them on the figure below.

Figure 1: CLI Command Modes


User EXEC
iS5comm >
Privileged EXEC
iS5comm #
Global Configuration
iS5comm(config)#
Interface Configuration
iS5comm(config-if)#
Router Configuration
iS5comm(config-router)#
Line Configuration
iS5comm(config-line)#

User Exec Mode

Prompt	Access method	Exit Method
iS5comm>	This is the initial mode to start a session.	logout

Privileged Exec Mode

Prompt	Access method	Exit Method
iS5comm#	The User EXEC mode command enable is used to enter the Privileged EXEC Mode	To return from the Privileged EXEC mode to User EXEC mode, the command disable is used.

Global Configuration Mode

Prompt	Access method	Exit Method
iS5comm(config)#	The Privileged EXEC mode command configure terminal is used to enter the Global Configuration Mode.	To return from the Global Configuration Mode to Privileged Mode, the command exit is used.

Interface Configuration Mode

Prompt	Access method	Exit Method
iS5comm(config-if)#	The Global Configuration mode command interface <interface-type><interface-id> is used to enter the Interface Configuration Mode.	To return from the Interface Configuration mode to Global Configuration Mode, the command exit is used. To exit from the Interface Configuration mode to Privileged EXEC Mode, the command end is used.

Port Channel Interface Configuration

Prompt	Access method	Exit Method
`iS5comm(config-if)#`	The Global Configuration mode command `interface port <port channel-id>` is used to enter the Port Channel Interface Configuration Mode.	To return from the Port Channel Interface Configuration mode to Global Configuration Mode, the command `exit` is used. To exit from the Port Channel Interface Configuration mode to Privileged EXEC Mode, the command `end` is used.

VLAN Interface Configuration Mode

Prompt	Access method	Exit Method
`iS5comm(config-if)#`	The Global Configuration mode command `interface vlan <vlan id>` is used to enter the Port Channel Interface Configuration Mode.	To return from the VLAN Interface Configuration mode to Global Configuration Mode, the command `exit` is used. To exit from the VLAN Interface Configuration mode to Privileged EXEC Mode, the command `end` is used.

UFD Configuration Mode

Prompt	Access method	Exit Method
`iS5comm(config-if)#`	The Global Configuration mode command `ufd group <group-id (1-65535)>` is used to enter the UFD Interface Configuration Mode.	To return from the UFD Configuration mode to Global Configuration Mode, the command `exit` is used. To exit from the UFD Configuration mode to Privileged EXEC Mode, the command `end` is used.

Privilege Levels and Command Access

The following table will list out the commands available for the different user levels in Privileged and User Exec levels.

Command	First Param	Guest	Tech	Admin	Description
archive	download-sw		x	x	Downloads software image

Command	First Param	Guest	Tech	Admin	Description
clear					Clears the specified parameters
	alarm	x	x	x	Alarm related information
	au-message	x	x	x	Address update messages related information
	cfa	x	x	x	CFA module related information
	interfaces	x	x	x	Protocol specific configuration of the interface
	meter-stats	x	x	x	Specific configuration for meter
	poe	x	x	x	PoE related configuration
	screen	x	x	x	Screen information
	ip		x	x	IP related configuration
	line		x	x	Configures line information
	logs		x	x	Log information
	protocol		x	x	Clears the specified protocol counters
	spanning-tree		x	x	Spanning tree related configuration
	tcp		x	x	TCP related configuration
clock	set		x	x	Sets the system clock value
config-restore					Configures the restore option
	flash		x	x	File in flash to be used for restoration
	norestore		x	x	No configuration restore
	remote		x	x	Remote location configuration
configure	terminal		x	x	Configures the terminal
copy			x	x	Various copy options
debug					Configures trace for the protocol
	ip	x	x	x	IP related configuration
	show	x	x	x	Show mempool status
	sntp	x	x	x	SNTP related configuration
	crypto		x	x	Crypto related information
	cybsec		x	x	Cybsec related information

Command	First Param	Guest	Tech	Admin	Description
	dot1x		x	x	PNAC related configuration
	etherchannel		x	x	Etherchannel related information
	firewall		x	x	Firewall related configuration
	garp		x	x	GARP related configuration
	interface		x	x	Configures trace for the interface management
	lacp		x	x	LACP related configuration
	lldp		x	x	LLDP related configuration
	lns		x	x	LCD notification server
	nat		x	x	Network Address Translation related configuration
	np		x	x	NPAPI configuration
	ptp		x	x	Precision time protocol related configuration
	qos		x	x	QOS related configuration
	security		x	x	Security related configuration
	spanning-tree		x	x	Spanning tree related protocol configuration
	ssh		x	x	SSH related configuration
	tacm		x	x	Transmission and admission control related configuration
	vlan		x	x	VLAN related configuration
display firewall rules				x	Display firewall rules
dot1x	clear	x	x	x	Clear dot1x configuration
	initialize		x	x	State machine and fresh authentication configuration
	re-authenticate		x	x	Re-authentication
dump					Display memory content from the given memory location

Command	First Param	Guest	Tech	Admin	Description
	mem		x	x	Dump memory
	que		x	x	Show the queue related information
	sem		x	x	Show the semaphore related information
	task		x	x	Show the task related information
egress bridge			x	x	
end			x	x	Exit to the privileged Exec (#) mode
erase			x	x	Clears the contents of the startup configuration
exit		x	x	x	Logout
factory reset				x	Reset to factory default configuration
factory reset	users			x	Reset all users on switch
firmware			x	x	Upgrades firmware
generate	tech		x	x	Generate the tech report of various system resources and protocol states for debugging
help		x	x	x	Displays help for commands
ip	igmp snooping clear counters	x	x	x	Clears the IGMP snooping statistics
	clear counters		x	x	Clear operation
	dhcp		x	x	DHCP related configuration
	pim		x	x	PIM related configuration
	ssh		x	x	SSH related information
listuser			x	x	List the user, mode and groups
lock			x	x	Lock the console
logout		x	x	x	Logout
memtrace			x	x	Configures memtrace
no ip					IP related information
	dhcp		x	x	DHCP related configuration
	ssh		x	x	SSH related information

Command	First Param	Guest	Tech	Admin	Description
no debug					Configures trace for the module
	ip	x	x	x	Stops debugging on IGMP or PIM
	sntp	x	x	x	Stops debugging on SNTP related configurations
	additional options...		x	x	Stops debugging for other options
ping					
	A.B.C.D	x	x	x	Ping host
	ip dns host name	x	x	x	Ping host
	ip A.B.C.D	x	x	x	Ping host
readarpfromHardware ip	A.B.C.D		x	x	Reads the arp for the given IP
readregister			x	x	Reads the value of the register from the hardware
release dhcp			x	x	Performs release operation
reload			x	x	Restarts the switch
renew dhcp			x	x	Performs renew operation
run script			x	x	Runs CLI commands
shell				x	Shell to Linux prompt
show		x	x	x	Shows configuration or information
sleep		x	x	x	Puts the command prompt to sleep
ssl				x	Configures secure sockets layer related parameters
snmpwalk mib					Allows the user to view Management Information Base related configuration.
	name	x	x	x	
	oid	x	x	x	
traceroute					Traces route to the destination IP
	A.B.C.D		x	x	

Command	First Param	Guest	Tech	Admin	Description
write			x	x	Writes the running-config to a flash file
writeregister			x	x	writes in the specified register

Configuration Terminal Access

The Guest user level does not have access to the configuration terminal.

The Administration level has access to all commands in the configuration terminal.

The Technical level has access to all commands in the configuration terminal with the following exceptions listed below.

- bridge-mode
- enableuser
- mst
- password
- traffic

2.3. Stopping Long Running Commands

Some *CLI* commands generate a long series of screen output. Typing ‘q’ will abort this text and quickly return the user to the command prompt.

This section will describe how to manage the text flow for commands that generate screens worth of text output. Examples will be provided using the **show running-config** command.

When a command generates more than one screen worth of text the user will be prompted to advance the screen when the following text appears **--More--**.

```
iS5comm# show running-config

#Building configuration...!!
syslog localstorage
syslog relay
syslog filename-one "is5"
logging local flash emergencies file is5
logging local flash alerts file is5
!
!
ip pim component 1
!
set gvrp disable
set gmrp disable
```

```
spanning-tree mode rst
interface gigabitethernet 0/1
!
interface gigabitethernet 0/2
!
interface gigabitethernet 0/3
!
interface gigabitethernet 0/4
--More--
```

In order to advance the text the user should hit the **spacebar**.

If the user would like to stop the text from scrolling and abort the output from the command then the user should type **q**.

Typing **q** will return the user to the prompt.

System Commands

3. System Commands

The System Commands are the commands used to manage access permissions, mode access, and terminal configuration.

3.1. help

To display a brief description for any given command, use the **help** command in the mode where command is used.

help

```
help [<command>]
```

Parameters

Parameter	Type	Description
<command>		Enter the name for the particular command for which help should be displayed. To display help description for commands with more than one word, do not provide any space between the words. The examples below show how help command is used in any of the modes.

Mode

Any Mode

Examples

iS5comm # help configure terminal

```
    EXEC commands :

    configure terminal
    [Desc]: Enter configuration mode.
```

iS5comm(config)# help interface

```
CONFIGURE commands :
interface range { <interface-type> <slot/port-port> | vlan <vlan-id
(1-4094)>- <vlan-id (1-4094)>}  [Desc]: Selects the range of L2 and IVR
interface to be configured  interface {mgmt0 | vlan <vlan-id/vfi-id>
[switch <switch-name>]| port-channel<port-channel-id (1-65535)> | tunnel
<tunnel-id (0-128)> | <interface-type> <interface-id> | linuxvlan
<interface-name> | loopback <interface-id (0-100)> | ppp<1-128> | pw
<interface-id (1-65535)> | ac <integer (1-65535)>| s-channel <integer
(1-65535)>}
[Desc]: Select an interface to configure.
```

iS5comm(config-crypto-map)# help setipv6peer

```
VPN commands :

set ipv6 peer <peer-ipv6 address>
[Desc]: This IPv6 address is the destination address in the packet
during authentication and encryption of outbound datagrams.
```

3.2. clear screen

To clear all contents from the screen, use the **clear screen** command in any mode.

clear screen

Mode

Any Mode

3.3. configure terminal

To enter Global Configuration Mode, use the **configure terminal** command in Privileged EXEC Mode.

configure terminal

Mode

Privileged EXEC Mode

Examples

iS5comm # configure terminal

iS5comm (config)#

3.4. listuser

listuser

Mode

Privileged EXEC Mode

Examples

iS5comm # listuser

USER	MODE	PRIVILEGE
root	/	16
admin	/	15
guest	/	1

3.5. lock

To lock the CLI console, use the **lock** command in Privileged EXEC Mode. The command allows the user/system administrator to lock the console to prevent unauthorized users from gaining access to the CLI command shell. Enter the login password to release the console lock and access the CLI command shell.

lock

Mode

Privileged EXEC Mode

Examples

iS5comm # lock

3.6. username

To create a user and sets the password and the privilege level for the user, use the **username** command in Global Configuration Mode. The no form of the command deletes the specified user.

username

```
username <user-name> [password [0 | 7 | LINE] <string(8-20)>] [privilege
<1-15>] [confirm-password [0 | 7 | LINE] <string(8-20)>] [status {enable |
disable}]
```

no username

```
no username <user-name>
```

Parameters

Parameter	Type	Description
<user-name>		Specify the login user name to be created
password		Specifies the password to be entered by the user to login to the system, and password encryption to be used. The size password entered must be a minimum of 8 and maximum of 20 characters containing at least one uppercase, one lowercase, one number and one special character. The password encryption options are as follows:
0	Integer	Uses the unencrypted password
7	Integer	Uses the hidden password
LINE		Uses the Line password; This feature is currently not supported
<string(8-20)>	integer	Specifies that the size of password entered must be a minimum of 8 and maximum of 20 characters
privilege <1-15>	integer	Applies restriction to the user for accessing the CLI commands. This values ranges between 1 and 15. For example, a user ID configured with privilege level as 4 can access only the commands having privilege ID lesser than or equal to 4
confirm-password		Specifies the password to be entered by the user to login to the system, and password encryption to be used. The size password entered must be a minimum of 8 and maximum of 20 characters containing at least one uppercase, one lowercase, one number and one special character. The password encryption options are as follows:
0	Integer	Uses the unencrypted password
7	Integer	Uses the hidden password
LINE		Uses the Line password; This feature is currently not supported
<string(8-20)>	integer	Specifies that the size of password entered must be a minimum of 8 and maximum of 20 characters
status		Specifies the status of the user name
enable		Enables the user name
status		Disables the user name

Mode

Global Configuration Mode

Prerequisites

- Only the root user can create new users using this command.
- When a new users are created, the user can login with any username and the respective password.
- Privilege ID is set as zero for all show commands and is set as 15 for all configuration commands, in the def files. Root users can access all commands and other users can access only the show commands. Users can change the privilege IDs of the commands in the def file to customize and segregate the commands as per the needs

Examples

iS5comm (config)# username products password Prod@1234 privilege 15

NOTE: The user products are created with the privilege level 15. Hence, the user will be visible to view all commands.

iS5comm (config)# username support password Supp@123 privilege 1

NOTE: The user support is created with the privilege level 1. Hence, the user will be visible to view only the below commands.

- Show - Show commands related to all features.
- Enable - Enables the privilege level.
- Disable - Disables the privilege level.
- Exit
- Logout
- Clear
- Debug
- No Debug

3.7. enable password

To enable privilege level for the password, use the command **enable password** in Global Configuration Mode. The no form of the command disables the password or privilege level for the password.

enable password

```
enable password level < 1 | 7 | 15 > <password (20)>
```

no enable password

```
no enable password level < 1 | 7 | 15 >
```

Parameters

Parameter	Type	Description
level		Specify level related configuration. There 3 predefined levels of privilege as shown by the parameters below:
1	Integer	Guest
7	Integer	Tech
15	Integer	Admin
<password(20)>	String	Specify the password to be enabled.The size of password entered must be a maximum of 20 characters. It should follow password configuration conventions. It should contain at least one uppercase, one lowercase, one number and one special character. Privilege level related configuration

Mode

Global Configuration Mode

Prerequisites

- Only the root user can enable the password for any other blocked user using this command
- This command allows the root user to enable a password for other users to access the commands in the specified privilege level. The other users can access commands in the privilege level using the password enabled for that level.

Examples

iS5comm (config)# enable password level 1 Ad@1231

3.8. alias

To replace a given token / command by a string, use the **alias** command in Global Configuration Mode. The no form of the command removes the alias created for the given string.

alias

```
alias {interface | configure} <alias-name> <token to be replaced> | token
```

no alias

```
no alias <alias-name>
```

Parameters

Parameter	Type	Description
interface		Enter for Interface Mode commands
configure		Enter for Global Mode commands
<alias-name>	String	Enter abbreviated/short form string to be used.
<token to be replaced>	String	Enter command for which alias name should be configured. <max 10 tokens>
token		Specify the token for which alias name should be configured.

Mode

Global ConfigurationMode

Examples

iS5comm(config)# alias int interface

iS5comm(config)# alias config ct configure terminal

iS5comm(config)# exit

iS5comm# show aliases

```
    ct -> configure terminal
    int -> interface
```

iS5comm(config)# exit

iS5comm(config)# no alias ct

iS5comm(config)# exitiS5comm# show aliases

```
    int -> interface
```

3.9. access-list

To create an IP access-list and specify packets to be forwarded depending on associated parameters, trigger provisioning of active filter rules to hardware based on configured priority, or configure the provision mode for the access list, use the command **access-list** in Global Configuration Mode. The no form of the command deletes the IP access-list with a specified access-list number.

access-list

```
access-list <access list> {permit | deny} {any | host <ucast_addr> |
A.B.C.D(<ucast_addr>) <ip_mask>} |
```

```
commit |
provision mode {consolidated | immediate}
```

no access-list

```
no access-list <access list>
```

Parameters

Parameter	Type	Description
<access list>		Enter an access list number- a number from 1 to 65535.
permit		Permits access if conditions are matched
deny		Deny access if conditions are matched
any		Enter to permit or deny packets from all addresses
host		Permits or denies packets from the source
<ucast_addr>	A.B.C.D	Enter unicast IP address of the source
A.B.C.D <ucast_addr>	A.B.C.D	Enter unicast IP address of the destination
<ip_mask>	A.B.C.D	Enter IP mask of the destination
commit		Specify to trigger provisioning of active filter rules to hardware based on configured priority. This command is applicable only when provision mode is consolidated. Traffic flow would be impacted when filter-rules are reprogrammed to hardware
provision mode		Enter to specify provisioning mode
consolidated		Enter to specify consolidated provisioning mode. When the provision mode is set to consolidated, the active filter rules are programmed to the hardware based on configured priority only when a commit trigger is issued.
immediate		Enter to specify immediate provisioning mode. In the immediate mode, the active filter rules are programmed immediately in the order of creation.

Mode

Global Configuration Mode

Examples

iS5comm(config)# access-list 2 permit any

iS5comm(config)# access-list provision mode consolidated

iS5comm(config)# access-list commit

iS5comm(config)# no access-list 2

3.10. exec-timeout

To set time (in seconds) for EXEC line disconnection with a value ranging from 1 to 18000 seconds, use the **exec-timeout** command in Line Configuration Mode. The no form of the command resets the EXEC timeout to its default value of 1800 seconds.

exec-timeout

```
exec-timeout <integer (1-18000)>
```

no exec-timeout

Parameters

Parameter	Type	Description
<integer (1-18000)>	Integer	Enter time (in seconds) for EXEC line disconnection. This value ranges from 1 to 18000 seconds.

Mode

Line Configuration Mode

Default

Integer - 18000 seconds

Examples

iS5comm# configure terminal

iS5comm(config)# line console

iS5comm(config-line)# exec-timeout 18000

iS5comm(config-line)# end

iS5comm#

3.11. logout

To exit from Privileged EXEC/ User EXEC mode to iS5Comm login prompt in case of console session, use the **logout** command in Privileged EXEC/ User EXEC Mode. In case of a Telnet session, this command terminates the session.

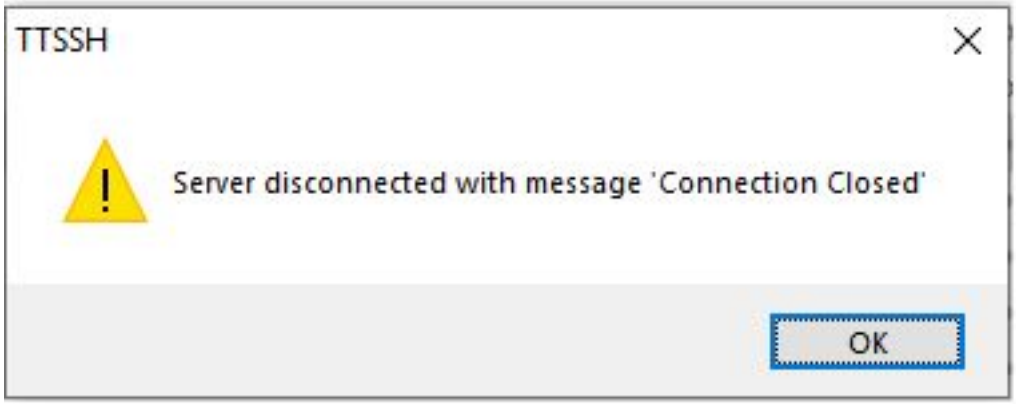
logout

Mode

Privileged EXEC/ User EXEC Mode

Examples

iS5comm # logout



iS5comm login:

3.12. end

To exit from the current mode to the Privileged EXEC mode, use the **end** command in all modes.

end

Mode

All modes

Examples

iS5comm(config-if)# end

iS5comm#:

iS5comm (config)# end

iS5comm#:

3.13. exit

To exit from the current mode and revert to the mode used prior to this mode, use the **exit** command in all modes.

exit

Mode

All modes

Examples

iS5comm(config-if)# exit

iS5comm(config)#:

3.14. enableuser

To release a blocked user specified by the user name string, use the **enableuser** command in Global Configuration Mode.

enableuser

```
enableuser <username>
```

Parameters

Parameter	Type	Description
<username>	String	Enter the user ID of the blocked user.

Mode

Global Configuration Mode

Examples

iS5comm (config)# enableuser user1

3.15. clear line vty

To clear the virtual terminal line (vty) to an idle stat, use the **clear line vty** command in Global Configuration Mode.

clear line vty

```
clear line vty {2 | all}
```

Parameters

Parameter	Type	Description
vty		Enter to clear the virtual terminal line information related configuration.
2	Integer	Enter 2 for ID of a Telnet session
all		Enter to clear all vty information

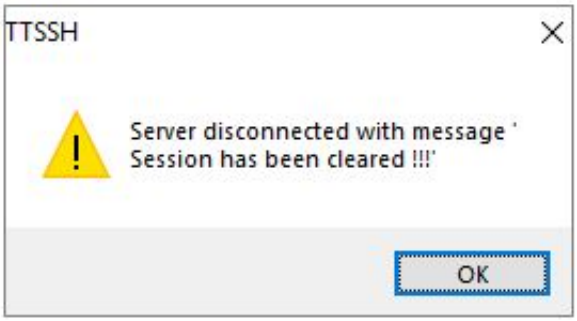
Mode

Global Configuration Mode

Examples

iS5comm# clear line vty all

The following message appears. Click OK.



3.16. password

To set the maximum life time after which the password has to be expired or determine a password validation mask, use the **password** command in Global Configuration Mode.

password

```
password max-life-time [<days (0-366)>] | validate char [lowercase] [upper-
case] [numbers] [symbols]
```

Parameters

Parameter	Type	Description
max-life-time		Enter to configure the time after which the user password has to expire.
<days (0-366)>		Enter expiry date in days. This value ranges from 0 to 366 days. The default value of password-max-life-time is 0 days, indicates the password does not expire.
validate	String	Enter to configure the type of characters to be considered for password validation rules and takes values as bit mas
char	String	Enter to create creates password rules
lowercase		Specify to configure the minimum number of lower case characters that are to be present in the password. If the given password has less than the configured number of lower case characters, it will not be allowed. This value ranges from 0 to 20. The default value is 1.
uppercase		Specify to configure the minimum number of upper case characters that are to be present in the password. If the given password has less than the configured number of upper case characters, it will not be allowed. This value ranges from 0 to 20. The default value is 1.
numbers		Specify to configure the minimum number of numbers that are to be present in the password. If the given password has less than the configured number of upper case characters, it will not be allowed. This value ranges from 0 to 20. The default value is 1.
symbols		Specify to configure the minimum number of symbols to be present in the password. If the given password has less than the configured number of numerical characters, it will not be allowed This value ranges from 0 to 20. The default value is 1. The list of supported symbols are as follows: !@#$%^&*()_+-:”;’{}[]|\~

Mode

Global Configuration Mode

Examples

iS5comm(config)# password max-life-time 1

iS5comm(config)# password validate lowercase 1

iS5comm(config)# password validate uppercase 1

iS5comm (config) # password validate numbers 1

iS5comm (config) # password validate symbols 1

3.17. set minimum password length

To configure minimum password length, use the **set minimum password length** command in Global Configuration Mode. If the given password has less than the configured password length, it will not be allowed.

set minimum password length

```
set minimum password length <minimum-len>
```

Parameters

Parameter	Type	Description
<minimum-len> (8-20)	Integer	Enter the minimum password length value which ranges from 8 to 20. The default value is 8.

Mode

Global Configuration Mode

Examples

iS5comm(config)# set minimum password length 8

3.18. set cli pagination

To enable and disable CLI pagination, use the **set cli pagination** command in Global Configuration Mode. The no form of the command **no pagination** disables the pagination as well.

set cli pagination

```
set cli pagination {on | off}
```

no pagination

```
no pagination
```

Parameters

Parameter	Type	Description
on		Enter the enable pagination.
off		Enter the disable pagination.

Mode

Global Configuration Mode

Examples

iS5comm(config)# set cli pagination off

iS5comm(config)# set cli pagination on

iS5comm(config)# no pagination

3.19. set banner-name

To configure the switch's banner name, use the **set banner-name** command in Global Configuration Mode.

set banner-name

```
set banner-name <string (50)>
```

Parameters

Parameter	Type	Description
<string (50)>	String	Enter a banner name. The banner name is a string with maximum size of 128.

Mode

Global Configuration Mode

Examples

iS5comm (config)# set banner-name bannername

3.20. set prompt-name

To configure the switch's CLI prompt name, use the **set prompt-name** command in Global Configuration Mode.

set prompt-name

```
set prompt-name <string (50)>
```

Parameters

Parameter	Type	Description
<string (50)>	String	Enter a prompt name. The banner name is a string with maximum size of 128.

Mode

Global Configuration Mode

Examples

iS5comm (config)# set prompt-name promptname

3.21. factory reset

To reset to the default configuration of the switch and erase user privileges and group flash files, use the **factory reset** command in Privileged EXEC Mode.

factory reset

```
factory reset users
```

Parameters

Parameter	Type	Description
users		Enter to erase user privileges and group flash files.

Mode

Privileged EXEC Mode

Examples

iS5comm # factory reset

```
Factory reset will erase following configurations..
1. Startup-config
2. NVRAM settings
3. Flash files
- users
- privil
- groups
Are you sure you want to reset device to factory default settings? (Y/N)
[N]?
```

3.22. show privilege

To show current user privilege level, use the **show privilege** command in Privileged EXEC Mode.

show privilege

```
show privilege
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show privilege

3.23. show line

To display TTY line information such as EXEC timeout, use the **show line** command in Privileged EXEC Mode.

show line

```
show line {console | vty <line>}
```

Parameters

Parameter	Type	Description
console		Enter to display the console information
vty		Enter to display information for the virtual terminal line
<line>	Integer	Enter the ID of a specific Telnet session for which the information will be displayed. The range is from 2 to 9.

Mode

Privileged EXEC Mode

Examples

iS5comm# show line console

```
    Current Session Timeout (in secs) = 180
    Default Telnet Session Timeout (in secs) = 180
```

iS5comm# show line vty 3

```
    Current Session Timeout (in secs) = 180
    Default Telnet Session Timeout (in secs) = 180
    % Line 2 not active
```

iS5comm# show line vty 2

```
    % Line 2 not active
```

3.24. show aliases

To display all aliases, use the **show aliases** command in Privileged EXEC Mode.

show aliases

```
show aliases
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show aliases

```
ct -> configure terminal
int -> interface
```

3.25. show history

To display a list of recently executed commands, use the **show history** command in Privileged EXEC Mode.

show history

```
show history
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show history

```
3  show privilege
4  show line vty 3
5  show vty 2
6  show line vty 2
7  show line console
8  show aliases
9  c t
10  alias ct configure terminal
11  alias config ct configure terminal
```

```
12  alais int interface
13  alias int interface
14  exit
15  show aliases
16  show users
17  show history
```

3.26. show eula

To display the information about the end user license agreement (eula), use the **show eula** command in Privileged EXEC Mode.

show eula

```
show eula
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show eula

3.27. set cli-console access

To enable or disable the switch's CLI console port

set cli-console

```
set cli-console access {enable | disable }
```

Parameters

Parameter	Type	Description
enable / disable	String	Used to enable or disable access to the cli console port

Mode

Global Configuration Mode

Examples

iS5comm (config)# set cli-console access enable

Related Commands

iS5comm# show nvram

3.28. set mgmt-port access

To enable or disable the switch's management port

set mgmt-port

```
set mgmt-port access {enable | disable }
```

NOTE: This command is not supported on the iMR320

Parameters

Parameter	Type	Description
enable / disable	String	Used to enable or disable access to the management port

Mode

Global Configuration Mode

Examples

iS5comm (config)# set mgmt-port access enable

Related Commands

iS5comm# show nvram

3.29. set external-storage access

To enable or disable the switch's storage peripherals

set external-storage

```
set external-storage access {enable | disable}
```

Parameters

Parameter	Type	Description
enable / disable	String	Used to enable or disable access to the storage peripherals such as the SD Card and USB port.

Mode

Global Configuration Mode

Examples

iS5comm (config)# set external-storage access enable

Related Commands

iS5comm# show nvram

System Features

4. System Features

A rich set of system features are available to the user, such as login services, copying / writing facilities, duplex / negotiation support, and many other capabilities.

Some features have special hardware requirements, and others have special design considerations.

4.1. ip address

To set the IP address for an interface, use the command **ip address** in Interface Configuration Mode. The no form of the command delete the IP Address configured on the given interface, resets the IP address of the interface to its default value, and deletes the IP address used in VPN and firewall.

ip address

```
ip address <ucast_addr> <ip_mask> [secondary {node0 | node1}] | dhcp
{client-id (FastEthernet <string(32)> | GigabitEthernet <string(32)> |
Port-channel <string(32)> | Vlan <string(32)>) | hostname <string(32)>} |
rarp {client-id (FastEthernet | GigabitEthernet | Port-channel | Vlan) |
hostname <string(32)>}
```

no ip address

```
no ip address {<ucast_addr> | cybsec}
```

Parameters

Parameter	Type	Description
<ucast_addr>	A.B.C.D	Sets the IP address for an interface. If the network in which the switch is implemented contains a server such as DHCP server, dynamically allocating IP address, the configured IP address should not be within the range of the addresses that will be allocated by the server to the other switches. This precaution avoids creation of IP address conflicts between the switches.
<ip_mask>	A.B.C.D	Sets the subnet mask for the configured IP address. The configured subnet mask should be in the same subnet of the network in which the switch is placed.
secondary	A.B.C.D	Sets the configured IP address as an additional IP address for the interface (the configured address is used as secondary address instead of primary address). **NOTE:** this parameter is not supported on OOB and PPP interface.
node0	A.B.C.D	Specifies the secondary IP address associated with the OOB interface of Node0.
node1	A.B.C.D	Specifies the secondary IP address associated with the OOB interface of Node1.
dhcp		Enter to allow the client device to obtain configuration parameters such as network address, from the DHCP server.
client-id		Enter to set the client identifier that specifies the interface type and hexadecimal MAC address of the specified interface. The various interface types that can be specified areas shown below.
FastEthernet		Enter to set FastEthernet client-id. FastEthernet is officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
<string(32)>		Enter string for interface name. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel and VLAN. Only VLAN or port-channel ID is provided, for interface types VLAN and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
GigabitEthernet		Enter to set GigabitEthernet client-id. GigabitEthernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

Parameter	Type	Description
<string(32)>		Enter string for interface name. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel and VLAN. Only VLAN or port-channel ID is provided, for interface types VLAN and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
Port-channel		Enter to set Port-channel client-id. Port-channel is a logical interface that represents an aggregator that contains several ports aggregated together.
<string(32)>		Enter string for interface name. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel and VLAN. Only VLAN or port-channel ID is provided, for interface types VLAN and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
Vlan		Enter to set Vlan client-id. Vlan is a logical interface that specifies a group of hosts that can communicate with each other as in the same broadcast domain.
<string(32)>		Enter string for interface name. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel and VLAN. Only VLAN or port-channel ID is provided, for interface types VLAN and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
hostname		Enter to set Port-channel client-id. Port-channel is a logical interface that represents an aggregator that contains several ports aggregated together.
<string(32)>		Enter string for interface name. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel and VLAN. Only VLAN or port-channel ID is provided, for interface types VLAN and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
rarp		Enter to set Port-channel client-id. Port-channel is a logical interface that represents an aggregator that contains several ports aggregated together.
client-id		Enter to set the client identifier that specifies the interface type and hexadecimal MAC address of the specified interface. The various interface types that can be specified areas shown below:

Parameter	Type	Description
FastEthernet		Enter to set FastEthernet client-id. FastEthernet is officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
<string(32)>		Enter string for interface name. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel and VLAN. Only VLAN or port-channel ID is provided, for interface types VLAN and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
GigabitEthernet		Enter to set GigabitEthernet client-id. GigabitEthernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<string(32)>		Enter string for interface name. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel and VLAN. Only VLAN or port-channel ID is provided, for interface types VLAN and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
Port-channel		Enter to set Port-channel client-id. Port-channel is a logical interface that represents an aggregator that contains several ports aggregated together
<string(32)>		Enter string for interface name. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel and VLAN. Only VLAN or port-channel ID is provided, for interface types VLAN and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
Vlan		Enter to set Vlan client-id. Vlan is a logical interface that specifies a group of hosts that can communicate with each other as in the same broadcast domain.
<string(32)>		Enter string for interface name. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel and VLAN. Only VLAN or port-channel ID is provided, for interface types VLAN and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
hostname		Enter to set Port-channel client-id. Port-channel is a logical interface that represents an aggregator that contains several ports aggregated together.

Parameter	Type	Description
<string(32)>		Enter string for interface name. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel and VLAN. Only VLAN or port-channel ID is provided, for interface types VLAN and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
cybsec		Enter IP address used in VPN and firewall.

Mode

Interface Configuration Mode

This command is applicable in VLAN Interface Mode/Router Interface / OOB Interface Mode / PPP mode

Default

- IP address specified in nvram.txt is taken as default for the default VLAN identifier.
- IP address is assigned as 0.0.0.0 and subnet mask as 255.255.255.255 for other interfaces.

Prerequisites

- The interface should be shut down before executing this command.
- The primary and secondary IP addresses should be different.
- The primary address should be configured before configuring the secondary address.
- The connection to the switch is lost if the IP address of the connected interface is modified.
- When the same network interface is used for OOB and NFS mounting, the operation done on OOB will have impact on NFS.
- For PPP mode, PPP interface should be attached to the physical interface first.

Examples

iS5comm(config-if)# ip address 10.0.0.3 255.255.255.0

iS5comm(config-if)# ip address 10.0.0.2 255.255.255.0 secondary

iS5comm (config-ppp)# ip address 17.0.0.100 255.255.255.

iS5comm(config-if)# ip address dhcp

iS5comm(config-if)# ip address rarp

4.2. switchport

To configure the port as switch port, use the command **switchport** in Interface Configuration Mode. Switch port-related commands are made available for the interface, only when the port is configured as switch port. The no form of the command resets the port as a router port. Only router port related commands are made available for the interface, when the port is configured as router port.

switchport

```
switchport
```

no switchport

```
no switchport
```

Mode

Interface Configuration Mode

Default

- switchport

Prerequisites

- The interface should be shut down before executing this command

Examples

iS5comm(config-if)# switchport

iS5comm(config-if)# no switchport

4.3. default ip address allocation protocol

To configure the protocol used by the default interface for acquiring its IP address, use the command **default ip address allocation protocol** in Global Configuration Mode. This configuration takes effect only on rebooting the system.

default ip address allocation protocol

```
default ip address allocation protocol {bootp | rarp | dhcp}
```

Parameters

Parameter	Type	Description
bootp		Enter to allow the client device to obtain its own IP address, address of a server host and name of a boot file to be executed from a BOOTP server.
rarp		Enter to allow the client device to dynamically find its IP address from RARP server, when it has only its hardware address such as MAC address
dhcp		Enter to allow the client device to obtain configuration parameters such as network address, from the DHCP server.

Mode

Global Configuration Mode

Default

dhcp

Prerequisites

- This command executes only if the default mode is configured as Dynamic.
- If the default interface is configured as OOB and if the same network interface is used for OOB and NFS mounting, then the operation done on OOB will have impact on NFS.

Examples

iS5comm(config)# default ip address allocation protocol bootp

4.4. ip http

To set the HTTP port, use the command **ip http** in Global Configuration Mode. The no form of the command resets the HTTP port to its default value.

ip http

```
ip http {port <port-number (1-65535)> | secure (ciphersuite {TLS_ECDHE_R-
SA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 |
TLS_AES_256_GCM_SHA384 | TLS_CHACHA20_POLY1305_SHA256 | TLS_AES_128_GCM_-
SHA256 } | port (1-65535) | minimum version { TLSv1_2 | TLSv1_3 } | crypto
key RSA2048 { default | current | string values } server)}
```

no ip http

```
no ip http port | secure
```

Parameters

Parameter	Type	Description
port		Enter to configure HTTP port. his port is used to configure the router using the Web interface. The available port numbers are from 1 to 65535
<port-number (1-65535)>	Integer	Enter a port number. The available port numbers are from 1 to 65535 **NOTE:** TACACS user will be given root privilege by default or local user privilege if the user exists in local database
secure		Enter for SSL secure server related configuration. The options are as follows:
ciphersuite		Enter for Cipher-suites list options.
CR		Enter to disable SSL server on the device and also to disable ciphersuites and crypto key configuration. If you want to specify an encryption algorithm, enter one of the shown below options.
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384		Enter for this encryption algorithm.
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256		Enter for this encryption algorithm.
TLS_AES_256_GCM_SHA384		Enter for this encryption algorithm.
TLS_CHACHA20_POLY1305_SHA256		Enter for this encryption algorithm.
TLS_AES_128_GCM_SHA256		Enter for this encryption algorithm.
minimum version		This is used to specify the minimum level of TLS to be used. The choices are as follows.
TLSv1_2		TLS version 1.2
TLSv1_3		TLS version 1.3
rsa-with-aes-256-cbc-sha		Enter for this encryption algorithm.
crypto		Enter a name of the created list.
key		

Parameter	Type	Description
RSA2048		Enter for RSA algorithm.
default		This option will use the default RSA 2048 certificate values. A carriage return is entered after this option.
current		Use the current certificate subject name
Certificate Values are entered	A series of Strings	Up to 2 characters for the country code string Up to 100 characters for the state/province value Up to 100 characters for the city/locality value Up to 100 characters for the organization value Up to 100 characters for the organizational unit name Up to 100 characters for the common name
server		Enter to enable the SSL server on the device and also to configure the ciphersuites.
port		The port option when used after secure. For example “ip http secure port” allows the user to specify the port number of the HTTPS server. It is followed by a port number.
<port-number (1-65535)>	Integer	Value of the port number to be used by the HTTPs server.

Mode

Global Configuration Mode

Default

80

Prerequisites

HTTP port number configuration takes effect only when HTTP is disabled and enabled again

Examples

iS5comm(config)# ip http port 90

iS5comm(config)# ip http secure ciphersuite

For a new certificate to be used the http service must be disabled and then re-enabled. iS5comm(config)# no ip http secure server

iS5comm(config)# ip http secure server

4.5. login authentication

To configure the authentication method for user logins for accessing the GUI to manage the switch, use the command **login authentication** in Global Configuration Mode. Few network routers and other network equipment allows access to a server or a managing computer to determine if the user attempting to log in has the proper rights or is in the user database. The no form of the command resets the authentication method for user logins to its default values. Changing login authentication from default to another value may disconnect the telnet session.

login authentication

```
login authentication {radius | tacacs | local | default <string(32)>
```

no login authentication

```
no login authentication default <string(32)>
```

Parameters

Parameter	Type	Description
radius		Enter to set the RADIUS server to be used as an authentication server. Enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. **NOTE:** RADIUS user will be given privilege based on service type attribute value received in access accept packet from radius server
tacacs		Enter to set the TACACS server to be used as an authentication server. It communicates with the authentication server commonly used in networks.RADIUS user will be given privilege based on service type attribute value received in access accept packet from radius server **NOTE:** TACACS user will be given root privilege by default or local user privilege if the user exists in local database
local		Enter to set locals authentication. The user identification, authentication, and authorization method is chosen by the local system administration and does not necessarily comply with any other profiles..
default		Enter to set the default authentication method for User Login.
<string 932)>		Enter a name of the created list.

Mode

Global Configuration Mode

Default

local

Examples

iS5comm(config)# login authentication radius

iS5comm(config)# login authentication default

4.6. set ip http

To enable / disable HTTP in the switch, use the command **set ip http** in Global Configuration Mode.

set ip http

```
set ip http {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enter to enable HTTP in the switch.
disable		Enter to disable HTTP in the switch.

Mode

Global Configuration Mode

Default

enable

Examples

iS5comm(config)# set ip http disable

4.7. authorized-manager ip-source

To configure an IP authorized manager, use the command **authorized-manager ip-source** in Global Configuration Mode. The no form of the command removes manager from authorized managers list.

authorized-manager ip-source

```
authorized-manager ip-source <ip_addr> [<subnet-mask> |
<prefix-length(1-32)>] | [interface {[fastethernet interface-type <0/a-b,
0/c, ...>] | [gigabitethernet interface-type <0/a-b, 0/c, ...>] |
[extreme-ethernet <interface-type <a,b or a-b or a,b,c-d...>] | [vlan [vlan
<a,b or a-b or a,b,c-d>] [cpu0] [service [snmp] | [service [snmp] | [telnet]
| [http] | [https] | [ssh]] | port-channel <port_channel list (a,b or a-b or
a,b,c-d)>
```

no authorized-manager ip-source

```
no authorized-manager ip-source <ip_addr> [<subnet-mask> |
<prefix-length(1-32)>]
```

Parameters

Parameter	Type	Description
ip_addr	A.B.C.D	Enter to set the network or host address from which the switch is managed. An address 0.0.0.0 indicates 'Any Manager'.
<subnet-mask>		Enter to set the subnet mask for the configured IP address. The configured subnet mask should be in the same subnet of the network in which the switch is placed
<prefix-length(1-32)>	Integer	Enter to configure the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges from 1 to 32.
interface		Configures the network or host address for the specified interface. The details to be provided are:
fastethernet		Enter for fastethernet. Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
interface-type <0/a-b, 0/c, ...>		Enter to set the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
gigabitethernet		Enter for gigabitethernet.
interface-type <0/a-b, 0/c, ...>		Enter to set the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
extreme-ethernet		Enter for extreme-ethernet.
interface-type <a,b or a-b or a,b,c-d...>		Enter to set the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
vlan		Enter for vlan. It set the list of VLANs or a single specifc VLAN in which the IP authorized manager can reside
vlan <a,b or a-b or a,b,c-d>		Enter to determine the set of vlan interfaces.
cpu0		Enter to configure the access rights for the manager of the switch through OOB Port

Parameter	Type	Description
service		Enter to configure the type of service to be used by the IP authorized manager. The values can be
snmp		Enter for snmp. It manages complex networks. SNMP works by sending messages, called PDUs, to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in MIBs and return this data to the SNMP requesters
http		Enter for HTTP service. It defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page
https		Enter for HTTPS service. It transmits data securely over the World Wide Web. S-HTTP is designed to transmit individual messages in a secured manner.
ssh		Enter for SSH service. It logs into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist. SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force ssh to disconnect. He or she cannot play back the traffic or hijack the connection when encryption is enabled
telnet		Enter for Telnet service.
port-channel		Enter for port-channel.
port_channel list (a,b or a-b or a,b,c-d)		Enter a combination for port_channel list. This value is a combination of numbers separated by a slash. Use comma as a separator without space while configuring list.

Mode

Global Configuration Mode

Default

All services are allowed for the configured manager

Examples

iS5comm(config)# authorized-manager ip-source 10.203.113.5 255.255.255.255 inter face gigabiteth-ernet 0/1

4.8. mtu

To configure the Maximum Transmission Unit (MTU) frame size for all frames transmitted and received on all interfaces in a switch, use the command **mtu** in Interface Configuration Mode. The no form of this command sets the maximum transmission unit to the default value in all interfaces.

mtu

```
mtu <frame-size(46-9216)>
```

Parameters

Parameter	Type	Description
<frame-size (46-9216)>	Integer	Enter a size of the MTU frame. The value ranges from 46 to 9216 and defines the largest PDU that can be passed by the interface without any need for fragmentation. This value is shown to the higher interface sub-layer and should not include size of the encapsulation or header added by the interface. This value represents the IP MTU over the interface, if IP is operating over the interface

Mode

Interface Configuration Mode

Default

1500

Examples

iS5comm (config-if)# mtu 900

4.9. loopback local

To enables loopback on a physical interface, use the command **loopback local** in Interface Configuration Mode. The no form of this command disables the loopback on a physical interface.

loopback local

no loopback local

Mode

Interface Configuration Mode

Examples

iS5comm (config-if)# loopback local

4.10. archive download-sw

To perform an image download operation on a switch stack or download a new image from a TFTP or SFTP from a remote location to the switch and to overwrite or keep the existing image, use the command **archive download-sw** in Privileged EXEC Mode.

archive download-sw

```
archive download-sw /overwrite {<tftp://server/filename> |
<sftp://<user-name>:<pass-word>@server/filename> | <flash://}
```

Parameters

Parameter	Type	Description
/overwrite		Enter to overwrites the software image in flash with the downloaded one. This option should be specified only if the flash device has sufficient space to hold two images.
tftp://server/filename startup-config		Enter to configure the source URL and filename used to overwrite / update the existing image. The file is transferred using TFTP.
<sftp://<user-name>:<pass-word>@server/filename>		Enter to configure the source URL, user name, password and filename used to overwrite / update the existing image. The file is transferred using SFTP.
user-name		Enter for the user name of remote host or server
pass-word		Enter for the password for the corresponding user name of remote host or server
server	A.B.C.D	Enter for the IP address or host name of the server
filename		Enter for filename in which we are copying
flash		Enter to configure the name of the flash file used to overwrite / update the existing image

Mode

Privileged EXEC Mode

Prerequisites

Filenames and directory names are case sensitive

Examples

iS5comm# archive download-sw /overwrite tftp://20.0.0.1/IS5COM.exe

```
    Download is in Progress...
```

4.11. interface

To configure interface features, such as out of band management, port channel, tunnel, etc., use the command **interface** in Global Configuration Mode. The no form of the command deletes interface such as VLAN, port-channel, tunnel interface, etc.

interface

```
interface {Extreme-Ethernet <interface-id> | gigabitethernet <interface-id>]
| ac <integer (1-65535)> | linuxvlan <interface name> | loopback <loopback
(1-1000)> | mgmt0 | port-channel <port-channel-id (1-65535)> | ppp <inter-
face-id(1-128)> | pw <interface-id (1-65535)> | range {Extreme-Ethernet |
fastethernet | gigabitethernet} | s-channel <s-channel-id (1-65535)> |
tunnel <interface-id(1-128)> | {vlan <vlan-id(1-4094> [switch default]}
```

no interface

```
interface {Extreme-Ethernet <interface-id> | gigabitethernet <interface-id>]
| ac <integer (1-65535)> | linuxvlan <interface name> | loopback <loopback
(1-1000)> | port-channel <port-channel-id (1-65535)> | ppp <inter-
face-id(1-128)> | pw <interface-id (1-65535)> | range {Extreme-Ethernet |
fastethernet | gigabitethernet} | tunnel <interface-id(1-128)> | {vlan
<vlan-id(1-4094>}
```

Parameters

Parameter	Type	Description
Gigabitethernet		Enter to configure gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to configure a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to configure the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
ac		Enter to configure the Attachment Circuit identifier in the system. Attachment Circuit (AC) is a physical or virtual circuit attaching a Customer Edge to a Provider Edge port.
<integer(1-65535)>	Integer	Enter a specific ac ID. This value ranges from 1 to 65535.
linuxvlan		Enter to configure the interface name of the Linux VLAN Interface.
<interface name>	Integer	Enter a specific Linux VLAN ID. This value ranges from 1 to 65535.
loopback		Enter to display the IP interface configuration for the specified loopback ID
<loopback-id (0-100)>	Integer	Enter a specific loopback ID. This is a unique value that represents the specific loopback created that ranges from 0 to 100.
mgmt0		Enter for Out of Band management interface.
port-channel		Enter to display the Port channel interface configuration for the specified port channel ID
<port-channel-id (1-65535)>	Integer	Enter a specific port channel ID. This value ranges from 1 to 65535.
ppp		Enter to configure the PPP interface configuration.
<interface-id (1-128)>	Integer	Enter a PPP ID. This value ranges from 1 to 128.
pw		Enter to configure the Pseudo wire interface
<interface-id (1-65535)>	Integer	Enter a specific pw ID. This value ranges from 1 to 65535.

Parameter	Type	Description
range		Enter to configure interface range configuration
Gigabitethernet		Enter to configure gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
fastethernet		Enter to configure fastenetherner type of interface or as referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits / second.
Extreme-Ethernet		Enter to display the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
s-channel		Enter to configure S-channel interface or the specified S-channel ID.
<interface-id (1-65535)>	Integer	Enter a specific s-channel ID. This value ranges from 1 to 65535.
tunnel		Enter to display the tunnel interface configuration for the specified tunnel ID
<tunnel-id (1-128)>	Integer	Enter a tunnel ID. This value ranges from 1 to 128.
vlan		Enter a specific VLAN ID. This is a unique value that represents the specific VLAN created that ranges from 1 to 4094.
<vlan-id(1-4094)>	Integer	Enter a specific VLAN ID. This is a unique value that represents the specific VLAN created that ranges from 1 to 4094.
switch default		Enter to specify default switch.

Mode

Global Configuration Mode

Prerequisites

- The command no shutdown must be executed for the interface to be active.
- Logical interfaces cannot be created in the switch, if the base bridge mode is configured as transparent bridging.

Examples

iS5comm# interface tunnel 0

iS5comm(config-if)#

4.12. mac-addr

To configure unicast MAC address for the interface, use the command **mac-addr** in Interface Configuration Mode.

mac-addr

```
mac-addr <aa:aa:aa:aa:aa:aa>
```

Mode

Interface Configuration Mode

Default

MAC address of the switch is assigned as MAC address for the interface.

Prerequisites

- The MAC address can be set only when ifMainAdminStatus for the interface is down.
- The object is valid only for interfaces that have the ifMainType set as ethernetCsmacd(6) or ieee8023ad(161)

Examples

iS5comm (config-if)# mac-addr 00:22:33:44:55:66

4.13. system

To configure the Maximum Transmission Unit (MTU) frame size for all frames transmitted and received on all interfaces in a switch, to assign system contact information, name, and location, use the command **system** in Global Configuration Mode. The no form of this command sets the maximum transmission unit to the default value in all interfaces

system

```
system [mtu <frame-size(46-9216)>] [contact <string(255)>] [location
<string(255)>] [name <string(255)>]
```

no system mtu

Parameters

Parameter	Type	Description
mtu		Enter to configure the Maximum Transmission Unit (MTU) frame size.
<frame-size(46-9216)>	Integer	Enter a size of the MTU frame. The value ranges from 46 to 9216. This value defines the largest PDU that can be passed by the interface without any need for fragmentation. This value is shown to the higher interface sub-layer and should not include size of the encapsulation or header added by the interface. This value represents the IP MTU over the interface if IP is operating over the interface.
contact		Enter to configure the system contact information.
<string(255)>		Enter a string for contact information / location / system name respectively
location		Enter to configure the system location.
name		Enter to configure the system name.

Mode

Global Configuration Mode

Examples

iS5comm(config)# system mtu 200

iS5comm(config)# system contact support@x.com

iS5comm(config)# system location Controls

S5comm(config)# system name Raptor

4.14. snmp trap link-status

To enable snmp trap link-status, use the command **snmp trap link-status** in Global Configuration Mode. The interface generates linkUp or linkDown trap. The linkUp trap denotes that the communication link is available and ready for traffic flow. The linkDown trap denotes that the communication link failed and is not ready for traffic flow. The no form of this command disables trap generation on the interface.

snmp trap link-status

no snmp trap link-status

Mode

Interface Configuration Mode

Default

SNMP trap link status is enabled

Prerequisites

- This configuration can be done, only if the interface is administratively down.
- Any messages larger than the MTU are divided into smaller packets before transmission

Examples

iS5comm (config-if)# snmp trap link-status

4.15. bridge port-type

To the bridge port type for an interface, use the command **bridge port-type** in Interface Configuration Mode.

bridge port-type

```
bridge port-type {customerBridgePort | customerEdgePort | customerNetwork-
Port {c-tagged | port-based | s-tagged} | propCustomerEdgePort | propCustom-
erNetworkPort | propProviderNetworkPort | providerNetworkPort | uplinkAc-
cessPort}
```

Parameters

Parameter	Type	Description
customerBridgePort		Enter to set bridge port type as Customer Bridge Port. The port is to be used in customer bridges and in provider (Q-in-Q) bridges. This port type is not valid in PCBs and PEBs
customerEdgePort		Enter to set the bridge port type as Customer Edge Port. The port is in a PEB that is connected to a single customer. The packets received on this port are initially classified to a CVLAN. CVLAN classification is done based on the VID in the C-tag present in the packet or from the PVID of the port. Service instance selection is done for a frame based on the entry present in the C-VID registration table for the pair (C-VID, reception port)
customerNetworkPort		Enter to set the bridge port type as customer network port.
c-tagged		Enter to set the bridge port type as c-tagged.
port-based		Enter to set the bridge port type as port-based.
s-tagged		Enter to set the bridge port type as s-tagged.
propCustomerEdgePort		Enter to set the bridge port type as Proprietary Customer Edge Port. The port is connected to a single customer, where multiple services can be provided based on only proprietary SVLAN classification tables. S-VLAN classification is not done based on C-VID registration table on the port.
propCustomerNetworkPort		Enter to set bridge port type as Proprietary Customer Network Port. The port is connected to a single customer, where multiple service can be provided based on CVLANs by assigning one of the proprietary SVLAN classification tables to the port. The services can also be assigned using other proprietary SVLAN classification tables, where CVLAN is not the index of the table.
propProviderNetworkPort		Enter to set bridge port type as Proprietary Provider Network Port. The port is connected to a Q-in-Q bridge located inside the provider network. The port acts as a part of S-VLAN component. The packets to be tagged and sent out of the port contain 0x8100 as its Ethertype. The packets received with standard Q tag is considered as S-Tagged packet.

Parameter	Type	Description
providerNetworkPort		Enter to set the bridge port type as provider network port. This option is applicable in provider bridges and provider backbone b-component bridge modes. The port is connected to a single provider.
uplinkAccessPort		Enter to set a port on a Port-mapping S-VLAN component that connects an EVB Bridge with an EVB Station

Mode

Interface Configuration Mode

Default

- providerNetworkPort for provider core and edge bridges.
- customerBridgePort for customer bridges.

Prerequisites

- Tunneling must be enabled to change port type from Provider Network Port.
- Tunneling must be disabled to change port type to Provider Network Port.
- Port must be administratively down for changing to another port type.
- Bridge port-type is supported only in the following Bridge Modes:
  - Provide Edge Bridge
  - Provider Core Bridge
  - Provider Backbone Bridge I Component
  - Provider Backbone Bridge B Component
- In case of Provider Bridge or Customer Bridge, bridge port type will always be customerBridgePort. CustomerEdgePort is valid only in Provider Edge Bridge.
- All other port types excluding customerBridgePort and customerEdgePort are valid in both Provide Edge Bridge and Provider Core Bridge.
- Bridge port type can be set only for switch ports and not for router ports, IVR interfaces and I-LAN interfaces.
- The port type cannot be set for a port-channel port, if physical ports are aggregated in the port-channel.
- The port type cannot be set for a port that is part of a port-channel.

Examples

iS5comm (config-if)# bridge port-type providerNetworkPort

4.16. monitor session

To configure port mirroring, use the command **monitor session** in Global Configuration Mode. The no form of this command cancels the specified session.

monitor session

```
monitor session <index of mirroring session(1-7)> destination (interface
{Extreme-Ethernet <ifnum> | Gigabitethernet <ifnum>} | comp) | source
(interface {Extreme-Ethernet <ifnum> | Gigabitethernet <ifnum>} | {both | rx
| tx} | comp)}
```

no monitor session

```
no monitor session local | range <port_list> | destination <index of
mirroring session(1-7)> destination (interface {Extreme-Ethernet <ifnum> |
Gigabitethernet <ifnum>} | comp) | source (interface {Extreme-Ethernet
<ifnum> | Gigabitethernet <ifnum>} | {both | rx | tx} | comp)}
```

Parameters

Parameter	Type	Description
<index of mirroring session(1-7)>	Integer	Enter a number for monitoring session. The scope is from 1 to 7.
local		Enter to remove all local mirroring configuration sessions.
<port_list>	Integer	Enter a number for monitoring session to be removed.
destination		Enter for destination port related configuration.
interface		Enter for Interface related configuration.
Extreme-Ethernet		Enter for Extreme Ethernet interface.
<ifnum>		Enter a number combination for interface. For example, 0/1 or port channel ID.
Gigabitethernet		Enter for Gigabit Ethernet interface.
<ifnum>		Enter a number combination for interface. For example, 0/1 or port channel ID.
comp		Enter for Compatibility Mode.
source	Integer	Enter for source port related configuration.
both	Integer	Enter to mirror both received and transmitted traffic.
rx	Integer	Enter to mirror received traffic.
tx	Integer	Enter to mirror transmitted traffic.

Mode

Global Configuration Mode

Examples

iS5comm(config)# monitor session 1 destination interface Gigabitethernet 0/2

iS5comm(config)# monitor session 1 source interface gig 0/1

4.17. show monitor

To display the mirroring Information present in the system, use the command **show monitor** in Privileged EXEC Mode.

show monitor

```
show monitor {session <session-id (1-7)> | local [detail] | range
<session-list> | all} [detail]
```

Parameters

Parameter	Type	Description
session		Enter to display the mirroring information for a session.
<session-id (1-7)>	Integer	Enter a number of an session for which the mirroring information will be displayed. The scope is from 1 to 7.
local		Enter to display the Mirroring information for the Flash.
detail		Enter Displays the detailed information regarding the session.
range		Enter to display the mirroring information for the specified range of sessions.
<session-list>	Integer	Enter a number of a range of sessions for which the mirroring information will be displayed.
all		Enter to display mirroring information for all sessions.

Mode

Privileged EXEC Mode

Examples

iS5comm# show monitor all

```
Mirroring is globally Enabled.
Session     : 1
-------
Source Ports
Rx              : None
Tx              : None
Both            : None
Destination Ports : Gi0/1
Session Status    : Inactive
Rspan Disabled
```

4.18. mirror cpu-port

To configure the type of mirroring and mirror-to port for CPU traffic, use the command **mirror cpu-port** in Global Configuration Mode.

mirror cpu-port

```
mirror cpu-port {both | both_meta | rx | rx_meta | tx | tx_meta} destination
{interface (Extreme-Ethernet <ifnum (0/1-28)> | Gigabitethernet <ifnum
(0/1-28)>)}
```

Parameters

Parameter	Type	Description
both		Enter to configure mirroring of both egress and ingress traffic over CPU port to the CPU mirrored-to port in the system.
both_meta		Enter to configure mirroring of both egress and ingress traffic over CPU port to the CPU mirrored-to port in the system with meta data.
rx		Enter to configure mirroring of ingress traffic over CPU port to the CPU mirrored-to port in the system.
rx_meta		Enter to configure mirroring of ingress traffic over CPU port to the CPU mirrored-to port in the system with meta data.
tx		Enter to configure mirroring of egress traffic over CPU port to the CPU mirrored-to port in the system.
tx_meta		Enter to configure mirroring of egress traffic over CPU port to the CPU mirrored-to port in the system with meta data.
interface		Enter for Interface related configuration.
Extreme-Ethernet		Enter for Extreme Ethernet interface.
<ifnum (0/1-28)>		Enter a number combination for interface. For example, 0/1 or port channel ID.
Gigabitethernet		Enter for Gigabit Ethernet interface.
<ifnum (0/1-28)>		Enter a number combination for interface. For example, 0/1 or port channel ID.

Mode

Global Configuration Mode

Examples

iS5comm (config)# mirror cpu-port both destination interface gi 0/1

4.19. show cpu-mirroring

To display the CPU mirroring Information present in the system, use the command **show cpu-mirroring** in Privileged EXEC Mode.

show cpu-mirroring

```
show cpu-mirroring
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show cpu-mirroring

```
    CPU Traffic Mirror-To port : Gi0/1
    CPU Traffic Mirroring Type : Ingress & Egress
```

4.20. write

To write the running-config in a flash, startup-configuration file or to a remote site, use the command **write** in Global Configuration Mode.

write

```
write <flash:filename> | <sftp://<user-name>:<pass-word>@server/filename> |
<tftp://server/filename> | startup-config
```

Parameters

Parameter	Type	Description
flash		Enter to write the configuration to a flash drive.
filename		Enter to configure the name of the file to which the configuration is to be saved. This file is present in the flash drive.
sftp		Enter to configure the SFTP option to be used for writing the configuration to a file in SFTP server.
user-name		Enter the username of remote host or server.
pass-word		Enter the password for the corresponding username of remote host or server.
server		Enter the IP address or host name of the server in which configuration should be maintained.
filename		Enter the name of the file in which the configuration should be written.
tftp		Enter to configure the TFTP related details for writing the configuration to a file in TFTP server.
server		Enter the IP address or host name of the server in which configuration should be maintained.
filename		Enter the name of the file in which the configuration should be written.
startup-config		Enter to start the switch with the saved configuration during reboot.

Mode

Privileged EXEC Mode

Prerequisites

- Filenames and directory names are case sensitive

Examples

iS5comm# write startup-config

4.21. copy

To copy the configuration from a remote site to flash, make a backup of the initial configuration in flash or at a remote location, or write the system logs to a remote site, SD card or USB, use the command **copy** in Privileged EXEC Mode.

copy

```
copy <flash_url> | <sftp://<user-name>:<pass-word>@server/filename> |
<tftp://server/filename> startup-config | flash {coredump <file_name>
(<tftp_url> | SD-Card | usb) <file_name>} | log <file_name> (<sftp_url> |
<tftp_url> | SD-Card | usb) <file_name> | tech_report (<sftp_url> |
<tftp_url> | SD-Card | usb) <file_name> | startup-config {<flash:/> |
<tftp://server/filename> | <sftp://<user-name>:<pass-word>@server/filename>
| usb} | running-config startup-config
```

Parameters

Parameter	Type	Description
<flash_url>		Enter to copy to flash or remote site.
<sftp://<user-name>:<pass-word>@server/filename>		Enter to configure the name of the file in remote location to be copied (downloaded) into configuration file (iS5Com.conf). This option configures the SFTP server details.
user-name		Enter for the user name of remote host or server
pass-word		Enter for the password for the corresponding user name of remote host or server
server	A.B.C.D	Enter for the IP address or host name of the server
filename		Enter for filename in which we are copying
tftp://server/filename startup-config		Enter to configure the address from which the file is to be copied and the file name from which configuration is to be copied. This option configures the TFTP server details
flash		Enter for flash related configuration
coredump		Enter for coredump file in flash
<file_name>		Enter file name of size (1-128) characters
<tftp_url>		Enter for a file in remote location using the TFTP option.
SD-Card		Enter for SD-Card file transfer operation
usb		Enter for a USB file transfer operation
<file_name>		Enter file name of size (1-128) characters
<file_name>		Enter file name of size (1-128) characters
SD-Card		Enter for SD-Card file transfer operation
usb		Enter for a USB file transfer operation
tech_report		Enter for tech.report file in flash
<sftp_url>		Enter for a file in remote location to be copied using the SFTP option.
<tftp_url>		Enter for a file in remote location to be copied using the TFTP option.
SD-Card		Enter for SD-Card file transfer operation
usb		Enter for a USB file transfer operation

Parameter	Type	Description
`startup-config`		Enter to copy the running configuration to the startup configuration file in NVRAM, where the running-config is the current configuration in the router and the startup config is the configuration that is loaded when the router boots up
`<flash://`		Enter to configure the name of the file in which the initial configuration should be stored. This file is available in the Flash.
`running-config`		Enter to copy running-configuration to startup-configuration. This command copies the variables from the running configuration to the startup configuration file in NVRAM, where the running-config is the current configuration in the router and the startup config is the configuration that is loaded when the router boots up

Mode

Privileged EXEC Mode

Prerequisites

Filenames and directory names are case sensitive

Examples

iS5comm# copy flash:clcliser startup-config

iS5comm# copy startup-config flash:clcliser

iS5comm# copy running-config startup-config

iS5comm# copy logs tftp://12.100/log.txt standby

```
    Log Upload Successful
```

iS5comm# copy tftp://12.0.0.2/clclirel flash:clcliser

iS5comm# copy flash log file_name SD-Card myfile

4.22. set linkup-delay

To enable / disable the Linkup-delay of the interface, use the command **set linkup-delay** in Global Configuration Mode.

set linkup-delay

```
set linkup-delay {enable | disable}
```

Parameters

Parameter	Type	Description
`enable`		Enter to enable linkup delay in the system by suspending operational status of the link for a configured delay time
`disable`		Enter to disable linkup delay in the system by not delaying and indicating the operational status of the link to the higher layers immediately.

Mode

Global Configuration Mode

Prerequisites

- Linkup-delay configurations are supported only on physical interfaces.
- Linkup-delay configurations are not supported for the logical interfaces like port-channel, router ports.

Examples

iS5comm (config)# set linkup-delay enable

4.23. linkup-delay

To enable the Linkup-delay of the interface, use the command **linkup-delay** in Interface Configuration Mode. The no form of the command disables the Linkup-delay of the interface or resets the Linkup-delay Timer.

linkup-delay

```
linkup-delay [timer] <integer (1-1000)>
```

no linkup-delay

```
no linkup-delay [timer]
```

Parameters

Parameter	Type	Description
`timer`		Enter to set up timer for Linkup-delay
`<integer (1-1000)>`	Integer	Enter a number for timer value. The scope is from 1 to 1000.

Mode

Interface Configuration Mode

Prerequisites

- The command **linkup-delay** executes only if LinkUp Delay is enabled in the system Configuration Mode. See command **set linkup-delay**.
- The command **linkup-delay timer** executes only if LinkUp Delay is enabled in the system Configuration Mode. Execute first the command **linkup-delay**.

Examples

S5comm (config)# set linkup-delay enable

iS5comm (config-if)# linkup-delay

iS5comm (config-if)# linkup-delay timer 10

4.24. show linkup-delay

To display the mirroring Information present in the system, use the command **show linkup-delay** in Privileged EXEC Mode.

show linkup-delay

```
show linkup-delay [interface {gigabitethernet <ifnum (0/1-28)> |
extreme-ethernet] <ifnum (0/1-28)>}]
```

Parameters

Parameter	Type	Description
interface		Enter to display the mirroring information for a session.
gigabitethernet		Enter for interface type.
<ifnum (0/1-28)>		Enter an interface combination. The format is <0>/<1-28> which stands for slot number / port number.
extreme-ethernet		Enter for interface type.

Mode

Privileged EXEC Mode

Examples

iS5comm# show linkup-delay interface gi 0/9

```
    LinkUp Delay Table
    -------------------
    Interface Id                          : Gi0/9
    Link Up Delay System Status           : ENABLED
    Link Up Delay Port Status             : ENABLED
    Link Up Delay Port Time               : 10 SecondsLink Up Delay
    Remaining Time           : 0 Seconds
```

4.25. firmware switch

To perform switch firmware primary or secondary partition, use the command **firmware switch** in Privileged EXEC Mode.

firmware switch

```
firmware switch partition
```

Mode

Privileged Mode

Examples

S5comm # firmware switch partition

4.26. firmware upgrade

To perform firmware upgrade using TFTP from a remote location, SFTP, or from a USB flash drive, use the command **firmware upgrade** in Privileged EXEC Mode.

firmware upgrade

```
firmware upgrade <tftp://ip_addr//File-path/file-name.tgz-name> |
sftp://<user_name>:<pass_word>@ip_addr//File-path/file-name.tgz | usb
file-name.tgz
```

Parameters

Parameter	Type	Description
tftp://		Enter for upgrade by TFTP from a remote location.
ip_addr	A.B.C.D	Enter for IP address or host name of the TFTP server.
File-path		Enter for the file path to be used for firmware upgrade.
file-name		Enter for the file name of the upgrade software.
sftp://		Enter for upgrade by TSFTP.
<user_name>		Enter for user name of remote host or server.
pass-word		Enter for password for the corresponding username of remote host or server.
ip_addr	A.B.C.D	Enter for IP address or host name of the server.
File-path		Enter for name of the file path where the information is to be copied.
usb		Enter for upgrade from a USB flash drive.
file-name		Enter for the file name of the upgrade software.

Mode

Privileged EXEC Mode

Prerequisites

Filenames and directory names are case sensitive

Examples

iS5comm# firmware upgrade tftp: //192.168.10.10//UpgradeFolder/firmware_upgrade.tgz

4.27. clock set

To manage the system clock, use the command **clock set** in Privileged EXEC Mode.

clock set

```
clock set hh:mm:ss <day (1-31)> <month (01-12)> {january | february | march
| april | may | june | july | august | september | october | november |
december} <year (2000 - 2037)>
```

Parameters

Parameter	Type	Description
hh:mm:ss://		Enter to set the current time.
<day (1-31)>		Enter to set the current day. This value ranges from 1 to 31.
<month (01-12)>		Enter the month. This value ranges from 01 (January) to 12 (December)..
january		Enter to set the month as January.
february		Enter to set the month as February.
march		Enter to set the month as March.
april		Enter to set the month as April.
may		Enter to set the month as May.
june		Enter to set the month as June.
july		Enter to set the month as July.
august		Enter to set the month as August.
september		Enter to set the month as September.
october		Enter to set the month as October.
november		Enter to set the month as November.
december		Enter to set the month as December.
<year (2000 - 2037)>		Enter to set the year. This value ranges from 2000 to 2037

Mode

Privileged EXEC Mode

Examples

iS5comm# clock set 4:42:55 9 july 2019

4.28. erase

To clear the contents of the startup configuration or set parameters in NVRAM to default values or erase the syslog file from an internal flash, use the command **erase** in Privileged EXEC Mode.

erase

```
erase {startup-config | nvram: | flash log | <flash_url>}
```

Parameters

Parameter	Type	Description
`startup-config`		Enter to clear the startup configuration file.
`nvram:`		Enter to clear the content from NVRAM.
`flash`		Enter to clear the content from flash files.
`log`		Enter to clear the content of the log file.
`<flash_url>`		Enter to clear the content from the local system flash file.

Mode

Privileged EXEC Mode

Examples

iS5comm# clock erase startup-config

4.29. cli console

To enable the console CLI through a serial port, use the command **cli console** in Privileged EXEC Mode. The no form of the command disables console CLI.

cli console

no cli console

Mode

Privileged EXEC Mode

Default

Enabled

Examples

iS5comm# cli console

4.30. flowcontrol

To set the send or receive flow-control value for an interface, use the command **flowcontrol** in Interface Configuration Mode.

- If flowcontrol send is on for a device and if it detects any congestion at its end, then it notifies the link partner or the remote device of the congestion by sending a pause frame.
- If flowcontrol receive is on for the remote device and it receives a pause frame, then it stops sending any data packets. This prevents any loss of data packets during the congestion period.
- PAUSE is a flow control mechanism that is implied on full duplex Ethernet link segments. The mechanism uses MAC control frames to carry the PAUSE commands.

flowcontrol

```
flowcontrol {send | receive} {on | off | desired}
```

Parameters

Parameter	Type	Description
send		Enter to set the interface to send flow control packets to a remote device.
receive		Enter to set the interface to receive flow control packets from a remote device.
on		Enter for “on” option. If used with “receive”, it allows an interface to operate with the attached device to send flow control packets. If used with “send”, the interface sends flowcontrol packets to a remote device if the device supports it.
off		Enter to turn-off the attached devices (when used with receive) or the local ports (when used with send) ability to send flow-control packets to an interface or to a remote device respectively.
desired		Enter to allow a local port to operate with an attached device that is required to send flow control packets or that may send the control packets, when used with receive option. Allows the local port to send administrative status to a remote device if the remote device supports it, when used with send option

Mode

Interface Configuration Mode

Prerequisites

Interface must first be made administratively down before setting flow control status.

Default

The default flow control for the interfaces are

- flowcontrol receive on
- flowcontrol send on

Examples

iS5comm# (config-if)# flowcontrol send on

4.31. shutdown

To disable a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface, use the command **shutdown** in Interface Configuration Mode. The no form of the command enables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.

shutdown

no shutdown

Mode

Interface Configuration Mode for physical interface / port-channel/tunnel interface/OOB Interface / VLAN Interface Mode for VLAN interface

Prerequisites

- All functions on the specified interface are disabled by the shutdown command
- if OOB interface is enabled, then the Physical Interface eth0 is disabled.
- When the same network interface is used for OOB and NFS mounting, the operation done on OOB will have impact on NFS. For example, when interface eth0 is used for OOB and NFS mounting, executing shutdown command on the OOB interface will make the admin down and the NFS communication will be lost.

Default

- The Physical Interface eth0 is enabled
- The interface VLAN 1 is enabled
- The Port-channel interface is disabled

Examples

iS5comm# (config-if)# shutdown

4.32. debug interface

To set the debug traces for the specified level and severity for all interfaces, use the command **debug interface** in Privileged EXEC Mode. The no form of the command resets the configured debug traces.

debug interface

```
debug interface [track] [enetpktdump] [ippktdump] [arppktdump] [trcerror]
[os] [failall] [buffer] [all {<short (0-7)> | alerts | critical | debugging
| emergencies | errors | informational | notification | warnings}]
```

no debug interface

```
debug interface [track] [enetpktdump] [ippktdump] [arppktdump] [trcerror]
[os] [failall] [buffer] [all]
```

Parameters

Parameter	Type	Description
track		Enter to generate debug messages for all track messages.
enetpktdump		Enter to generate debug messages for Ethernet packet dump messages.
ippktdump		Enter to generate debug messages for IP protocol related packet dump messages.
arppktdump		Enter to generate debug messages for address resolution protocol related packet dump messages.
trcerror		Enter to generate debug messages for trace error messages.
os		Enter to generate debug messages for OS resources. For example, when there is a failure in mem pool creation / deletion, this trace level is used.
failall		Enter to generate debug messages for all failures including packet validation.
buffer		Enter to generate debug messages for buffer trace levels where packet buffer is used.i.e in cases where packet is enqueued .
all		Enter to generate debug messages for buffer trace levels where packet buffer is used.i.e in cases where packet is enqueued .
<short (0-7)>		Enter to generate debug statements for the specified severity level. This value ranges from 0 to 7.
alerts		Enter to generate debug statements for alert messages.
critical		Enter to generate debug statements for critical conditions.
debugging		Enter to generate debug statements for debugging messages.
emergencies		Enter to generate debug statements when system is unusable.
errors		Enter to generate debug statements for error conditions.
informational		Enter to generate debug statements for informational messages.
notification		Enter to generate debug statements for normal but significant messages.
warnings		Enter to generate debug statements for warning conditions.

Mode

Privileged EXEC Mode

Examples

iS5comm# debug interface trcerror critical

4.33. debug-logging

To configure the debug logging option in the system and specifies whether the logging is to be done at console, to a file (system buffer), or through flash, use the command **debug-logging** in Global Configuration Mode. The no form of the command displays debug logs in the console.

debug-logging

```
debug-logging <flash_url> {console | file | flash} [standby]
```

no debug-logging

```
no debug-logging [standby]
```

Parameters

Parameter	Type	Description
<flash_url>		Enter to debug logs in a flash URL
console		Enter to configure debugging logs in console.
file		Enter to debug logs in a flash URL.
flash		Enter to specify that the traces are logged into a file.
standby		Enter for logs in standby node as file or flash.

Mode

Global Configuration Mode

Default

console

Examples

iS5comm(config)# debug-logging flash standby

iS5comm(config)# debug-logging console standby

4.34. rollback

To enable /disable the rollback function, use the command **rollback** in Global Configuration Mode.

rollback

```
rollback {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enter to enable the rollback function.
disable		Enter to disable the rollback function.

Mode

Global Configuration Mode

Default

enable

Examples

iS5comm(config)# rollback enable

4.35. shutdown

To shut down all ports in the corresponding modules and releases all allocated memory, use the command **shutdown** in Global Configuration Mode.

shutdown

```
shutdown {bgp | dot1x | garp | isis | ldp | lldp | ospf | ospf3 |
port-channel | ptp | rsvte | snooping | spanning-tree | split-horizon |
switch-instance-shared-port | ufd | vlan}
```

Parameters

Parameter	Type	Description
bgp		Enter to shut down the Border Gateway Protocol (BGP) module.
dot1x		Enter to shut down the PNAC related configuration.
garp		Enter to shut down the GARP related configuration.
isis		Enter to shut down the ISIS protocol.
ldp		Enter to shut down the LDP protocol.
lldp		Enter to shut down the LLDP related configuration.
ospf		Enter to shut down the Open Shortest Path First (OSPF) module.
ospf3		Enter to shut down the Open Shortest Path First version 3 (OSPFv3) module.
port-channel		Enter to shut down the port channel related configuration.
ptp		Enter to shut down the ptp configuration.
rsvte		Enter to shut down the Resource Reservation Protocol with Traffic Engineering (RSVPTE) module.
snooping		Enter to shut down the snooping related configuration.
spanning-tree		Enter to shut down the Spanning tree related protocol configuration.
split-horizon		Enter to shut down the Split-Horizon related configuration.
switch-instance-shared-port		Enter to shut down the Switch instance shared port related configuration.
ufd		Enter to shut down the UFD related configuration.
vlan		Enter to shut down the VLAN related configuration.

Mode

Global Configuration Mode

Prerequisites

BGP, OSPF, ISIS, RSVPTE, LDP shutdown command implementations are applicable only for stack environment

Examples

iS5comm(config)# shutdown ospf

4.36. start

To start and enable the corresponding modules and allocate the required resources to the corresponding module, use the command **start** in Global Configuration Mode.

start

```
start {bgp | ospf | ospf3 | isis | rsvte | ldp}
```

Parameters

Parameter	Type	Description
bgp		Enter to start and enable the Border Gateway Protocol (BGP) module.
ospf		Enter to start and enable the Open Shortest Path First (OSPF) module.
ospf3		Enter to start and enable the Open Shortest Path First version 3 (OSPFv3) module.
isis		Enter to start and enable the ISIS protocol.
rsvte		Enter to start and enable the Resource Reservation Protocol with Traffic Engineering (RSVPTE) module.
ldp		Enter to start and enable the LDP protocol.

Mode

Global Configuration Mode

Examples

iS5comm(config)# start ospf

4.37. set switch

To set the switch maximum threshold values of RAM, CPU, and Flash, or the maximum and minimum temperature threshold values of the switch in Celsius, or the maximum and minimum threshold values of the switch power supply in volts, use the command **set switch** in Global Configuration Mode.

set switch

```
set switch [<string(15)>] [maximum {RAM | CPU | flash} threshold <percentage
(1-100)>] [temperature {min | max} threshold <celsius ((-15)-35)/(30-40)>]
[power {min | max} threshold <volts (100-230)>]
```

Parameters

Parameter	Type	Description
<string(15)>		Enter a switch name (Example: my-switch)
maximum		Enter to set maximum threshold values of RAM, CPU, and Flash for the switch. When the current resource usage rises above the threshold limit, the SNMP trap message with maximum severity will be sent for the specified resource and the syslog message will be displayed. This threshold value is represented as percentage and ranges between 1 and 100 percent.
RAM		Enter to indicate the maximum RAM usage of the switch in percentage. When the RAM usage crosses the threshold percentage, an SNMP trap with maximum severity will be sent to the manager.
CPU		Enter to indicate the maximum CPU usage of the switch in percentage. When the CPU usage crosses the threshold percentage, an SNMP trap with maximum severity will be sent to the manager.
flash		Enter to indicate the maximum flash usage of the switch in percentage. When the flash usage crosses the threshold percentage, an SNMP trap with maximum severity will be sent to the manager.
threshold		Enter to configure the threshold.
<percentage (1-100)>		Enter to configure the threshold value as percentage. This value ranges from 1 to 100 percents.
temperature		Enter to indicate the maximum and minimum temperature threshold values of the switch in Celsius. When the current temperature drops below the threshold, an SNMP trap with maximum severity will be sent to the manager.
min		Enter to indicate the minimum temperature threshold value for the switch. When the current temperature drops below the threshold, an SNMP trap with maximum severity will be sent to the manager. This threshold value ranges between from -15 to 30 degree Celsius.
max		Enter to indicate the maximum temperature threshold value for the switch. When the current temperature rises above the threshold, an SNMP trap with maximum severity will be sent to the manager. This threshold value ranges between from 30 to 40 degree Celsius
threshold		Enter to configure the temperature threshold.
<celsius ((-15)-35)/(30-40)>		Enter to configure the temperature threshold value in Celsius.

Parameter	Type	Description
power		Enter to indicate the maximum and minimum threshold values of the switch power supply in volts. When the current temperature drops below the threshold, an SNMP trap with maximum severity will be sent to the manager. This threshold value ranges between 100 and 230 V.
min		Enter to indicate the minimum threshold power supply for the switch. When the voltage drops below the threshold, an SNMP trap with maximum severity will be sent to the managerr.
max		Enter to indicate Sets the maximum threshold power suppy for the switch.When the voltage rises above the threshold, an SNMP trap with maximum severity will be sent to the manager.
threshold		Enter to configure the power supply threshold.
<volts (100-230)>		Enter to configure the threshold value in volts.

Mode

Global Configuration Mode

Default

Switch defaults

- RAM - 100%
- CPU - 100 %
- flash - 100%

Temperature

- min - 10 degree Celsius
- max - 40 degree Celsius

Power Supply

- min - 100 V
- max - 230 V

Examples

iS5comm(config)# set switch maximum RAM threshold 98

iS5comm(config)# set switch temperature min threshold -10

iS5comm(config)# set switch temperature max threshold 37

iS5comm(config)# set switch power min threshold 110

iS5comm(config)# set switch power max threshold 220

4.38. hostname

To configure the name of the switch, use the command **hostname** in Global Configuration Mode.

hostname

```
hostname <switchname>
```

Parameters

Parameter	Type	Description
<switchname>		This is a string with maximum size of 15.

Mode

Global Configuration Mode

Examples

iS5comm(config)# hostname switch1

4.39. set designated-uplink

To configure the name of the switch, use the command **set designated-uplink** in UFD Configuration Mode.

set designated-uplink

```
set designated-uplink <ifXtype> {fastethernet <ifnum> | gigabitethernet
<ifnum> | extreme-ethernet <ifnum>} | port-channel <integer <1-65535)>
```

Parameters

Parameter	Type	Description
<ifXtype>		Enter to set the type of interface. The interface can b
fastethernet		Enter for fastethernet. Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
gigabitethernet		Enter for gigabitethernet. A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
extreme-ethernet		Enter for extreme-ethernet. A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
<ifnum>		Enter to set the interface identifier for the specific interface type. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash
port-channel		Enter to set the port-channel for the desiginated-uplinks.
<integer (1-65535)>	Integer	Enter a port channel identifier. This is a unique value that represents the specific port-channel created. This value ranges from 1 to 65535.

Mode

UFD Configuration Mode

Prerequisites

This command executes only if,

- UFD group is configured
- uplink port is added in the group

Examples

iS5comm (config-ufd)# set designated-uplink gigabitethernet 0/6

4.40. mac-learn-rate

To configure the maximum number of unicast dynamic MAC (L2) MAC entries hardware can learn in the system, in a configured time interval, use the command **mac-learn-rate** in Global Configuration Mode. The no form of the command removes the limit on number of unicast MAC entry indications (limit value is set as 0) and resets the configured time interval to default value.

In next subsequent time interval, hardware can learn number of previously learnt MAC entries plus present MAC entries, this cycle will continue until MAC learning reaches to maximum number of L2 unicast dynamic entries learning capacity of the system. If rate limit is changed while timer is running, new rate limit value takes effect on next timer restart. This limit is to control the number of MAC entries indication to control plane from hardware, when hardware MAC learning is enabled. Configuration value '0' disables this feature in the system.

mac-learn-rate

```
mac-learn-rate <no of MAC entries(0-2147483647)> [interval <millisec-
onds(1-100000)>]
```

no mac-learn-rate

Parameters

Parameter	Type	Description
<no of MAC entries(0-2147483647)>		Enter to configure the maximum number of unicast dynamic MAC (L2) entries that can be learned in the switch within the specified time interval. The configured value takes effect on next timer restart if this value is changed while the timer is running. This value is used to control the number of MAC entries indicated to control plane from the hardware, when hardware MAC learning is enabled and ranges from 0 to 2147483647. The value 0 represents that no limit is set in the switch. This limit value does not impose any restrictions on multicast / broadcast and dynamic / static / protocol (MMRP) MAC learning capability limits.
interval		Enter to configure the time interval (in milli-seconds) for maximum number of MAC entries to be learned in the switch. The configured value takes effect from the next timer restart. This value ranges from 1 to 100000 milli-seconds..
<milliseconds(1-100000)>		Enter an interval value. The configured value takes effect from the next timer restart and ranges from 1 to 100000 milli-seconds.

Mode

Global Configuration Mode

Default

This command executes only if,

- <no of MAC entries(0-2147483647)> - 1000
- interval - 1000

Examples

iS5comm (config)# mac-learn-rate 100 interval 500

4.41. ports

To configure the ports for the UFD group, use the command **ports** in UFD Configuration Mode.

ports

```
ports {add | delete} [fastethernet <interface-id> | gigabitethernet <inter-face-id> | Extreme-Ethernet <interface-id> | port channel <port channel ID>] counters
```

Parameters

Parameter	Type	Description
add		Enter to add ports to the UFD group.
delete		Enter to delete ports from the UFD group.
Gigabitethernet		Enter to set to gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to set to Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links.
fastethernet		Enter to set to fastethernet type of interface. Fast Ethernet is officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
port-channel		Enter to set to port channel interface. This is a logical interface that represents an aggregator which contains several ports aggregated together.
<port channel ID>	Integer	Enter a number for port channel ID. The range is from 1 to 65535.

Mode

UFD Configuration Mode

Prerequisites

This command executes only if UFD group is configured.

Examples

iS5comm (config-ufd)# ports add gigabitethernet 0/1

4.42. set port-role

To configure the ports for the UFD group, use the command **set port-role** in Interface Configuration Mode.

set port-role

```
set port-role {uplink [designated] | downlink}
```

Parameters

Parameter	Type	Description
uplink		Enter to set the port role for an interface as uplink.
designated		Enter to set the port role for an interface as designated uplink.
downlink		Enter to set the port role for an interface as downlink

Mode

Interface Configuration Mode

Examples

iS5comm (config-if)# set port-role uplink

4.43. clear interfaces

To clear current interface counters for all interfaces or for only specific interface types and numbers, use the command **clear interfaces** in Global Configuration Mode. When used in Privileged EXEC Mode, the command can be used to clear port channel interface counters as well.

clear interfaces

```
clear interfaces [gigabitethernet <interface-id> | Extreme-Ethernet <inter-
face-id>] counters
```

When used in Privileged EXEC Mode

clear interfaces

```
clear interfaces [gigabitethernet <interface-id> | Extreme-Ethernet <inter-face-id>] [port channel <port channel ID>] counters
```

Parameters

Parameter	Type	Description
Gigabitethernet		Enter to clear gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to clear Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
counters		Enter to clear all interface counters
port-channel		Enter to clear port channel interface.
<port channel ID>	Integer	Enter a number for port channel ID. The range is from 1 to 65535.

Mode

Privileged EXEC Mode / Global Configuration Mode

Examples

iS5comm# clear interfaces counters

iS5comm# clear interfaces port-channel 1 counters

iS5comm(config)# clear interfaces counters

iS5comm(config)# clear interfaces gigabitethernet 0/1 counters

4.44. clear counters

To clear current interface counters for all interfaces or for only specific interface types and numbers, use the command **clear counters** in Global Configuration Mode. When used in Privileged EXEC Mode, the command can be used to clear port channel interface counters as well.

clear counters

```
clear counters [gigabitethernet <interface-id> | Extreme-Ethernet <inter-face-id>] counters
```

When used in Privileged EXEC Mode

clear interfaces

```
clear counters [fastethernet <interface-id> | gigabitethernet <interface-id> | Extreme-Ethernet <interface-id>] [port channel <port channel ID>] counters
```

Parameters

Parameter	Type	Description
Gigabitethernet		Enter to clear gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to clear Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
fastethernet		Enter to clear fastethernet type of interface. Fast Ethernet is officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
counters		Enter to clear all interface counters
port-channel		Enter to clear port channel interface.
<port channel ID>	Integer	Enter a number for port channel ID. The range is from 1 to 65535.

Mode

Privileged EXEC Mode / Global Configuration Mode

Examples

iS5comm# clear counters

iS5comm# clear counters port-channel 1

iS5comm(config)# clear counters

iS5comm(config)# clear interfaces gigabitethernet 0/1

4.45. show ip interface

To display the IP interface configuration, use the command **show ip interface** in Privileged EXEC Mode.

show ip interface

```
show ip interface [vlan <vlan-id(1-4094>] [switch default]] [gigabitethernet
<interface-id>] [Extreme-Ethernet <interface-id>] [loopback <loopback ID
(1-1000>] [vlan-counters]
```

Parameters

Parameter	Type	Description
vlan		Enter to display the IP interface configuration for the specified VLAN ID.
<vlan-id(1-4094)>		Enter a specific VLAN ID. This is a unique value that represents the specific VLAN created that ranges from 1 to 4094.
switch default		Enter to specify default switch.
Gigabitethernet		Enter to display gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to display the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
loopback		Enter to display the IP interface configuration for the specified loopback ID.
<loopback-id(0-100)>	Integer	Enter a specific loopback ID. This is a unique value that represents the specific loopback created that ranges from 0 to 100.
vlan-counters		Enter to display VLAN counters related configuration.

Mode

Privileged EXEC Mode

Examples

iS5comm# show ip interface vlan 1

```
vlan1 is up, line protocol is up
Internet Address is 192.168.10.1/24
Broadcast Address  192.168.10.255
Vlan counters disabled
```

4.46. show authorized-managers

To display the configured authorized managers' related information available in the switch, use the command **show authorized-managers** in Privileged EXEC Mode.

show authorized-managers

```
show authorized-managers [ip-source <ip_addr>]
```

Parameters

Parameter	Type	Description
ip-source		Enter to display a Network or Host address
<ip_addr>	A.B.C.D	Enter an IP Address for a network or host

Mode

Privileged EXEC Mode

Examples

iS5comm# show authorized-managers

```
    Ip Authorized Manager Table
    ---------------------------
    Ip Address       : 12.0.0.1
    Ip Mask          : 255.255.255.255
    Services allowed : ALL
    Ports allowed    : Gi0/1
    On cpu0         : Deny
    Vlans allowed    : All Available Vlans
```

4.47. show interfaces

To display the interface status and configuration, use the command **show interfaces** in Privileged EXE Mode.

show interfaces

```
show interfaces
 [<interface-type> <interface-id>] etherchannel
```

```
 | [{[<interface-type> <interface-id>] [{description |storm-control | flow-
control | capabilities | status |port-security-state |rate-limit}] | {vlan
<vlan_vfi_id> | [{switch <switch-name>}] }| tunnel <tunnel ID (1-128)>}]

 |[bridge port-type [{port-channel <port-channel ID(1-65535)>] <inter-
face-id> <ifnum> | pw <integer (1-65535)>] [s-channel <integer(1-65535)>]]

 | configuration hardware

 | hardware

 | [mtu {vlan <vlan_vfi_id> [{switch <switch-name>}] | port-channel
<port-channel ID(1-65535)>] | <interface-type> <interface-id>}]

 | port-role

 | redundant {[<number (1-8)>] {config | node-table | proxy-node-table | map
| quad-box | quad-box-table}}

 [counters [gigabitethernet <interface-id>]

 | statistics

 | transceivers

 | {counters |HC-counters [{ppp <PPP-id range (1-4094)>] | <interface-type>
<interface-id>] [Extreme-Ethernet <interface-id>] | {vlan <vlan_vfi_id> |
[{switch <switch-name>}] }| tunnel <tunnel ID (1-128)>}] | redundant
{[<number (1-8)>] | CPU}]
```

Parameters

Parameter	Type	Description
<interface-type>		• Enter Gigabitethernet to display gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • Enter Extreme-Ethernet to display the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex link
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
etherchannel		Enter to display the interface specific port-channel information
description		Enter to display the interface description.
storm-control		Enter to display the broadcast, multicast, and unicast storm control suppression levels for the specified interface.
flowcontrol		Enter to display the flow control related statistics information for the specified interface.
capabilities		Enter to display the interface type, interface speed, duplex operation and flow control status for the specified interface.
status		Enter to display the status, duplex details, speed and negotiation mode of the specified interface.
port-security-state		Enter to display the state of the port security option.
rate-limit		Enter to display the rate limit burst size and rate-limit value of the interface.
vlan		Enter to display the IP interface configuration for the specified *VLAN* ID.
<vlan-id(1-4094)>		Enter a specific *VLAN* ID. This is a unique value that represents the specific *VLAN* created that ranges from 1 to 4094.
switch		Enter to display by switch name.
<switch-name>	Integer	Enter a specific switch name.
tunnel		Enter to display Tunnel interface configuration

Parameter	Type	Description
<tunnel IP (1-128)>	Integer	Enter a specific tunnel ID. The range is from 1 to 128.
bridge port-type		Enter to display the bridge port type of interfaces.
port-channel		Enter to display the port channel interfaces.
<port-channel ID(1-65535)>		Enter a specific port channel ID that ranges from 1 to 65535.
bridge port-type		Enter to display the bridge port type of interfaces.
port-channel		Enter to display the port channel interfaces.
<port-channel ID(1-65535)>		Enter a specific port channel ID that ranges from 1 to 65535.
pw		Enter to display the pseudo wire interface.
<pw range(1-255)>		Enter a specific pw ID that ranges from 1 to 255.
s-channel		Enter to display the s-channel interfaces.
<s-channel ID(1-65535)>		Enter a specific s-channel ID that ranges from 1 to 65535.
configuration		Enter to display the configuration-related statistics information for the specified interface.
hardware		Enter to display the hardware-related statistics information for the specified interface.
mtu		Enter to display the Maximum Transmission Unit (*MTU*) of interfaces in the switch.
port-role		Enter to display the interface port role configuration details and detailed information of *UFD* mapped in the interface.
redundant		Enter to display the *HSR-PRP* redundancy-related configuration.
<number (1-8)>		Enter to display the configuration for a specific number *RED*.
config		Enter to display the hsp-prp specific configuration.
node-table		Enter to display the node table information.
proxy-node-table		Enter to display the proxy node table information.
map		Enter to display the mapping of physical and logical ports.
quad-box		Enter to display the quad-box configuration.
quad-box-table		Enter to display the Quad-Box node table information.

Parameter	Type	Description
counters		Enter to display the counter statistics for specified interface.
statistics		Enter to display the *UFD* global configuration details.
transceivers		Enter to display the transceiver related live diagnostic information
HC-counters		Enter to display the HC interface counters related information
ppp		Enter to display the Protocol Packet Processing (*PPP*) interface related configuration
<PPP-id range (1-4094)>	Integer	Enter a specific *PPP* ID. The range is from 1 to 4094.
CPU		Enter to display information for the port related to the CPU.

Mode

Privileged EXEC Mode

Examples

iS5comm# show interfaces gigabitethernet 0/1

```
    Gi0/1 up, line protocol is up (connected)
    Bridge Port Type: Customer Bridge Port
    Interface SubType: Gigabit Ethernet
    Interface Alias: interface1
    Hardware Address is 00:03:02:03:04:01
    MTU  200 bytes,
    Error in Duplex status
    100 Mbps,  Auto-Negotiation
    HOL Block Prevention disabled.
    CPU Controlled Learning disabled.
    Auto-MDIX on

    Link Up/Down Trap is enabled

    Reception Counters
    Octets                    : 0
    Unicast Packets           : 0
    Multicast Packets         : 0
    Broadcast Packets         : 0
```

```
Discarded Packets         : 0
Error Packets             : 0
Unknown Protocol          : 0

Transmission Counters
Octets                    : 158406
Unicast Packets           : 0
Multicast Packets         : 1702
Broadcast Packets         : 0
Discarded Packets         : 0
Error Packets             : 0
```

iS5comm # show interfaces port-role

```
Gi0/1       Downlink
Gi0/2       Downlink
Gi0/3       Downlink
Gi0/6       Uplink
vlan1       Uplink
```

iS5comm # show interfaces statistics

```
Interface    DownlinkEnabledCount DownlinkDisabledCount
Gi0/1                         1                   1
Gi0/2                         0                   0
Gi0/3                         0                   0
Ex0/1                         0                   0
Ex0/2                         0                   0
Ex0/3                         0                   0
Ex0/4                         0                   0
vlan1                         0                   0
```

iS5comm # show interfaces status

```
Port        Status           Duplex   Speed       Negotiation
Capability
----        ------           ------   -----       ----------- ----------
Gi0/1       not connected    -        -           Auto Auto-MDIX on
Gi0/2       not connected    -        -           Auto Auto-MDIX on
Gi0/3       not connected    -        -           Auto Auto-MDIX on
Gi0/4       connected        Full     1 Gbps      Auto Auto-MDIX on
Gi0/5       not connected    -        -           Auto Auto-MDIX on
Gi0/6       not connected    -        -           Auto Auto-MDIX on
Gi0/7      not connected    -       -         Auto Auto-MDIX onGi0/8
not connected    -        -           Auto Auto-MDIX on
Gi0/9(I)    admin down       -        -           Auto Auto-MDIX on
```

```
Gi0/11(I)    admin down       -        -           Auto Auto-MDIX on
Red3
Red3A       not connected    -        -           Auto Auto-MDIX on
Red3B       not connected    -        -           Auto Auto-MDIX on
Red4
Red4A       not connected    -        -           Auto Auto-MDIX on
Red4B       not connected    -        -           Auto Auto-MDIX on
```

4.48. show system-specific port-id

To display the custom-parameters configurations, use the command **show system-specific port-id** in Privileged EXEC Mode.

show system-specific port-id

```
show system-specific port-id
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show system-specific port-id

```
Interface PortID
--------------------------
Slot0/1   45
```

4.49. set custom-param

To configure the custom parameters for a particular port, use the command **set custom-param** in Interface Configuration Mode. The no form of the command deletes the custom parameter configuration.

set custom-param

```
set custom-param {type <integer> | length <integer> | value <string>} |
attribute <integer (1-4)> | value <integer (0-4294967295)>}
```

no set custom-param

```
no set custom-param [type <integer>] [attribute <integer (1-4)]
```

Parameters

Parameter	Type	Description
`type`		Enter to set the type of TLV information.
`integer`	Integer	Enter a specific TLV information type value.
`length`		Enter to set the length of TLV information.
`integer`	Integer	Enter a specific TLV information length value.
`value`		Enter to set the value of TLV information.
`string`		Enter a specific TLV information value
`attribute`		Enter to set the opaque attribute ID configured on the port.
`integer (1-4)`	Integer	Enter a specific opaque attribute ID. This value ranges from 1 to 4.
`value`		Enter to set the value for the Opaque attribute.
`integer (0-4294967295)`	Integer	Enter a specific Opaque attribute value. This value ranges from 0 to 4294967295.

Mode

Interface Configuration Mode

Default

value -0

Examples

iS5comm (config-if)# set custom-param attribute 2 value 40

4.50. show custom-param

To display the custom-parameters configurations, use the command **show custom-param** in Privileged EXEC Mode.

show custom-param

```
show custom-param
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show custom-param

```
Slot0/1
AttrID    AttrValue
--------  --------
4         5454
Slot0/2
AttrID    AttrValue
--------  --------
2         2424
Type      Length    Value
--------  --------  --------
2         4         root
5         4         root
```

4.51. show env

To display the configured authorized managers' related information available in the switch, use the command **show env** in Privileged EXEC Mode.

show env

```
show env {all | temperature | RAM | CPU | flash | power}
```

Parameters

Parameter	Type	Description
all		Enter to display the threshold information of all resources such as CPU, Flash, RAM, power and temperature
temperature		Enter to display temperature threshold values of the switch in Celsius
RAM		Enter to display maximum RAM usage of the switch in percentage
CPU		Enter to display maximum CPU usage of the switch in percentage
flash		Enter to display the maximum flash usage of the switch in percentage
power		Enter to display power suply(ies) for the switch

Mode

Privileged EXEC Mode

Examples

iS5comm# show env all

```
    CPU Threshold                    : 80%
    Current CPU Usage                : 3%
    RAM Threshold                    : 80%
    Current RAM Usage                : 37%
    Flash App Threshold              : 80%
    Flash Dedicated for App          : 95%
    Dedicated Flash Usage by App     : 19%
    Flash Size                       : 8GByte
    Power Supply 1 Presence          : Uknown
    Power Supply 2 Presence          : Uknown
    Switch Thermal Limit             : 85C
    Switch High Threshold            : 80C
    Switch Low Threshold             : -35C
    Switch Current Temperature       : 36C
    Core Temperature                 : 58C
    Line Module 1 Temperature        : 42C
    Line Module 2 Temperature        : 45C
```

```
    Line Module 3 Temperature          : 39C
    Line Module 4 Temperature          : 37CMgmt Port Routing
    : Disabled
```

4.52. show system

To display the configured authorized managers' related information available in the switch, use the command **show system** in Privileged EXEC Mode.

show system

```
show system {acknowledgement | information | port-id}
```

Parameters

Parameter	Type	Description
acknowledgement		Enter to display acknowledgment for open sources used in the system
information		Enter to display the system informaion
port-id		Enter to custom-parameters configuration

Mode

Privileged EXEC Mode

Examples

iS5comm# show system acknowledgement

```
    Product Name: U-Boot 2016.09
    License     : GPLv2
    Description : U-Boot Boot Loader

    Product Name: NXP SDK v2.0-1703
    License     : GPLv2
    Description : Linux Drivers, Linux Kernal-4.1.3

    Product Name: OpenSSL v1.1.1
    License     : OpenSSL License and the original SSLeay license
    Description : OpenSSL is a toolkit for the Transport Layer Security an
```

```
 Secure Sockets Layer protocols.

Product Name: libssh v0.8.90
License     : LGPL
Description : Multiplatform C library implementing the SSHv2 protocol on
 client and server side

Product Name: Marvell CPSS v4.1.622 Components
License     : GPLv2
Description : Buildroot and Patches Linux cross compilation tool.
```

iS5comm# show system information

```
iBiome Software Version          : 1.3.01A17
Model Name                       : N\A
Serial Number                    : N\A
Factory Name                     : iMX350
Factory Version                  : 1531-0001-B02
Factory Sub revision             : 001
Factory S/N                      : 1531-0001-B02-30-18-13
Line Module 1 Name               : iRM-8GSFP
Line Module 1 Version            : 1531-0001-A01.001
Line Module 2 Name               : iRM-8GRJ45
Line Module 2 Version            : 1531-0009-A01.001
Line Module 3 Name               : iRM-8PGRJ45
Line Module 3 Version            : 1531-0004-A02.001
Line Module 4 Name               : iRM-TGSFP
Line Module 4 Version            : 1531-0003-B01.001
Primary Software Version         : 9.2.9
FPGA Firmware Version            : 3.15
UBoot Software Version           : U-Boot 2016.09 ver 1.30
Linux Software Version           : Linux iS3000 Local version v1.20
CPLD Version                     : N\A
PSM Version                      : N\A
Switch Name                      : iS5com
Prompt Name                      : iS5comm
Banner Name                      : RAPTOR iBiome OS
System Contact                   : iS5com
System Name                      : iS5com
System Location                  : iS5com
Logging Option                   : Console Logging
```

```
Device Uptime                    : 2 Days, 11 Hrs, 3 Mins, 50 Secs
Login Authentication Mode        : Local
Config Save Status               : Not Initiated
Remote Save Status               : Not Initiated
Config Restore Status            : Not Initiated
Traffic Separation Control       : none
```

4.53. show flow-control

To display the flow-control information, use the command **show flow-control** in Privileged EXEC Mode.

show flow-control

```
show flow-control [interface {gigabitethernet <interface-id>]
[Extreme-Ethernet <interface-id>] [port-channel <port-channel ID
(1-65535)>]}
```

Parameters

Parameter	Type	Description
interface		Enter to display the protocol-specific configuration of the interface.
Gigabitethernet		Enter to display gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to display the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
port-channel		Enter to display the IP interface configuration for the specified loopback ID
<port-channelID (1-65535)>	Integer	Enter a specific port-channel ID. This is a unique value that represents the specific loopback created that ranges from 0 to 65535.

Mode

Privileged EXEC Mode

Examples

iS5comm# show flow-control Interface gigabitethernet 0/1

```
Port    Admin    Oper     Tx Pause   Rx Pause   HC TxPause     HC RxPause
Tx   Rx  Tx   Rx
----    -------  -------  --------   --------   ---------- ----------
Gi0/1   off off  on  off  0          0          0              0
```

4.54. show debug-logging

To display the debug logs stored in file or the standby lob file, use the command **show debug-logging** in Privileged EXEC Mode.

show debug-logging

```
show debug-logging [standby]
```

Parameters

Parameter	Type	Description
standby		Enter to display the standby log file.

Mode

Privileged EXEC Mode

Examples

iS5comm# show debug-logging standby

```
Creating log file fsir.log.4693
iS5comm# show debug-logging standby
% File does not exist
```

4.55. show debugging

To display the state of each debugging option, use the command **show debugging** in Privileged EXEC Mode.

show debugging

```
show debugging
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show debugging

```
LLDP :
LLDP critical debugging is on
```

4.56. show clock

To display the system date and time, use the command **show clock** in Privileged EXEC Mode.

show clock

```
show clock
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show clock

```
Mon Jan 20 23:54:44 2020 (UTC +00:00)
```

4.57. show running-config

To display the configuration information currently running on the router, the configuration for a specific interface, or map class information and this configuration is lost if the system is restarted, use the command **show running-config** in Privileged EXEC Mode. The command is useful when there are multiple interfaces and you want to look at the configuration of a specific interface

show running-config

Mode

Privileged EXEC Mode

Examples

iS5comm# show running config ?

```
<CR>                                    Command to enable or disable
memtrace
<CR>                    Displays the currently operating
configuration in the system
<CR>                                    show memtrace
Openflow                                Client related configuration
acl                                     ACL related configuration
alarm                                   alarm related configuration
beep-server                             BEEP-SERVER related configuration
bfd                                     BFD related configuration
bgp                                     BGP related configuration
clkiwf                                  CLKIWF related configuration
cn                                      CN related configuration
cru                                     Common routing utilities
dcbx                                    DCBX related configuration
dhcp                                    DHCP related configuration
dhcp6                                   DHCP6 related configuration
disable                                 Disable memtrace
dns                                     DNS related configuration
dsmon                                   DSMON related configuration
dvmrp                                   DVMRP related configuration
ecfm                                    ECFM related configuration
elmi                                    ELMI related configuration
elps                                    ELPS related configuration
enable                                  Enable memtrace
entity-mib                              ENTITY-MIB related configuration
eoam                                    EOAM related configuration
erps                                    ERPS related configuration
firewall                                FIREWALL related configuration
fm                                      FM related configuration
fsb                                     FSB related configuration
hb                                      Heartbeat related configuration
hs                                      HS related configuration
http                                    HTTP related configuration
icch                                    ICCH related configuration
igmp                                    IGMP related configuration
igmp-proxy                              IGMP-PROXY related configuration
igs                                     IGS related configuration
interface                               Interface related configuration
ip                                      IP related configuration
ipsourceguard                           IPSOURCEGUARD related configuration
```

```
ipv6                    IPv6 related configuration
isis                    ISIS related configuration
l2dhcsnp                L2Dhcsnp related configuration
la                      LA related configuration
lldp                    LLDP related configuration
mbsm                    MBSM related configuration
mef                     MEF related configuration
mempool                 Mempool related information
memtrace                Memtrace related information
mld                     MLD related configuration
mlds                    MLD Snooping related configuration
mpls                    MPLS related configuration
msdp                    MSDP related configuration
msdpv6                  MSDPV6 related configuration
nat                     NAT related configuration
network-clock           network-clock related configuration
ospf                    OSPF related configuration
ospf3                   OSPF3 related configuration
ospfte                  OSPFTE related configuration
pbb                     PBB related configuration
pim                     PIM related configuration
pimv6                   PIMV6 related configuration
pnac                    PNAC related configuration
poe                     POE related configuration
ppp                     PPP related configuration
ptp                     PTP related configuration
qosxtd                  QOSXTD related configuration
radius                  Radius related configuration
rbridge                 RBridge related configuration
rip                     RIP related configuration
rip6                    RIP6 related configuration
rm                      RM related configuration
rmon                    RMON related configuration
route-map               ROUTE-MAP related configuration
rsna                    RSNA related configuration
snmp                    SNMP related configuration
sntp                    SNTP related configuration
split-horizon           Split-Horizon related configuration
ssh                     SSH related configuration
ssl                     SSL related configuration
```

```
status                                  Memtrace status
stp                                     STP related configuration
switch                                  Switch related configuration
syslog                                  Syslog related configuration
system                                  System related configuration
tac                                     TAC related configuration
tacacs                                  TACACS related configuration
tlm                                     TLM related configuration
ufd                                     Uplink Failure Detection(UFD)
related configuration
vlan                                    VLAN related configuration
vrrp                                    VRRP related configuratio
wss                                     WSS related configuration
```

iS5comm# show running-config

```
#Building configuration...
!
!
syslog localstorage
syslog relay
syslog filename-one "is5"
logging local flash emergencies file is5
logging local flash alerts file is5
!
!
interface gigabitethernet 0/1
!
interface gigabitethernet 0/2
!
interface gigabitethernet 0/3
!
set banner-name "RAPTOR iBiome OS"
system contact "iS5com"
system name "iS5com"
system location "iS5com"
username root password xxxxxxxx privilege 16
username guest password xxxxxxxx privilege 1
!
end
```

4.58. show health status

To display the device's health status and error reasons, use the command **show health status** in Privileged EXEC Mode.

This command displays the device's health status and error reason. The list of health-check status for device is as follows:

- upAndRunning - Indicates that device is up and running.
- downNonRecoverableErr - Indicates that the health status of device is down due to occurence of some critical error.
- upRecoverableRuntimeErr - Indicates that the health status of device is up but indicates the occurence of a runtime error that is recoverable.

The list of error reasons for is as follows;

- None - Indicates no errors
- nonRecovTaskInitializationFailure - Indicates the occurence of non-recoverable failure during Task initialization.
- nonRecovInsufficientStartupMemory - Indicates that there is insufficient memory for successful startup. This error is non-recoverable and requires sufficient memory to be available in the system for successful device startup.
- recovCruBuffExhausted - Indicates that CRU Buffer Exhausted.
- recovConfigRestoreFailed - Indicates that config-restore failed. This is a recoverable error.
- recovProtocolMemPoolExhausted - Indicates that a mem-pool associated with a specific module in the device has drained out. This error may affect the functioning of the specific protocol alone and is treated as a recoverable error

show health status

Mode

Privileged EXEC Mode

Examples

iS5comm# show health status

```
    SWITCH HEALTH STATUS--------------------------------
```

4.59. show mac-learn-rate

To display the maximum number of unicast dynamic MAC (L2) MAC entries hardware can learn in the system, in MAC learning limit rate interval, use the command **show mac-learn-rate** in Privileged EXEC Mode.

show mac-learn-rate

```
show mac-learn-rate
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show mac-learn-rate

```
    Switch MAC Learn Limit Rate :  100
     Switch MAC Learn Limit Rate Interval: 1000
```

4.60. set timer speed

To configure the system timer speed, use the command **set timer speed** in Global Configuration Mode.

set timer speed

```
set timer speed <timer-speed(1-1000)>
```

Parameters

Parameter	Type	Description
<timer-speed(1-1000)>	Integer	Enter a value for the timer. This value ranges from 1 to 1000.

Mode

Global Configuration Mode

Examples

iiS5comm(config)# set timer speed 100

4.61. audit-logging

Audit logging uses Syslog platform as tools to send/store Audit logs. So for allowing the Audit-logging to work, the Syslog should configured and working. Audit-logging uses configuration, supported by Syslog. Audit logging provides two ways to save audit messages: local and remote. Both ways work independently between each other. Both local and remote logging are disabled by default.

audit-logging

```
audit-logging { [ local [ enable | filename <string(128)> ] | remote [ enable |
[ipv4-address <ip_addr>] [port <integer(1-65535)>] [{ tcp | udp | tls}] ] }
```

Parameters

Parameter	Type	Description
local enable		enable the local audit-logging
local filename <string (128)>		set the local audit-logging file name
remote enable		enable the remote audit-logging
remote [ipv4-address <ip_addr>] [port <integer(1-65535)>] [{ tcp | udp | tls}]		set the remote server parameters

Mode

Global Configuration Mode

Examples

Audit messages are saved to the local file, which can be default file or user defined file.

Local file name can not be changed if the local audit-logging enabled.

The way to change the file name is:

1) disable the local audit-logging (if enabled)
2) change the file name
3) enable the local audit-logging (if required)

Example

iS5comm(config)# no audit-logging local

iS5comm(config)# audit-logging local filename LOCAL_FILE.txt

iS5comm(config)# audit-logging local enable

Default paramters:

1. local logging status: disabled

2. local file name is “audit.txt”

Remote Logging Example

Remote audit-logging is done by sending the audit messages to the remote server by tcp or udp protocol.

To enable the remote audit logging user should configure the server ip , port and protocol first.

The way to change the server parameters is:

1) disable the remote audit-logging (if enabled)
2) To enable TLS use the “**secure logging crypto key**” command.
3) change the remote server parameters
4) enable the remote audit-logging (if required)

iS5comm(config)# no audit-logging remote

iS5comm(config)# audit-logging remote ipv4-address 192.168.0.100 port 5000 tls

iS5comm(config)# audit-logging remote enable

iS5comm(config)#

NOTE: To enable TLS protocol, the certificates should be present

Default parameters:

1) remote logging status: disabled
2) remote server ipv4 address: NOT_VALID (0.0.0.0)
3) remote server tcp/udp port number: 514
4) remote server tls port number: 6514
5) protocol: udp

Disabling Audit-Logging

iS5comm(config)# no audit-logging remote

iS5comm(config)# no audit-logging local

Seeing all available local files including current

All audit-logging files can be shown by “show audit-logging loglist”

example:

iS5comm# show audit-logging loglist

Audit Directory name: /mnt/log/audit/Name: audit.txt , Size: 0 , Updated: Wed Nov 6 03:12:05 2019Name: audit_new.txt , Size: 152 , Updated: Wed Nov 6 20:42:48 2019iS5comm#

Seeing content of the local file

Content of the current local audit file can be shown by the “show audit-logging” command.

example:

iS5comm# show audit-logging file

To view a specific number of lines:

iS5comm# show audit-logging file lines 3

To view a specific audit log file

iS5comm# show audit-logging file audit.txt lines 3

Viewing the audit logging configuration

example:

iS5comm# show audit-logging config

Audit Local Status : Enabled

Audit Local File : audit_new.txt

Audit Remote Status : Enabled

Audit Remote Config : tcp, 192.168.0.100:5000

iS5comm#

4.62. show audit-logging

Audit logging uses Syslog platform as tools to send/store Audit logs. So for allowing the Audit-logging to work, the Syslog should configured and working. Audit-logging uses configuration, supported by Syslog. Audit logging provides two ways to save audit messages: local and remote. Both ways work independently between each other. Both local and remote logging are disabled by default.

show audit-logging

```
show audit-logging [ config | file [ lines <integer(1-65535)> ] ]
```

Parameters

Parameter	Type	Description
config		show the current local and remote status and configuration
file [lines <integer(1-65535)>]		show the content of the local audit-logging file, default number of lines: 20

Mode

Privileged Exec Mode

Examples

Content of the local audit file can be shown by “show command”

Example

iS5comm# show audit-logging file

<134>Jul 27 02:19:52 ISS[2102]: AUDIT : admin audit-logging local enable #012 SUCCESS CONSOLE

<134>Jul 27 02:22:53 ISS[2102]: AUDIT : admin Idle Timer expired, Logging out ...! SUCCESS CONSOLE

<134>Jul 27 02:26:35 ISS[2102]: AUDIT : Attempt to login as admin via console Succeeded

<134>Jul 27 02:26:35 ISS[2102]: AUDIT : admin Logging in ...! SUCCESS CONSOLEiS5comm#

user can choose to see specific number of lines:

iS5comm# show audit-logging file lines 3<134>Jul 27 02:26:35 ISS[2102]: AUDIT : admin Logging in ...! SUCCESS CONSOLE<134>Jul 27 02:28:25 ISS[2102]: AUDIT : admin show audit-logging file #012 SUCCESS CONSOLEiS5comm#

4.63. shutdown ufd

To disable Uplink Failure Detection (UFD) feature in the system, use the command **shutdown ufd** in Global Configuration Mode. The no form of the command enables UFD feature in the system.

shutdown ufd

no shutdown ufd

Mode

Global Configuration Mode

Examples

iS5comm (config)# no shutdown ufd

4.64. set ufd

To enable or disable Uplink Failure Detection (UFD) feature in the system, use the command **set ufd** in Global Configuration Mode.

set ufd

```
set ufd {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enter to enable UFD.
disable		Enter to disable UFD

Mode

Global Configuration Mode

Examples

iS5comm(config)# set ufd enable

4.65. ufd group

To configure a UFD group that is identified by the group ID, use the command **ufd group** in Global Configuration Mode. Each group has uplink interfaces to monitor and downlink interfaces to disable.

ufd group

```
ufd group <integer(1-65535)> [groupname <string(32)>]
```

no ufd group

```
no ufd group <integer(1-65535)> [groupname <string(32)>]
```

Parameters

Parameter	Type	Description
<integer(1-65535)>		Enter a group ID for the UFD group. This value ranges from 1 to 65535.
groupname		Enter to add a group name.
<string(32)>		Enter configure the name of the UFD group. This groupname is a string of maximum size 32. Note that the groupname should be only characters - no numerals allowed.

Mode

Global Configuration Mode

Examples

iS5comm(config)# no shutdown ufd

iS5comm(config)# set ufd enable

iS5comm(config)# ufd group 2 groupname group

iS5comm(config-ufd)

4.66. internal-lan

To add an internal LAN interface and its parameters, use the command **internal-lan** in Global Configuration Mode. The no form of the command deletes the internal LAN interface.

internal-lan

```
internal-lan <ilan-id (1-65535)> [add interface virtual <iface_list> |
delete interface virtual <iface_list>]
```

no internal-lan

```
no internal-lan <ilan-id (1-65535)>
```

Parameters

Parameter	Type	Description
`<ilan-id (1-65535)>`	Integer	Enter to specify the internal LAN ID. This value ranges from 1 to 65535.
`add interface virtual`		Enter to add the internal LAN interface and its parameters. Specifies the virtual interface.
`<iface_list>`		Enter to enable UFD.
`delete interface virtual`		Enter to delete the internal LAN interface and its parameters.

Mode

Global Configuration Mode

Prerequisites

This command executes only if virtual interface is created in the system.

Examples

iS5comm(config)# internal-lan 1 add interface virtual 1

4.67. show internal-lan

To display the internal LAN parameters, use the command **show internal-lan** in Privileged EXEC Mode.

show internal-lan

```
show internal-lan <iface_list>
```

Parameters

Parameter	Type	Description
<iface_list>	A.B.C.D	Enter an IP Address for a network or host

Mode

Privileged EXEC Mode

Prerequisites

This command executes only if virtual interface is created in the system.

Examples

iS5comm# show internal-lan 1

```
    Intra Bridge Connections
    -------------------------------
    I-LAN : internal-lan1
    Switch :        Port : virtual1         Bridge Port Type: Customer
    Bridge Port
```

4.68. show iftype protocol deny table

To display the entries of iftype protocol deny table, use the command **show iftype protocol deny table** in Privileged EXEC Mode.

show iftype protocol deny table

```
show iftype protocol deny table [switch default]
```

Parameters

Parameter	Type	Description
switch default		Enter to displays iftype for the specified context. This value is default.

Mode

Privileged EXEC Mode

Prerequisites

This command executes only if virtual interface is created in the system.

Examples

iS5comm# show iftype protocol deny table

```
Switch default
IfType                BridgePortType       Protocol
-------------------------------------------------
Pip                 PropCustomerEdgePortlldp
Pip                 PropCustomerEdgePortqos
Pip                 CustomerBackbonePortecfm
Pip                 CustomerBackbonePortbridge
```

4.69. login block-for

To configure the maximum number of successful login attempts and the lock out time to block the user, use the command **login block-for** in Global Configuration Mode.

login block-for

```
login block-for <seconds(30-600)> attempts <tries(1-10)>
```

Parameters

Parameter	Type	Description
<seconds(30-600)	Integer	Enter to specify the lock out time in seconds for which a user is blocked following unsuccessful logins. This value ranges from 30 to 600
attempts		Enter to configure number of login attempts.
<tries(1-10)>	Integer	Enter to configure login attempts. This is the number of times a user is allowed to login using wrong password in the login prompt. This value ranges from 1 to 10.

Mode

Global Configuration Mode

Defaults

- seconds - 30
- tries - 3

Examples

iS5comm(config)# login block-for 60 attempts 4

4.70. show ufd

To display the detailed UFD configuration, use the command **show ufd** in Privileged EXEC Mode.

show ufd

```
show ufd [brief] [group <integer(1-65535)>]
```

Parameters

Parameter	Type	Description
brief		Enter to display the related UFD configuration.
group		Enter to display the UFD configurations of the specified UFD group.
<integer(1-65535)>	Integer	Enter a group identifier. The range is from 1 to 65535.

Mode

Privileged EXEC Mode

Examples

iS5comm# show ufd group 2

```
    UFD Configurations
    ------------------
    UFD Status : Enabled
    Group Id: 2
    Group Name: group
    Group Status : UP
    Designated Uplink Port : Gi0/6
```

```
Interface   Role                UFD Status
---------   ----                ----------
Gi0/1       Downlink            Up
Gi0/6       Uplink              Up
```

4.71. feature telnet

To enable the Telnet service in the system, use the command **feature telnet** in Global Configuration Mode. The no form of the command disables the Telnet service.

feature telnet

no feature telnet

Mode

Global Configuration Mode

Default

Enabled

Examples

iS5comm (config)# feature telnet

4.72. show telnet server

To display the Telnet server status, use the command **show telnet server** in Privileged EXEC Mode.

show telnet server

Mode

Privileged EXEC Mode

Examples

iS5comm# show telnet server

```
telnet service enabled
```

4.73. set http

To configure the HTTP authentication scheme or its redirection related parameters, use the command **set http** in Global Configuration Mode. The no form of the command disables the HTTP redirection feature.

set http

```
set http authentication-scheme {default | basic | digest} | redirection
enable
```

no http

```
no http redirection enable
```

Parameters

Parameter	Type	Description
`authentication-scheme`		Enter to specify the HTTP authentication scheme.
`default`		Enter to set the configurable HTTP authentication scheme to default.
`basic`		Enter to set the configurable HTTP authentication scheme to the legacy authentication scheme.
`digest`		Enter to set the configurable HTTP authentication scheme to digest.
`redirection`		Enter to specify the HTTP redirection feature.
`enable`		Enter to enable the HTTP redirection feature

Mode

Global Configuration Mode

Default

- Authentication scheme - default
- Redirection - enable

Examples

iS5comm(config)# set http authentication-scheme basic

iS5comm (config)# set http redirection enable

4.74. show http

To display the operational and configurable authentication scheme values, all redirection entries or filtered by URL, or HTTP server and port status, use the command **show http** in Privileged EXEC Mode.

show http

```
show http authentication-scheme | redirection [URL] | server status
```

Parameters

Parameter	Type	Description
`authentication-scheme`		Enter to display the operational and configurable authentication scheme values.
`redirection`		Enter to display all redirection entries or filtered by URL.
`URL`		Enter to display the URL for which the redirection entry has to be displayed.
`server status`		Enter to display the HTTP server and port status.

Mode

Privileged EXEC Mode

Examples

iS5comm# show http authentication-scheme

```
    The Operational HTTP authentication scheme is Default
    The Configured HTTP authentication scheme is Basic
```

iS5comm# show http redirection

```
    HTTP Redirection Entries
    ------------------------
    URL                              Server IP/DomainName
    ---                              --------------------
    % No Entries Found
```

iS5comm# show http server status

```
    HTTP server status             : Enabled
```

```
    HTTP port is                    : 80
    HTTP Requests In                : 0
    HTTP Invalids                   : 0
```

4.75. http redirect

To configure the alternate server for the URL specified, use the command **http redirect** in Global Configuration Mode. The no form of the command removes the redirection entry added to the server specified for the URL.

http redirect

```
http redirect <URL to be redirected> server {<Domain name> | <IPv4 Address>
| <IPv6 Address>}
```

no http redirect

```
no http redirect <URL to be redirected>
```

Parameters

Parameter	Type	Description
<URL to be redirected>	/url	Enter to specify the URL which has to be redirected. On receiving request for the URL, a redirection status is sent as response for the request.
server		Enter to set the server for the URL which is redirected. The options are:
<Domain name>		Enter to set the domain name of the alternate server.
<IPv4 Address>		Enter to set the IP address of the alternate server in v4 format.
<IPv6 Address>		Enter to specify the IP address of the alternate server in v6 format.

Mode

Global Configuration Mode

Default

- Authentication scheme - default
- Redirection - enable

Examples

iS5comm(config)# http redirect /sample/ server 12.0.0.2

4.76. set split-horizon

To enable or disable split horizon feature in the system, use the command **set split-horizon** in Global Configuration Mode.

set split-horizon

```
set split-horizon {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enter to enable the split horizon feature in the system.
disable		Enter to disable the split horizon feature in the system.

Mode

Global Configuration Mode

Prerequisites

To execute this command Split Horizon should be started in the system

Examples

iS5comm(config)# set split-horizon enable

4.77. shutdown split-horizon

To disable split horizon feature in the system, use the command **shutdown split-horizon** in Global Configuration Mode. The no form of the command enables the split horizon feature in the system.

shutdown split-horizon

no shutdown split-horizon

Mode

Global Configuration Mode

Examples

iS5comm(config)# no shutdown split-horizon

4.78. show split-horizon

To display the detailed information of the split horizon on the interface, use the command **show split-horizon** in Privileged EXEC Mode.

show split-horizon

```
show split-horizon [all] [interface [gigabitethernet <interface-id> |
Extreme-Ethernet <interface-id>]
```

Parameters

Parameter	Type	Description
`all`		Enter to display all configurations.
`interface`		Enter to display the interface-related configuration.
`Gigabitethernet`		Enter to display gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
`<interface-id>`		Enter a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
`Extreme-Ethernet`		Enter to display Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links

Mode

Privileged EXEC Mode

Examples

iS5comm# show split-horizon interface 1

```
    Ingress Port      VlanId     StorageType    Egress List
    ============      ======     ===========    ===========
    Gi0/1              -         Volatile     Gi0/2,Gi0/3,Gi0/6
```

4.79. speed

To set the speed of the interface, use the command **speed** in Interface Configuration Mode. The no form of the command sets the speed of the interface to its default value.

speed

```
speed {10 | 100 | 1000 | 10000 | 2500 | 25000 | 40000 | 50000 | auto | none-
gotiate}
```

Parameters

Parameter	Type	Description
10		Enter to set the port to run at 10Mbps.
100		Enter to set the port to run at 100Mbps.
1000		Enter to set the port to run at 1000Mbps.
10000		Enter to set the port to run at 10000Mbps.
2500		Enter to set the port to run at 2500Mbps.
25000		Enter to set the port to run at 25000Mbps.
40000		Enter to set the port to run at 40000Mbps.
auto		Enter to have the speed of the port automatically detected and set based on the peer switch
nonegotiate		Enter to disable negotiation on the ports.

Mode

Interface Configuration Mode

Prerequisites

To execute this command Split Horizon should be started in the system

Examples

iS5comm(config-if)# speed 10

4.80. port-type providerInstancePort

To configure the PIP (Provider Instance Port) type, use the command **port-type providerInstancePort** in Interface Configuration Mode.

port-type

```
port-type providerInstancePort
```

Parameters

Parameter	Type	Description
providerInstancePort		Enter to set the port type as PIP. PIP is nothing but a Backbone Edge Bridge Port that can receive and transmit I-tagged frames for multiple customers. PIPs are applicable only on PBB I Components.

Mode

Interface Configuration Mode (Physical/ Portchannel)

Prerequisites

This command executes only if

- PBB functionality is started in the bridge.
- Bridge Mode is Provider backbone bridge I-Component mode.

Examples

iS5comm(config-if)# port-type providerInstancePort

4.81. sleep

To make the CLI idle for a specified time, use the command **sleep** in Privileged EXEC Mode.

sleep

```
sleep <seconds(1-65535)>
```

Parameters

Parameter	Type	Description
<seconds(1-65535)>		Enter a value to specify idle time. This value ranges from 1 to 65535 in seconds.

Mode

Privileged EXEC Mode

Examples

iS5comm# sleep 5

4.82. rate-limit pause

To enable the pause ingress rate limit above which PAUSE frames are transmitted on the interface, use the command **rate-limit pause** in Interface Configuration Mode.

rate-limit pause

```
rate-limit pause [<high-watermark>] [<low-watermark>]
```

Parameters

Parameter	Type	Description
[<high-watermark>]		Enter a value to configure the ingress rate equal to or above which PAUSE frames are transmitted. This value ranges from 1 to 2800.
[<low-watermark>]		Enter a value to configure the ingress rate below which transmission of PAUSE frames are not sent. This value ranges from 1 to 2800.

Mode

Interface Configuration Mode (Physical)

Examples

iS5comm (config-if)# rate-limit pause 400000 300000

4.83. cpu controlled learning

To enable software learning of MAC Address from the packets arriving on the interface instead of hardware learning of MAC address, use the command **cpu controlled learning** in Interface Configuration Mode. The no form of the command disables CPU controlled learning of MAC Address on the interface

cpu controlled learning

no cpu controlled learning

Mode

Interface Configuration Mode (Physical)

Examples

iS5comm (config-if)# cpu controlled learning

4.84. traffic-separation control

To configure the method for receiving control packets by CPU, use the command **traffic-separation control** in Global Configuration Mode. This control ensures that the CPU processing capacity is utilized appropriately, according to the need of the protocol.

traffic-separation control

```
traffic-separation control {system_default | user_defined | none}
```

Parameters

Parameter	Type	Description
system_default		Enter to configure the method for receiving control packets by CPU as system default. This implies that the software can automatically install the ACL and QoS rules for all control packets. **NOTE:** If the configuration is changed from 'system_default' to 'user_defined' option, then all default ACL/QoS rules for carrying protocol control packets to CPU are removed. Then user has to install the specific ACL/QoS rules, to carry the intended control packets to CPU for the processing.
user_defined		Enter to configure the method for receiving control packets to CPU as user defined. This implies that the software cannot automatically install the ACL and QoS rules for all control packets. Only the administrator can install the required rules for receiving control packets to CPU
none		Enter to indicate only ACL rules. **NOTE:** If the configuration is changed from 'none' to 'system_default' option, then all default ACL filters for carrying protocol control packets to CPU are removed and new set of filters will be installed. Each filter will be associated with Qos rules **NOTE:** If the configuration is changed from 'none' to 'user_defined' option, then all default ACL filters for carrying protocol control packets to CPU are removed. Then user has to install the specific ACL/QoS rules, to carry the intended control packets to CPU for the processing

Mode

Global Configuration Mode

Examples

iS5comm (config)# traffic-separation control system_default

4.85. mdix auto

To enable the MDI/MDIX Auto Crossover of the interface, use the command **mdix auto** in Interface Configuration Mode. The no form of the command disables the MDI/MDIX Auto Crossover of the interface and sets the port as MDIX port.

mdix auto

no mdix auto

Mode

Interface Configuration Mode (Physical)

Default

AutoCross is disabled

Examples

iS5comm (config-if)# mdix auto

4.86. set port

To set the port to MDI or MDIX mode, use the command **set port** in Interface Configuration Mode. This command is hardware specific and MDIX is the vice versa of MDI.

set port

```
set port {mdi | mdix}
```

Parameters

Parameter	Type	Description
mdi		Enter to set the port to MDI mode. This is hardware specific where transmit pair are pins 1,2 and the receive pair are 3,6 pins respectively for the particular port.
mdix		Enter to set the port to MDIX mode. This is hardware specific where transmit pair are pins 3, 6 and the receive pair are 1, 2 pins respectively for the particular port. MDIX is the vice versa of mdi.
downlink		Enter to indicate downlink interface.
uplink		Enter to indicate uplink interface.

Mode

Interface Configuration Mode

Examples

iS5comm (config)# traffic-separation control system_default

4.87. config-restore

To configure the startup configuration restore option, use the command **config-restore** in Privileged EXEC Mode.

config-restore

```
config-restore {flash | remote <ucast_addr> file <filename> | norestore}
```

Parameters

Parameter	Type	Description
flash		Enter for restoring the flash file that is to be used for restoration when the system is restarted
remote		Enter for restoring the Unicast IP address of the remote system from where the switch configurations have to be downloaded to the 'Startup Configuration File' in the flash.
ucast_addr	A.B.C.D	Enter the Unicast IP address to be used.
file		Enter for restoring the specified remote location file.
filename		Enter a file name for the remote location file-a string with a maximum size of 12.
norestore		Enter to specify that the switch configurations need not be restored when the system is restarted

Mode

Privileged EXEC Mode

Default

norestore

Examples

iS5comm# config-restore flash

4.88. set mgmt-port routing

To enable or disable the management port routing function, use the command **set mgmt-port routing** in Global Configuration Mode.

set mgmt-port routing

```
set mgmt-port routing {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enter to enable the routing function over the Management Interface. This object can be configured only if the Management Port is used for IP Access.
disable		Enter to disable the routing function over the Management Interface. This object can be configured only if the Management Port is used for IP Access

Mode

Global Configuration Mode

Default

disable

Examples

iS5comm(config)# set mgmt-port routing enable

4.89. set switch-name

To set a name for the switch, use the command **set switch-name** in Global Configuration Mode.

set switch-name

```
set switch-name string <15>
```

Parameters

Parameter	Type	Description
string <15>		Enter to set a Switch Name (e.g. my-Switch). The value is a string with maximum size of 15.

Mode

Global Configuration Mode

Examples

iS5comm(config)# set switch-name default

4.90. packet

To configure the packet pattern and mask for pattern matching on the received packets, set the port and value for the packet transmitter and transmit the packet provided the packet pattern is configured, or set the packet pattern for the packet transmitter and transmits the packet, provided the interface is configured, use the command **packet** in Global Configuration Mode.

packet

```
packet {receive index <integer (0-4)> {value | mask | port <port_list>} |
{send index <integer (0-4)> {port <port_list> [count <integer (0-65536)>
[interval <integer (1-65535)>] | value}}
```

no packet

```
no packet receive index <integer (0-4)> [mask] | send index <integer (0-4)>
```

Parameters

Parameter	Type	Description
receive		Enter to configure received packets.
index		Enter to configure the index for the Pattern Analyzer / Pattern Transmitter row.
<integer (0-4)>	Integer	Enter to configure the packet receive / send index value which uniquely identifies a pattern to be matched. This value ranges from 0 to 4.
value		Enter to set a value for the pattern to be matched with the received packets
mask		Enter to set a value for the mask the received packets. This value is the mask for the pattern to be matched by the Pattern Analyzer and ranges from 1 to 1600.
port		Enter to configure the port / list of ports of the pattern receiver. This is the complete set of ports over which the pattern is to be matched by the packet
<port_list>		Enter a value for the ports list. This value ranges from 1 to 320. The syntax is a,b a-b a,b,c-d. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
send		Enter to set the port and value for the packet transmitter and transmit the packet provided the packet pattern is configured.
count		Enter to configure the number of packets to send.
<integer (0-65536)>	Integer	Enter an integer for number of packets.
interval		Enter to configure the time interval for the Pattern Transmitter.
<integer (1-65535>	Integer	Enter an integer for time interval.
value	Integer	Enter to configure the value of the packet for Packet Transmitter. The packet send value ranges between 1 and 1600. Enter a value when prompted.

Mode

Global Configuration Mode

Examples

iS5comm(config)# packet receive index 0 port 223

iS5comm(config)# packet send index 1 port 5

iS5comm(config)# packet send index 1 value

```
Enter Value: 4
```

4.91. show packet

To display the values of the packet receiver table and packet transmitter table, use the command **show packet** in Privileged EXEC Mode.

show packet

```
show packet {receive [index <integer (0-4)>] | send [index <integer (0-4)>]}
```

Parameters

Parameter	Type	Description
receive		Enter to configure received packets.
index		Enter to configure the index for the Pattern Analyzer row.
<integer (0-4)>	Integer	Enter to configure the packet receive / send index value which uniquely identifies a pattern to be matched. This value ranges from 0 to 4.
send		Enter to set the port and value for the packet transmitter and transmit the packet provided the packet pattern is configured.

Mode

Privileged EXEC Mode

Examples

iS5comm# show packet receive index 1

```
Packet Analyzer
```

iS5comm# show packet send

```
 Index              : 1
Value of the Pkt   :
Ports to send Pkt  :
No of Pkts to send : 1
```

```
    Time Interval      : 1
```

4.92. alias

To configure the alias name for the interface, use the command **alias** in Interface Configuration Mode.

alias

```
alias string <63>
```

Parameters

Parameter	Type	Description
`string <15>`		Enter analias name for the interface. The value is a string with maximum size of 63.

Mode

Interface Configuration Mode

Examples

iS5comm (config-if)# alias interface1

4.93. port-security-state

To configure the port security state of the interface, use the command **port-security-state** in Interface Configuration Mode. The interface port security state specifies whether the port is connected to trusted hosts or not.

port-security-state

```
port-security-state {trusted | untrusted}
```

Parameters

Parameter	Type	Description
`trusted`		Enter to set a port security state as trusted.This specifies that packets coming on these ports will be trusted.
`untrusted`		Enter to set a port security state as untrusted.

Mode

Interface Configuration Mode

Default

trusted

Examples

iS5comm (config-if)# port-security-state trusted

4.94. default-value save

To specify whether default values needs to be saved or not when incremental save option is enabled, use the command **default-value save** in Global Configuration Mode. On configuring this command, iS5Com-nvram.txt file is updated. The configured value is effective only after rebooting the system.

default-value save

```
default-value save {enable | disable }
```

Parameters

Parameter	Type	Description
`trusted`		Enter to enable the default value save option.This specifies that MSR stores default values also when Incremental save is enabled.
`untrusted`		Enter to disable the default value save option.This specifies MSR does not store default values when Incremental save is enabled.

Mode

Global Configuration Mode

Default

disable

Examples

iS5comm(config)# default-value save enable

4.95. set mirroring

To enable or disable the mirroring in the system, use the command **set mirroring** in Global Configuration Mode.

set mirroring

```
set mirroring {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enter to enable mirroring in the system. When set as enabled all mirroring configurations present will be programmed in hardware.
disable		Enter to disable mirroring in the system and remove all configuration from the hardware.

Mode

Global Configuration Mode

Examples

iS5comm(config)# set mirroring enable

4.96. default exec-timeout

To configure the default exec-timeout value for line disconnection, use the command **default exec-timeout** in Global Configuration Mode.

default exec-timeout

```
default exec-timeout <integer (1-18000)>
```

Parameters

Parameter	Type	Description
<integer (1-18000)>		Enter to a default exec-timeout value for line disconnection. This value ranges from 1 to 18000 seconds

Mode

Global Configuration Mode

Examples

iS5comm(config)# default exec-timeout 5

4.97. port

To configure port and CVLAN id to AC interface, use the command **port** in Interface Configuration Mode.

port

```
port {gigabitethernet <interface-id> | Extreme-Ethernet <interface-id>] |
fastethernet <interface-id> | port-channel <interface-id>} | vlan <integer
(1-65535)>
```

Parameters

Parameter	Type	Description
`Gigabitethernet`		Enter for gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
`<interface-id>`		Enter for a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
`Extreme-Ethernet`		Enter for the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
`fastethernet`		Enter for fastethernet. fastethernet is referred to as 100BASE-T standard and is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
`port-channel`		Enter for port-channel. This is the logical interface that represents an aggregator which contains several ports aggregated together.
`vlan <integer (1-65535)>`		Enter an integer for vlan id number. It configures the specified customer VLAN for the AC interface. This value ranges between 1 and 65535.

Mode

AC Interface Configuration Mode

Examples

iS5comm (config-if)# port 1 gi 0/1

iS5comm (config-if)# port gigabitethernet 0/1

4.98. web-session timeout

To configure the web-session timeout in seconds after which the session expires, use the command **web-session timeout** in Global Configuration Mode.

web-session timeout

```
web-session timeout <integer (30-1800)>
```

Parameters

Parameter	Type	Description
<integer (30-1800)>		Enter a web-session timeout value in seconds. This value ranges from 30 to 1800 seconds.

Mode

Global Configuration Mode

Prerequisites

300

Examples

iS5comm(config)# web-session timeout 1800

4.99. clear http server statistics

To clear the HTTP server requests received and discarded statistics, use the command **clear http server statistics** in Global Configuration Mode.

clear http server statistics

Mode

Global Configuration Mode

Examples

iS5comm(config)# clear http server statistics

4.100. show web-session timeout

To display web-session timeout, use the command **show web-session timeout** in Privileged EXEC Mode.

show web-session timeout

Mode

Privileged EXEC Mode

Examples

iS5comm# show web-session timeout

4.101. show config-restore status

To display the config-restore status, use the command **show config-restore status** in Privileged EXEC Mode.

The list of health-restore status for the device is as follows;

- configRestoreSuccess—indicates that configuration restore operation is successfully done.
- configRestoreFailed—indicates that configuration restoration is unsuccessful.
- configRestoreInProgress—indicates that configuration restore operation is in-progress.
- configRestoreDefault—indicates the absence of config-restore file (iS5Com.conf) and that the device has started with default values.

show config-restore status

Mode

Privileged EXEC Mode

Default

configRestoreDefault

Examples

iS5comm# show config-restore status

```
SWITCH CONFIGURATION RESTORE STATUS
--------------------------------
Config Restore Status     : default configuration-restore
```

4.102. clear protocol counters

To clear the iS5Com counters for all protocols or only specified protocols, use the command **clear protocol counters** in Privileged EXEC Mode.

clear protocol counters

```
clear protocol counters [bgp] [ospf] [rip] [rip6] [ospf3] [ipv4] [ipv6]
```

Parameters

Parameter	Type	Description
bgp		Enter to clear the counters for BGP.
ospf		Enter to clear the counters for OSPF
rip		Enter to clear the counters for RIP.
rip6		Enter to clear the counters for RIP6.
ospf3		Enter to clear the counters for OSPF3.
ipv4		Enter to clear the counters for IPv4.
ipv6		Enter to clear the counters for IPv6.

Mode

Privileged EXEC Mode

Examples

iS5comm (config)# clear protocol counters

4.103. dump core-file

To configure the location where the dump core file has to be stored, use the command **dump core-file** in Global Configuration Mode.

dump core-file

Mode

Global Configuration Mode

Examples

iS5comm (config)# dump core-file flash:/home/twg

4.104. dump

To display memory content from the given memory location, use the command **dump** in Privileged EXEC Mode.

dump

```
dump {mem <integer(1-0xffffffff)> [len <integer(1-256)>] | que name
[<string(4)>] | sem name [<string(4)>] | task name [<string(4)>]}
```

Parameters

Parameter	Type	Description
mem		Enter to configure the memory location
<integer(1-0xffffffff)>		Enter an Hex (0x<address>) to specify memory location.
len		Enter to configure the byte length.
<integer(1-256)>		Enter a value for byte length. This value ranges from 1 to 256.
que		Enter to display queue-related information.
name		Enter to specify string name for queue-related information to be displayed.
<string(4)>		Enter a string for name for queue, semaphore/ task. This value is a string with maximum size 4.
sem		Enter to display semaphore-related information.
name		Enter to specify string name for semaphore related information to be displayed.
task		Enter to display task-related information.
name		Enter to specify string name for task-related information to be displayed.

Mode

Privileged EXEC Mode

Examples

iS5comm # dump mem 0x0ae07880 len 8

```
    0x7d    0x00          0x68    0xdf    0x4d    0x0a
```

dump sem name

```
     Name         Num Tasks
    Blocked
    MEMU         0
    BUFS         0
    000m         0
    001m         0
    002m         0
    TMMU         0
    IMSM         0
    001r         0
    002r         0
    SNDB         0
    TRIE         0
    003m         0
    004m         0
    005m         0
    tris         0
    006m         0
    007m         0
    008m         0
    TRRP         0
    TRLP         0 & the list continues
```

4.105. debug iss

To enable the tracing as per the configured debug levels, use the command **debug iss** in Global Configuration Mode. The trace statements are generated for the configured trace levels. The no form of the command disables the tracing of IS5COM as per the configured debug levels. The trace statements are not generated for the configured trace levels.

debug iss

```
debug iss {enable | disable} [init-shut] [management-trc] [data-path-trc]
[cntrl-plane-trc] [dump-trc] [os-resource-trc] [all-fail]
```

no debug iss

Parameters

Parameter	Type	Description
enable		Enter to enable debug traces for ISS
disable		Enter to disable debug traces for ISS
init-shut		Enter to generate debug statements for init and shutdown traces
management-trc		Enter to generate debug statements for management traces
data-path-trc		Enter to generate debug statements for data path traces
cntrl-plane-trc		Enter to generate debug statements for control plane traces
dump-trc		Enter to generate debug statements for dump traces
os-resource-trc		Enter to generate debug statements for OS resource traces
all-fail		Enter to generate debug statements for failure traces

Mode

Global Configuration Mode

Examples

iS5comm(config)# debug iss enable init-shut

4.106. show nvram

To display the current information stored in the NVRAM (nonvolatile random-access memory), use the command **show nvram** in Privileged EXEC Mode.

show nvram

Mode

Privileged EXEC Mode

Examples

```
iS5comm# show nvram
    Default IP Address                      : 192.168.10.1
    Default Subnet Mask                     : 255.255.255.0
    Default IP Address Config Mode          : Manual
    Default IP Address Allocation Protocol : DHCP
    Switch Base MAC Address                 : e8:e8:75:90:0b:01
    Default Interface Name                  : Gi0/1
    Default RM Interface Name               : NONE
    Config Restore Option                   : No restore
    Config Save Option                      : No save
    Auto Save                               : Disable
    Incremental Save                        : Disable
    Roll Back                               : Enable
    Config Save IP Address                  : 0.0.0.0
    Config Save Filename                    : iss.conf
    Config Restore Filename                 : iss.conf
    PIM Mode                                : Sparse Mode
    IGS Forwarding Mode                     : MAC based
    Cli Serial Console                      : Yes
    SNMP EngineID                           : 80.00.08.1c.04.46.53
    SNMP Engine Boots                       : 985
    Default VLAN Identifier                 : 1
    Stack PortCount                         : 0
    ColdStandby                             : Disable
    Store Default Value                     : Disable
    Hitless Restart  Flag                   : Disable
    iBiome Software Version                 : 1.3.01A17
    UBoot Software Version                  : U-Boot 2016.09 ver 1.30
    Switch Name                             : iS5com
    Prompt Name                             : iS5comm
    Banner Name                             : RAPTOR iBiome OS
    RM Heart Beat Mode                      : Internal
    RM Redundancy Type                      : Hot
```

```
RM Data Plane Type                    : Shared
RM Type                               : OOB
TimeStamp Method                      : TransHardware
Restore Flag                          : Enabled
Dynamic Port Count                    : 28
FIPS operation mode                   : Disabled
Restore Option                        : Disabled
Bridge Mode                           : Customer Bridge
Debugging Log File Location           : /mnt/log/
Management Port                       : Disabled
Automatic Port Create Flag            : Enabled
Restore Type                          : CSR
IMG_DUMP_PATH                         :
```

4.107. debug np module

To enable tracing and generates debug statements for NPAPI traces for the specified module, use the command **debug np module** in Privileged EXEC Mode. The no form of this command disables the NPAPI trace levels for the specified module.

debug np module

```
debug np module {see list of available parameters} severity {<integer (1-8)>
| alerts | critical | debugging | emergencies | errors | informational |
notification | warnings
```

no debug np module

```
no debug np module {see list of available parameters} severity {<integer
(1-8)> | alerts | critical | debugging | emergencies | errors | informa-
tional | notification | warnings
```

Parameters

The list of parameters are as follows:

- acl ACL related NP programming
- bcmx BCMX related NP programming
- bfd BFD related NP programming
- brg BRG related NP programming
- cfa CFA related NP programming
- cpss CPSS related NP programming
- diffserv DIFFSERV related NP programming
- dsmon DSMON related NP programming

- ecfm ECFM related NP programming
- elps ELPS related NP programming
- eoam EOAM related NP programming
- erps ERPS related NP programming
- ether ETHER related NP programming
- fmn FMN related NP programming
- igmp IGMP related NP programming
- p6 IPv6 related NP programming
- ipmc IPMC related NP programming
- iss ISS related NP programming
- la LA related NP programming
- lion LION related NP programming
- mau MAU related NP programming
- mbs MBS related NP programming
- mld MLD related NP programming
- mlds MLDS related NP programming
- mpls MPLS related NP programming
- mrp MRP related NP programming
- mstp MSTP related NP programming
- np NP related NP programming
- ofc OFC related NP programming
- pbb PBB related NP programming
- pnac PNAC related NP programming
- poe POE related NP programming
- ppp PPP related NP programming
- ptp PTP related NP programming
- pvrst PVRST related NP programming
- qos QOS related NP programming
- rbr RBR related NP programming
- red RED related NP programming
- rm RM related NP programming
- rmon RMON related NP programming
- rport RPORT related NP programming
- rstp RSTP related NP programming
- srcmv SRCMV related NP programming
- synce SYNCE related NP programming
- tac TAC related NP programming
- vcm VCM related NP programming

- vlan VLAN related NP programming

Parameter	Type	Description
see list of available parameters	Integer	Select a parameter from the list shown above.
<integer(1-8)>	Integer	Enter a number to determine severity level.
alerts		Enter to set the severity to alerts or immediate action needed.
critical		Enter to set the severity to critical or critical conditions.
debugging		Enter to set the severity to debugging or debugging messages.
emergencies		Enter to set the severity to emergencies or system is unusable.
errors		Enter to set the severity to errors or errors conditions.
informational		Enter to set the severity toinformational or information messages.
notification		Enter to set the severity to notification or normal but significant messages.
warnings		Enter to set the severity to warnings or warning conditions.

Mode

Privileged EXEC Mode

Examples

iS5comm # debug np module red severity informational

4.108. description

To set the description of an interface, use the command **description** in Interface Configuration Mode.

description

```
description <description of this interface>
```

Parameters

Parameter	Type	Description
<description of this interface>		Enter a string for description of the interface. This value is a string with a maximum size of 127.

Mode

Interface Configuration Mode

Examples

iS5comm (config-if)# description Interface1

```
iS5comm# show interfaces description
Interface    Status   Protocol  Description
---------    ------   --------  -----------
Gi0/1        up       down      interface1
Gi0/2        up       down
```

4.109. counters

To enable or disable the statistics collection status for the interface, use the command **counters** in Interface Configuration Mode.

counters

```
counters {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enter to enable the statistics collection for the interface.
disable		Enter to disable the statistics collection for the interface.

Mode

Interface Configuration Mode (Vlan)

Examples

iS5comm(config)# interface vlan 1

iS5comm(config-if)# counters enable

4.110. show l3vlan interfaces counters

To display the statistics counters for the L3 vlan interface, use the command **show l3vlan interfaces counters** in Privileged EXEC Mode.

show l3vlan interfaces counters

```
show l3vlan interfaces counters [vlan <vlan_vfi_id>
```

Parameters

Parameter	Type	Description
vlan		Enter a string for description of the L3 VLAN interface.
<vlan_vfi_id>		Enter a value for an interface to be displayed. • <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535. **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range. **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW. **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted.

Mode

Privileged EXEC Mode

Examples

iS5comm (config)# show l3vlan interfaces counters vlan 1 switch default

```
Port       InPkt     InOctets
----       -----     --------
vlan1      1           229
```

4.111. set entity physical-index

To configure the read-write objects of the physical components present in the system which defines a greater than zero value used to identify a physical entity, use the command **set entity physical-index** in Global Configuration Mode. The no form of the command deletes the configuration.

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP).

Entity MIB is a standardized way of representing a single agent that supports multiple instances of one MIB. With the entity MIB support in iss, all instances of the MIBs registered with agent are identifiable, so that the NMS (Network Management System) can easily communicate with the particular instance / logical entity. MIB also provides the complete hierarchal hardware component view to the user.

The single agent present in each of these cases implies a relationship binds these entities. Effectively, there is some "overall" physical entity which houses the sum of the things managed by that one agent,i.e., there are multiple "logical" entities within a single physical entity.

A "physical entity" or "physical component" represents an identifiable physical resource within a managed system. Zero or more logical entities may utilize a physical resource at any given time. Determining which physical components are represented by an agent in the EntPhysicalTable is an implementation-specific matter. Typically, physical resources (e.g., communications ports, backplanes, power supplies, the overall chassis) that can be managed via functions associated with one or more logical entities, are included in the MIB. Reference, RFC 4133.

The physical index is an arbitrary value that uniquely identifies the physical entity which can be small positive integer.

set entity physical-index

```
set entity physical-index <integer (1-2147483647)> [asset-id <SnmpAdmin-
String (1-32)>] [serial-number <SnmpAdminString (1-32)>] [alias-name
<SnmpAdminString (1-32)>] [uris <OCTET-STRING (1-255)>]
```

no set entity physical-index

```
no set entity physical-index <integer (1-2147483647)> [asset-id]
[serial-number] [alias-name] [uris]
```

Parameters

Parameter	Type	Description
<integer (1-2147483647)>		Enter to specify the Index of the physical entity. This value ranges from 1 to 2147483647
asset-id		Enter to specify the asset tracking identifier for the physical entity.
<SnmpAdminString (1-32)>	Integer	Enter a value for asset tracking identifier. This value is a string of size varying between 1 and 32 characters. Asset tracking identifier is not needed for the physical entities (such as repeater ports within a repeater module) that are not considered as a field replaceable unit by the vendor. A zero-length string is returned for these entities.
serial-number		Enter to specify the vendor-specific serial number string for the physical entity.
<SnmpAdminString (1-32)>	Integer	Enter a value for serial-number identifier. This value is a string of size varying between 1 and 32 characters. Serial number string is not needed for the physical entities (such as repeater ports within a repeater module) that are not considered as a field replaceable unit by the vendor. A zero-length string is returned for these entities
alias-name		Enter to specify the alias name for the physical entity.
<SnmpAdminString (1-32)>	Integer	Enter a value for alias-name identifier. This value provides a non-volatile handle for the entity and is a string of size varying between 1 and 32 characters.
uris		Enter to specify the additional identification information (URI-Uniform Resource Indicator) about the physical entity.
<OCTET-STRING (1-255)>	Integer	Enter a value for URI. This value ranges from 1 to 255

Mode

Global Configuration Mode

Default

- assetId - Zero-length string, on initial instantiation of the physical entity.

- Zero-length string, on initial instantiation of the physical entity, if a serial number is unknown or non-existent. Correct vendor-assigned serial number, on initial instantiation of the physical entity, if the serial number is available to the SNMP agent
- alias-name - Zero-length string, on initial instantiation of the physical entity. The SNMP agent may also set the value to a locally unique default value.

Prerequisites

- If write access is implemented for an instance of asset ID and a value is written into the instance, SNMP agent should retain the value as long as the entity associated with the instance remains instantiated. This instantiation includes the instantiation across all re-initialization / reboot of the NMS. and instantiation resulting in a change of the physical entity's index value.
- If write access is implemented for an instance of the serial number string and a value is written into the instance, SNMP agent should retain the value as long as the entity associated with the instance remains instantiated. This instantiation includes the instantiation across all re-initialization / reboot of the NMS. and instantiation resulting in a change of the physical entity's index value.
- If the agents cannot provide non-volatile storage for the serial number string, then the agents are not required to implement write access for the the serial number string object.
- Implementations that can correctly identify the serial numbers of all installed physical entities are not required to provide write access to the serial number string object
- If write access is implemented for an instance of the alias name and a value is written into the instance, SNMP agent should retain the value as long as the entity associated with the instance remains instantiated. This instantiation includes the instantiation across all re-initialization / reboot of the NMS. and instantiation resulting in a change of the physical entity's index value.

Examples

iS5comm (config)# set entity physical-index 2222222 asset-id 8 serial-number 7 alias-name GJG uris yg

4.112. show entity

To display details about MIB entity configuration of physical entities, logical entities, logical and physical entities mapping, mapping of logical and physical entities with external identifiers, or containment relationship details of physical components, use the command **show entity** in Privileged EXEC Mode.

show entity

```
show entity {physical [index <integer (1-2147483647)>] | logical [index
<integer (1-2147483647)>] | lp-mapping | alias-mapping [index <integer
(1-2147483647)>] phy-containment [index <integer (1-2147483647)>]
```

Parameters

Parameter	Type	Description
`physical`		Enter to specify displaying of the physical entities which are physical components that represents an identifiable physical resource within a managed system. Zero or more logical entities may utilize a physical resource at any given time.
`index`		Enter to a value for the physical entity, logical entity, mapping of logical and physical entities with external identifiers, or containment relationship details of physical components respectively. This value ranges from 1 to 2147483647.
`<integer (1-2147483647)>`		Enter to display the IP interface configuration for the specified VLAN ID.
`logical`		Enter to specify displaying of multiple logical entities within a single physical entity. The overall physical entity contains multiple (smaller) physical entities and each logical entity is associated with a particular physical entity.
`lp-mapping`		Enter to specify displaying of the mapping of logical and physical entities, interfaces, and non-interface ports managed by a single agent. The LPMapping contains mappings between logical entities and physical components supporting that entity. A logical entity can map to more than one physical component, and more than one logical entity can map to the same physical component.
`alias-mapping`		Enter to specify displaying of the mapping of logical and physical entity with alias external object identifiers values. This allows resources managed with other MIBs (e.g. repeater ports, bridge ports, physical and logical interfaces) to be identified in the physical entity hierarchy.
`phy-containment`		Enter to specify displaying of the simple mapping between the physical contained values for each container / containee relationship in the managed system.

Mode

Privileged EXEC Mode

Examples

iS5comm# show entity physical index 1

```
Physical Index: 1
Physical Descr: Network Element
Physical VendorType:
Physical ContainedIn: 0
Physical Class: Chassi
Physical ParentRelPos: 0
Physical Name: iS5com
Physical HardwareRev: 1531-0001-B04
Physical FirmwareRev: 6.7.2
Physical Serial Num: not available
Physical MfgName: iS5Com
Physical ModelName: not available
Physical Alias: DummyName
Physical AssetID: DummyId
Physical MfgDate: 2009-8-6,13:30:30.1
Physical Uris: not available
Physical FRU Status: True
```

iS5comm# show entity logical index 1

```
Logical Index: 1
Logical Description: iS5Com
Logical Type:
Logical Community: default
Logical Transport Address: 192.168.10.1:161
Logical Transport Domain:
Logical Context Engine Id: 80:00:08:1c:04:46:53
Logical Context Name: default
```

iS5comm# show entity lp-mapping

```
Logical Entity                Mapped Physical Entity
--------------                ----------------------
1 ()                          10 (Port)
2 ()                          12 (Port)
```

iS5comm# show entity alias-mapping

```
Physical Entity        Logical Entity      Mapped External Identifier
---------------        --------------      --------------------------
10 (Port)              all
1 (Port)              all
12 (Port)              all
13 (Port)              all
14 (Port)              all
15 (Port)              all
```

iS5comm# show entity phy-containment

```
Containment Relationship
------------------------
Physical Entity            : 1 (Chassis)
Member Physical Entities   : 2 (CPU), 3 (Power Supply), 4 (Fan)
5 (Fan), 6 (Fan), 7 (Fan)
8 (Fan), 9 (Module)
Physical Entity            : 9 (Module)
Member Physical Entities   : 10 (Port), 11 (Port), 12 (Port)
13 (Port), 14 (Port), 15 (Port)
16 (Port), 17 (Port), 18 (Port)
19 (Port), 20 (Port), 21 (Port)
22 (Port), 23 (Port), 24 (Port)
25 (Port), 26 (Port), 27 (Port)
28 (Port), 29 (Port), 30 (Port)
31 (Port), 32 (Port), 33 (Port)
34 (Port), 35 (Port), 36 (Port)
37 (Port)-----------------------------------------------------------
```

4.113. gratuitous arp

This command is used to enable the gratuitous arp feature on an interface.

ip arp gratuitous

```
no parameters are used for this command.
```

Parameters

None

Mode

Privileged EXEC Mode

Example: Enabling Gratuitous ARP

iS5comm# configure terminal

iS5comm (config)# interface gigabitethernet 0/1

iS5comm (config-if)# shutdown

iS5comm (config-if)# no switchport

iS5comm (config-if)# ip arp gratuitous

iS5comm (config-if)# no shutdown

iS5comm (config-if)# exit

iS5comm (config)# exit

iS5comm#

Example: Disabling Gratuitous ARP

Enabling Gratuitous ARP

iS5comm# configure terminal

iS5comm (config)# interface gigabitethernet 0/1

iS5comm (config-if)# shutdown

iS5comm (config-if)# no switchport

iS5comm (config-if)# no ip arp gratuitous

iS5comm (config-if)# no shutdown

iS5comm (config-if)# exit

iS5comm (config)# exit

iS5comm#

4.114. show grat-arp

This command is used to enable the gratuitous arp feature on an interface.

show grat-arp

```
show grat-arp
 [<interface-type> <interface-id>]
```

Parameters

Parameter	Type	Description
`interface-type`		Valid entries are either “Extreme-Ethernet” or “Gigabitethernet”.
`interface-id`		For the “Gigabitethernet” interface type valid entries are <0>/<1-28> For the “Extreme-Ethernet” interface type valid entries are <0>/<1-4>

Mode

Privileged EXEC Mode

Example: Show Gratuitous ARP

iS5comm# show grat-arp

iS5comm# show grat-arp gigabitethernet 0/1

```
iS5comm# show grat-arp gigabitethernet 0/1
Gratuitous Arp Details
----------------------

Record #1
        Interface                               : gigabitethernet 0/1
        Gratuitous Arp Status                   : Enable

        Gratuitous Arp Transmission Details

        Gratuitous Arp Request Tx Source IP     : 0.0.0.0
        Gratuitous Arp Response Tx Source IP    : 0.0.0.0
        Gratuitous Arp Request Tx Reason        : None Transmitted
        Gratuitous Arp Response Tx Reason       : None Transmitted
        Gratuitous Arp Request Tx Count         : 0
        Gratuitous Arp Response Tx Count        : 0

        Gratuitous Arp Received Details

        Gratuitous Arp Request Rx Source IP     : 0.0.0.0
        Gratuitous Arp Response Rx Source IP    : 0.0.0.0
        Gratuitous Arp Request Source MAC       : 00:00:00:00:00:00
        Gratuitous Arp Response Source MAC      : 00:00:00:00:00:00
        Gratuitous Arp Request Rx Count         : 0
        Gratuitous Arp Response Rx Count        : 0
iS5comm#
```

Output from show grat-arp gigabitethernet 0/1

RADIUS

5. RADIUS

RADIUS (Remote Authentication Dial-In User Service), is widely used in network environments, and is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for embedded network devices such as routers, modem servers, switches and so on. RADIUS is currently the de-facto standard for remote authentication. It is very prevalent in both new and legacy systems. It is used for several reasons:

- RADIUS facilitates centralized user administration (Authentication, Authorization and Accounting).
- RADIUS provides some protection against an active attacker.

5.1. radius-server host

To configure the RADIUS client with the parameters host, timeout, key, retransmit, use the command **radius-server host** in Global Configuration Mode. The no form of the command deletes the RADIUS server configuration.

radius-server host

```
radius-server host {<ipv4-address> | <ipv6-address> | <dns_host_name (255)>}
[auth-port <integer(1-65535)>] [acct-port <integer(1-65535)>] [timeout
<integer(1-120)>] [retransmit <integer(1-254)>] [key <secret-key-string
(46)>] [primary]
```

no radius-server host

```
no radius-server host {<ipv4-address> | <ipv6-address> | <dns_host_name
(255)>} [primary]
```

Parameters

Parameter	Type	Description
<ipv4-address>	A.B.C.D	Enter to configure the IPv4 address of the RADIUS server host.
<ipv6-address>	AAAA::BBBB	Enter to configure the IPv6 address of the RADIUS server host
<dns_host_name (255)>		Enter to configure the DNS (Domain Name System) name of the RADIUS server host. This value is a string of maximum size 255.
auth-port		Enter to configures a specific UDP (User Datagram Protocol) destination port on this RADIUS server to be used solely for the authentication requests.
<integer(1-65535)>	Integer	Enter a value for UDP destination port to be used for authentication requests. This value ranges from 1 to 65535.
acct-port		Enter to configure a specific UDP destination port on this RADIUS to be solely used for accounting requests. This value ranges from 1 to 65535.
<integer(1-65535)>	Integer	Enter a value for UDP destination port to be used for accounting requests. This value ranges from 1 to 65535
timeout		Enter to configure the time period in seconds for which a client waits for a response from the server before re-transmitting the request.
<integer(1-120)>	Integer	Enter a value for time before the request is retransmitting. This value ranges from 1 to 120 seconds.
retransmit		Enter to configure the maximum number of attempts to be tried by a client to get response from the server for a request.
<integer(1-254)>	Integer	Enter a value for the number of retransmitting attempts. This value ranges from 1 to 254.
key		Enter to configure the per-server encryption key which specifies the authentication and encryption key for all RADIUS communications between the authenticator and the RADIUS server.
<secret-key-string (46)>	Integer	Enter a secret key string. This value is a string of maximum size 46. If the key value is not configured, then the default key will be used.

Parameter	Type	Description
primary		Enter to set the RADIUS server as the primary server. Only one server can be configured as the primary server, any existing primary server will be replaced, when the command is executed with this option.

Mode

Global Configuration Mode

Default

- timeout - 10 seconds
- retransmit - 3 attempts
- auth-port - 1812
- acct-port - 1813
- key - RADIUS

Prerequisites

- The maximum number of radius servers that can be configured is 5.

Examples

iS5comm (config)# radius-server host 10.0.0.1 key pass

iS5comm (config)# radius-server host 10.0.0.100

```
    Radius will be configured with default secret key
```

5.2. set radius

The **set radius** command is used enable or disable RADIUS services.

set radius

```
set radius {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enables the RADIUS module.
disable		Disables the RADIUS module.

Mode

Global Configuration Mode

Examples

iS5comm# configure terminal

iS5comm(config)# set radius enable

5.3. show radius

To display RADIUS server Host information which contains, Index, Server address, Shared secret, Radius Server status, Response Time, Maximum Retransmission, Authentication Port and Accounting Port, and RADIUS Server Statistics for the data transfer between server and the client from the time of initiation, use the command **show radius** in Privileged EXEC Mode.

show radius

```
show radius {server [<ipv4-address> | <ipv6-address> | <dns_host_name
(255)>]} | module [ status ] | statistics}
```

Parameters

Parameter	Type	Description
server		Enter to display server-related information.
<ipv4-address>	A.B.C.D	Enter to display the related information for the specified IPv4 address of the RADIUS server host.
<ipv6-address>	AAAA::BBBB	Enter to display the related information for the specified IPv6 address of the RADIUS server host.
<dns_host_name (255)>		Enter to display the related information for the specified DNS (Domain Name System) name of the RADIUS server host. This value is a string of maximum size 255.
statistics		Enter to display statistics-related information
module status		Displays the status of the RADIUS module. It will show the module status, authentication port and accounting port.

Mode

Privileged EXEC Mode

Prerequisites

Debugging is disabled

Examples

iS5comm # debug radius all

iS5comm # show radius module status

5.4. debug radius

To enable RADIUS debugging options, use the command **debug radius** in Privileged EXEC Mode. The RADIUS debug traces capture error information and failure messages in the server. These are registered in a log file for future reference. Each trace has to be enabled individually. The no form of the command disables RADIUS debugging options.

debug radius

```
debug radius {all | errors | events | packets | responses | timers}
```

no debug radius

Parameters

Parameter	Type	Description
`all`		Enter to specify generating of traces for all RADIUS server messages.
`errors`		Enter to specify generating of traces for error code messages. All instances where an error is identified are captured by this trace and all errors is registered in the log.
`events`		Enter to specify generating of traces for events-related messages. Events such as an authentication query from authenticator or a response from server are registered in the log.
`packets`		Enter to specify generating of traces for number of packets, kind of packets received and sent from server.
`responses`		Enter to specify generating of traces for responses sent from the server to authenticator.
`timers`		Enter to specify generating of traces for the different timers used in the session before the system is rebooted.

Mode

Privileged EXEC Mode

Default

Debugging is disabled

Examples

iS5comm # debug radius all

TACACS

6. TACACS

TACACS (Terminal Access Controller Access Control System), widely used in network environments, is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for providing NAS (Network Access Security). NAS ensures secure access from remotely connected users. TACACS implements the TACACS Client and provides the AAA (Authentication, Authorization and Accounting) functionalities.

TACACS is used for several reasons:

- Facilitates centralized user administration
- Uses TCP for transport to ensure reliable delivery
- Supports inbound authentication, outbound authentication and change password request for the Authentication service
- Provides some level of protection against an active attacker

6.1. tacacs-server

To configure the TACACS client with the parameters host, timeout, key, retransmit, to set the retransmission related configuration with its retransmit value, and to configure the active server address and selects an active server from the list of servers available in the TACACS server table, use the command **tacacs-server** in Global Configuration Mode. The no form of the command deletes the server entry from the TACACS server table, resets the retransmit value to its default value, and disables the configured client active server.

tacacs-server

```
radius-server {host {<ipv4-address> | <ipv6-address> | <dns_host_name (255)>}
[key <secret-key-string (64)] [port <integer(1-65535)>] [single-connection]
[timeout <integer(1-255)>] | retransmit <retries (1-5)> | use-server address
{<ipv4-address> | <ipv6-address> | <dns_host_name (255)>}
```

no radius-server host

```
no radius-server host {<ipv4-address> | <ipv6-address> | <dns_host_name
(255)>} | retransmit | use-server
```

Parameters

Parameter	Type	Description
host	A.B.C.D	Enter to configure the IPv4 address of the TACACS server host.
<ipv4-address>	A.B.C.D	Enter to configure the IPv4 address of the TACACS server host.
<ipv6-address>	AAAA::BBBB	Enter to configure the IPv6 address of the TACACS server host
<dns_host_name (255)>		Enter to configure the DNS (Domain Name System) name of the TACACS server host. This value is a string of maximum size 255.
key		Enter to configure the authentication and encryption key for all TACACS communications between the authenticator and the TACACS server.
<secret-key-string (64)>	Integer	Enter a encryption key string. This value is a string of maximum size 64. If the key value is not configured, then the default key will be used.
port		Enter to configure the TCP port number in which the multiple sessions are established.
<integer(1-65535)>	Integer	Enter a value for the TCP port number. This value ranges from 1 to 120 seconds.
single-connection		Enter to configure the time period in seconds for which a client waits for a response from the server before re-transmitting the request.
timeout		Enter to configure the time period (in seconds) for which a client waits for a response from the server before closing the TCP connection. The link between the server and the client gets disconnected, if the specified time is exceeded.
<integer(1-255)>	Integer	Enter a value for time period for which a client waits for a response from the server before closing the TCP connection. This value ranges from 1 to 255 seconds.
retransmit		Enter to configure the retransmission related configuration and retransmit value. It is the number of times the client searches the active server from the list of servers maintained in the TACACS client, when active server is not configured.
<retries (1-5)>	Integer	Enter a number for retransmit retries.

Parameter	Type	Description
use-server		Enter to configure the active server address and selects an active server from the list of servers available in the TACACS server table.
address	Integer	Enter to configure IP address related configuration.
<ipv4-address>	A.B.C.D	Enter to configure the IPv4 address of the TACACS server host.
<ipv6-address>	AAAA::BBBB	Enter to configure the IPv6 address of the TACACS server host
<dns_host_name (255)>		Enter to configure the DNS (Domain Name System) name of the TACACS server host. This value is a string of maximum size 255.

Mode

Global Configuration Mode

Default

- port - 49
- timeout - 5 seconds
- key - iS5Com
- retries - 2

Prerequisites

- The maximum number of TACACS servers that can be configured is 5.
- The specified server should be any one of the entries from the TACACS server table.

Examples

iS5comm (config)# tacacs-server host 12.0.0.100

```
    TACACS+ server configured with default secret key !
```

iS5comm (config)# tacacs-server host 2005::33

```
    TACACS+ server configured with default secret key !
```

iS5comm (config)# tacacs-server retransmit 3

iS5comm (config)# tacacs use-server address 12.0.0.100

6.2. show tacacs

To display the server's details, such as IP address, single connection, port, etc, and statistical log information, such as authentication starts sent, aborts sent,etc, for TACACS+ client, use the command **show tacacs** in Privileged EXEC Mode.

show tacacs

Mode

Privileged EXEC Mode

Prerequisites

This command displays the information only for the servers configured in the TACACS server table.

Examples

iS5comm # show tacacs

```
    Server : 1
    Server address           : 12.0.0.100
    Address Type             : IPV4
    Single Connection : no
    TCP port          : 49
    Timeout           : 5
    Secret Key        :
    Server : 2
    Server address           : abc.google.com
    Address Type             : DNS
    Single Connection : yes
    TCP port          : 20
    Timeout           : 30
    Secret Key        :
    Active Server address: abc.google.com
    Authen. Starts sent    : 0
    Authen. Continues sent : 0
    Authen. Enables sent   : 0
    Authen. Aborts sent    : 0
    Authen. Pass rvcd.     : 0
    Authen. Fails rcvd.    : 0
    Authen. Get User rcvd. : 0
    Authen. Get Pass rcvd. : 0
```

```
Authen. Get Data rcvd. : 0
Authen. Errors rcvd.   : 0
Authen. Follows rcvd.  : 0
Authen. Restart rcvd.  : 0
Authen. Sess. timeouts : 0
Author. Requests sent  : 0
Author. Pass Add rcvd. : 0
Author. Pass Repl rcvd : 0
Author. Fails rcvd.    : 0
Author. Errors rcvd.   : 0
Author Follows rcvd.   : 0
Author. Sess. timeouts : 0
Acct. start reqs. sent : 0
Acct. WD reqs. sent    : 0
Acct. Stop reqs. sent  : 0
Acct. Success rcvd.    : 0
Acct. Errors rcvd.     : 0
Acct. Follows rcvd.    : 0
Acct. Sess. timeouts   : 0
Malformed Pkts. rcvd.  : 0
Socket failures        : 0
Connection failures    : 0
```

6.3. debug tacacs

To set the debug trace level for TACACS client module, use the command **debug tacacs** in Privileged EXEC Mode. The no form of the command disables the debug trace level for TACACS client module.

debug tacacs

```
debug tacacs {all | info | errors | dumptx | dumprx}
```

no debug radius

Parameters

Parameter	Type	Description
`all`		Enter to specify generating of debug messages for all possible traces (Dumptx, Dumprx, Error, Info).
`info`		Enter to specify generating of debug statements for server information messages such as TACACS session timed out, server unreachability, Session ID exceeded, etc.
`errors`		Enter to specify generating of traces for error debug messages such as failure caused during packet transmission and reception.
`dumptx`		Enter to specify generating of debug statements for handling traces. This trace is generated when there is an error condition in transmission of packets.
`dumprx`		Enter to specify generating of debug statements for handling traces. This trace is generated when there is an error condition in reception of packets.

Mode

Privileged EXEC Mode

Default

Debugging is disabled

Examples

iS5comm # debug tacacs all

SSH

7. SSH

SSH (Secure Shell) is a protocol for secure remote login and other secure network services over an insecure network. It consists of three major components:

- The Transport Layer Protocol provides server authentication, confidentiality and integrity.
- The User Authentication Protocol authenticates the client-side user to the server. It runs over the transport layer protocol.
- The Connection Protocol multiplexes the encrypted tunnel into several logical channels. It runs over the user authentication protocol.

A Secure Shell (SSH) configuration enables a SSH server and client to authorize the negotiation of only those algorithms that are configured from the allowed list. The client sends a service request once a secure transport layer connection has been established. A second service request is sent after user authentication is complete. This allows new protocols to be defined and coexist with these protocols.

7.1. ssh

To enable or disable SSH subsystem or perform SSH server-related configuration, use the command **ssh** in Global Configuration Mode.

ssh

```
ssh {enable | disable | server-address <ip-address> [port
<integer(1-65535)>]}
```

Parameters

Parameter	Type	Description
enable		Enter to enable ssh subsystem. When set to “enable”, the switch is accessible through ssh from remote location
disable		Enter to disable ssh subsystem. Setting ssh to disable, removes the ssh access to the switch.
server-address		Enter to configure the SSH server listening IP address.
<ip-address>		Enter the SSH server listening IP address.
port		Enter to configure the primary port number on which SSH server listens.
<integer(1-65535)>	Integer	Enter a number for the primary port number on which SSH server listens

Mode

Global Configuration Mode

Default

enable

Port 22

Examples

iS5comm(config)# ssh enable

iS5comm (config)# ssh server-address 12.0.0.0 port 1

7.2. show ssh

To display the SSH server listening IP address and port information, use the command **show ssh** in Privileged EXEC Mode.

show ssh

Mode

Privileged EXEC Mode

Examples

iS5comm # show ssh-configurations

```
SSH Listening IP 0.0.0.0
Port 22
```

7.3. show ssh-configurations

To display the SSH server listening IP address and port information, use the command **show ssh-configurations** in Privileged EXEC Mode.

show ssh-configurations

Mode

Privileged EXEC Mode

Examples

iS5comm # show ssh-configurations

```
SSH Listening IP 0.0.0.0
Port 22
```

7.4. show ip ssh

To display the SSH server information, such as version, cipher algorithm, authentication, and trace level, use the command **show ip ssh** in Privileged EXEC Mode.

show ip ssh

Mode

Privileged EXEC Mode

Examples

iS5comm # show ip ssh

```
Status          : SSH is Enabled
Version           : Both
Cipher Algorithm : AES128-CBC
Authentication    : HMAC-SHA1
Trace Level       : None
```

```
Max Byte Allowed :32768
```

7.5. ip ssh

To configure the various parameters associated with SSH server including secure socket layer (SSL) encryption ciphers, use the command **ip ssh** in Global Configuration Mode. The standard port used by SSH is 22. SSH server allows remote and secure configuration of the switch. The SSH server provides protocol version exchange, data integrity, cipher and key exchange algorithms negotiation between two communicating entities, key exchange mechanism, encryption and server authentication. The no form of the command resets the various parameters associated with the SSH server. Version 2 of SSH is supported.

ip ssh

```
ip ssh { cipher ([ALL] [DHE_RSA_AES256_SHA256] [ECDH_ECDSA_AES128_SHA256]
[ECDH_RSA_AES128_SHA256] [ECDH_RSA_AES256_SHA256] [ECDH_RSA_CHACHA20_PO-
LY1305])}
```

no ip ssh

```
no ip ssh { cipher ([ALL] [DHE_RSA_AES256_SHA256] [ECDH_ECDSA_AES128_SHA256]
[ECDH_RSA_AES128_SHA256] [ECDH_RSA_AES256_SHA256] [ECDH_RSA_CHACHA20_PO-
LY1305])}
```

Parameters

Parameter	Type	Description
cipher		Enter to configure a cipher or algorithm encryption. The SSL protocol supports a variety of different cryptographic algorithms, or ciphers, for use in operations such as authenticating the server and client to each other, transmitting certificates, and establishing session keys. Clients and servers may support different cipher suites, or sets of ciphers, depending on various factors such as the version of SSL they support, company policies, etc. The list of available cipher suites / lists is as follows:
DHE_RSA_AES256_SHA256		Enter for DHE_RSA_AES256_SHA256 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
ECDH_ECDSA_AES128_SHA256		Enter for ECDH_ECDSA_AES128_SHA256 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
ECDH_RSA_AES128_SHA256		Enter for ECDH_RSA_AES128_SHA256 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
ECDH_RSA_AES128_SHA256		Enter for ECDH_RSA_AES128_SHA256 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA256
ECDH_RSA_CHACHA20_POLY1305		Enter for ECDH_RSA_CHACHA20_POLY1305 Kx=ECDH Au=RSA Enc=CHACHA20/POLY1305(256)
ALL		Enter for All of the ciphers.

Mode

Global Configuration Mode

Default

- All

Examples

iS5comm (config)# ip ssh cipher ECDH_RSA_CHACHA20_POLY1305 DHE_RSA_AES256_SHA256

7.6. ip ssh pubkey-chain

To configure the SSH clients public key to be used for public key based authentication, use the command **ip ssh pubkey-chain** in Privileged EXEC Mode. The no form of the command disables the SSH clients public key that is to be used for public key based authentication.

ip ssh pubkey-chain

no ip ssh pubkey-chain

Mode

Privileged EXEC Mode

Examples

iS5comm # ip ssh pubkey-chain

7.7. debug ssh

To enable the trace levels for SSH, use the command **debug ssh** in Privileged EXEC Mode. System errors such as memory allocation failures are notified through LOG messages and TRACE messages. Interface errors and protocol errors are notified using TRACE messages. Setting all bits will enable all trace levels and resetting them will disable all trace levels. The no form of the command resets the SSH trace levels.

debug ssh

```
debug ssh {all | buffer | ctrl | data | dump | mgmt | resource | server |
shut}
```

no debug ssh

Parameters

Parameter	Type	Description
`all`		Enter to specify generating of debug messages for all possible traces.
`buffer`		Enter to specify generating of debug messages for allocation and freeing of buffer.
`ctrl`		Enter to specify generating of traces for Control Plane functionality traces.
`data`		Enter to specify generating of debug statements for data path.
`dump`		Enter to specify generating of debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.
`mgmt`		Enter to specify generating debug statements for management plane functionality traces.
`resource`		Enter to specify generating debug statements for traces for allocation and freeing of all resource except the buffers.
`server`		Enter to specify generating of debug statements while creating/ opening/ closing SSH server sockets and any failures to wake up SSH server sockets. Also generates debug statements during enabling /disabling of SSH server.
`shut`		Enter to specify generating of debug statements for shutdown traces. This trace is generated on successful shutting down of SSH related module and memory.

Mode

Privileged EXEC Mode

Default

Debugging is disabled

Examples

iS5comm # debug ssh all

SSL

8. SSL

SSL (Secure Sockets Layer) has been developed for transmitting private documents through Internet. It works by using a private key for encrypting data that is transferred over the SSL connection. By convention, URLs that require an SSL connection start with https: instead of http:

The SSL protocol is designed to provide privacy between two communicating applications (a client and a server) and authenticate the server, and optionally the client. SSL requires a reliable transport protocol (e.g., TCP) for data transmission and reception.

The advantage of the SSL protocol is that it is application protocol independent. A higher level application protocol (e.g., HTTP, FTP, TELNET and so on.) can layer on top of the SSL protocol transparently.

The SSL Protocol can negotiate an encryption algorithm and session key as well as authenticate a server before the application protocol transmits or receives its first byte of data. All of the application protocol data is transmitted encrypted, thus ensuring privacy.

8.1. show ssl server-cert

To display the SSL server certificate information, such as certificate, data, version, serial number, signature algorithm, etc, use the command **show ssl server-cert** in Privileged EXEC Mode. This command will display output only if SSL server certificate must had been created.

show ssl server-cert

Mode

Privileged EXEC Mode

Examples

iS5comm # show ssl server-cert

The output will be similar to the following image:

8.2. show ip http

To display the SSL status and configuration information, use the command **show ip http** in Privileged EXEC Mode. Information such as HTTP secure server status & http secure server cipher suite is displayed.

show ip http secure server status

Mode

Privileged EXEC Mode

Examples

iS5comm # show ip http secure server status

```
HTTP secure server status : Enabled
HTTP secure server port : 443
Minimum SSL Version : TLSv1.2
HTTP secure server ciphersuite : TLS_AES_128_GCM_SHA256
```

8.3. ip http

To set the HTTP port, use the command **ip http** in Global Configuration Mode. The no form of the command resets the HTTP port to its default value.

ip http

```
ip http {port <port-number (1-65535)> | secure (ciphersuite {TLS_ECDHE_R-
SA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 |
TLS_AES_256_GCM_SHA384 | TLS_CHACHA20_POLY1305_SHA256 | TLS_AES_128_GCM_-
SHA256 } | port (1-65535) | minimum version { TLSv1_2 | TLSv1_3 } | crypto
key RSA2048 { default | current | string values } server)}
```

no ip http

```
no ip http port | secure
```

Parameters

Parameter	Type	Description
port		Enter to configure HTTP port. his port is used to configure the router using the Web interface. The available port numbers are from 1 to 65535
<port-number (1-65535)>	Integer	Enter a port number. The available port numbers are from 1 to 65535 **NOTE:** TACACS user will be given root privilege by default or local user privilege if the user exists in local database
secure		Enter for SSL secure server related configuration. The options are as follows:
ciphersuite		Enter for Cipher-suites list options.
CR		Enter to disable SSL server on the device and also to disable ciphersuites and crypto key configuration. If you want to specify an encryption algorithm, enter one of the shown below options.
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384		Enter for this encryption algorithm.
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256		Enter for this encryption algorithm.
TLS_AES_256_GCM_SHA384		Enter for this encryption algorithm.
TLS_CHACHA20_POLY1305_SHA256		Enter for this encryption algorithm.
TLS_AES_128_GCM_SHA256		Enter for this encryption algorithm.
minimum version		This is used to specify the minimum level of TLS to be used. The choices are as follows.
TLSv1_2		TLS version 1.2
TLSv1_3		TLS version 1.3
rsa-with-aes-256-cbc-sha		Enter for this encryption algorithm.
crypto		Enter a name of the created list.
key		

Parameter	Type	Description
RSA2048		Enter for RSA algorithm.
default		This option will use the default RSA 2048 certificate values. A carriage return is entered after this option.
current		Use the current certificate subject name
Certificate Values are entered	A series of Strings	Up to 2 characters for the country code string Up to 100 characters for the state/province value Up to 100 characters for the city/locality value Up to 100 characters for the organization value Up to 100 characters for the organizational unit name Up to 100 characters for the common name
server		Enter to enable the SSL server on the device and also to configure the ciphersuites.
port		The port option when used after secure. For example “ip http secure port” allows the user to specify the port number of the HTTPS server. It is followed by a port number.
<port-number (1-65535)>	Integer	Value of the port number to be used by the HTTPs server.

Mode

Global Configuration Mode

Default

80

Prerequisites

HTTP port number configuration takes effect only when HTTP is disabled and enabled again

Examples

iS5comm(config)# ip http port 90

iS5comm(config)# ip http secure ciphersuite

For a new certificate to be used the http service must be disabled and then re-enabled. iS5comm(config)# no ip http secure server

iS5comm(config)# ip http secure server

8.4. crypto pki keygen

To create private keys and certificates which the switch can use for operations such as SSL, HTTPS, and IPSec.

crypto pki keygen

```
crypto pki keygen {name | {RSA2048 | RSA4096 } { default | <country(2)>
<state(100)> <locality(100)> <organization(100)> <organizational-unit(100)>
<common-name(100)> | current }
```

Parameters

Parameter	Type	Description
name	string	The prefix of the file name. 2 files are created prefixKey.pem and prefixCert.pem.
RSA2048 or RSA4096		Size of the key 2048 or 4096.
default		Certificate will be created with following default values: COUNTRY "CA" STATE "ONTARIO" LOCALITY "MISSISSAUGA" ORGANIZATION "iS5 COMMUNICATION INC" ORGANIZATIONAL_UNIT "ENGINEERING TEAM" COMMON_NAME “https://www.is5com.com”
<country(2)>		Country Code Attribute
<state(100)>		State Attribute
<locality(100)>		Locality Attribute
<organizational-unit(100)>		Organizational Unit Attribute
<common-name(100)>		Common Name Attribute
current		Use the Certificate attributes of the current certificate

Mode

Global Config Mode

Examples

iS5comm(config)# crypto pki keygen test1 RSA2048 default

Related Commands

show crypto pki

Example:

iS5comm# show crypto pki test1

8.5. crypto pki csrgen

This command is used to generate a certificate signing request.

crypto pki csrgen

```
crypto pki csrgen { file-prefix }
```

Parameters

Parameter	Type	Description
file-prefix	string	The filename to be signed. If the key is RaptorKey.pem, enter Raptor.

Mode

Global Config Mode

Examples

```
iS5comm# configure terminal
iS5comm(config)# crypto pki csrgen test1
-----BEGIN CERTIFICATE REQUEST-----
MIICzzCCAbcCAQIwgYkxCzAJBgNVBAYTAkNBMRAwDgYDVQQIDAdPTlRBUklPMRQw
EgYDVQQHDAtNSVNTSVNTQVVHQTEeMBwGA1UECgwVaVM1IENPTUlVTklDQVRJT04g
SU5DMRkwFwYDVQQLDBBFTkdJTkVFUklORyBURUFNMRcwFQYDVQQDDA53d3cuaXM1
Y29tLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANulFoy7Kjzs
fjwK0SLnlIeTrqWtg3eigfl+BONYVCnzkyrr/mAcPenmaNDZWfgxkJFjj30sux/B
OzoL25rprCORqDnZzAOE0yoeANCvP038G4m9BroHUYFN5I6g5lZO3aq7LRxCtW4w
9DS4+aJmzHOpdVhR7gXV/srRALscRwwergPIF3ILCnMtk3Mgq+7BF8oa/047+lRc
jEbI+yt2lSe3GEXTa24aaYrT3fvnZz/n8lJYiR2pPTl5gOjjqCsJcylCx2O9rvQO
g6+tWmaRXhMSBW+JsUtEI3O5stwSm3Lj006Gsex5lyn93LzORZR7nhcIeprMhVBu
piJKZlIXNjECAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQCMMKUo2ZAnGfVkZnda
XX9tz8r+CX8S/zp04E7XWtjGhp8x4SmrVVcU3rAfhGIc0eCFLufUtMTfTVlAnZfw
FolaN8fZHsppMcH2ykcycrpEIXDdmHxa5T8dehk4pSgIgjmgArPTYKtOSYB9oRhb
lCx79VGAtbEB7qBQFfaM3Hq6KTd732NLhyXjFUXC390UsFd4KY5tui3Z2J/f6wpn
e6ltkqpFuZPtqbk6PHt7h/iy5AGpl0dRFfdUSXxWUowS8UYcIGCrrNyYQxcpxlFT
5vk/2ij4IhAT5DTssTmuWO2TZ+vsvMPlCmex8GPW2KadhFmGF5zw0olvpV3MaCit
38AW
-----END CERTIFICATE REQUEST-----

iS5comm(config)#
```

8.6. crypto pki import

This command is used to import a certificate to the device.

crypto pki import

```
crypto pki import {key | cert | ca-cert}
```

Parameters

Parameter	Type	Description
key|cert|ca-cert	string	The file to be imported: a key, a cert or a ca-cert.
name	string	The name of the file to store. Limited to 32 characters.
file	string	If the file is to be installed via SFTP or USB then the path name of the file would be provided. If the path is not specified then the contents of the file can be pasted into the CLI directly.

Mode

Global Config Mode

Examples

iS5comm(config)# crypto pki import cert i1

Enter Cert:

-----BEGIN CERTIFICATE-----
MIIDlTCCAn2gAwIBAgIJAM5w8Azqdww5MA0GCSqGSIb3DQEBCwUAMIGJMQswCQYDVQQGEwJDQTEQMA4GA1UECAwHT05UQVJJTzEUMBIGA1UEBwwLTUlTU0lTU0FVR0ExHjAcBgNVBAoMFWlTNSBDT01NVU5JQ0FUSU9OIElOQzEZMBcGA1UECwwQRU5HSU5FRVJJTkcgVEVBTTEXMBUGA1UEAwwOd3d3LmlzNWNvbS5jb20wHhcNMjEwODA2MTIwNTExWhcNMjQwODA1MTIwNTExWjCBiTELMAkGA1UEBhMCQ0ExEDAOBgNVBAgMB09OVEFSSU8xFDASBgNVBAcMC01JU1NJU1NBVUdBMR4wHAYDVQQKDBVpUzUgQ09NTVVOSUNBVElPTiBJTkMxGTAXBgNVBAsMEEVOR0lORUVSSU5HIFRFQU0xFzAVBgNVBAMMDnd3dy5pczVjb20uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxDin2xPyY3v9X2zv974dyGQHg95psL1jq8aYRB/E4YmnaBMVnqT63cFBdQW3vL3y1NgBg/Pu33bfmBgW8NIlylkI8k3lCG58xsw80B5V0Tzzly5Do0VY8PlfiiPCg6XfPGIQLLeOPVc7woqK8MYkuEVgoi2HV1I0MK6ybNtZy5A+hRwIFiCpEWn77/Vy4yqRljsWRqSXIcPqH0mSQNonltw/XwHRn5Rqd65KZSDpe+hnXdxjsq2lF+olqR1+KQyh83fwI916Dcf23dpcYz6DaKYrJJfIQ2/Uccxa8qfzr3erkUxLQW9hwOWMtbG6ctbWfRSrEWbpx0/H4xZVftMZTQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBZ6yClyGiJMgO13Iei3J+1HbFuPS9fQHYeUzlYjK5ZNbMf53iHNdptdwrZuqm/hFqjjxNEzC96okEqncTgtvyiV7e/KEm/TyiA1WPUa/rk/g0aDwbkGR7K5I393SmKCkzfj/eEfa+4IdJxAqMjupSvI9w5naRIYWZf+bWzqNPoZnXL899gRGwrZdp5jhKQasDik48FztaZLVU5VDeTO3EfepkwRnwNjs8BHAgwzG39Y9k/wwUPw16KNRM0/vQVKIJqTZ1wQ3NJ4Tyx+Rr1NxxvgOo7Lh8t3uVbgqr1egZQDgz+skB2Xe8m6qJKj8-JFGs3Irs9Lq/Ma1rBZ1lTJF2xN

-----END CERTIFICATE-----

8.7. ip http secure crypto key

This command is used to specify the web server certificate and private key.

ip http secure crypto key

```
ip http secure crypto key <key-name> cert <cert-name>
```

Parameters

Parameter	Type	Description
key-name	string	HTTPS server private key file.
cert-name	string	HTTPS server certificate file.

Mode

Global Config Mode

Examples

```
iS5comm# show running-config ssl

#Building configuration...
!
ip http secure ciphersuite TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_W
ITH_CHACHA20_POLY1305_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256
 TLS_AES_128_GCM_SHA256
ip http secure crypto key HttpsKey.pem cert HttpsCert.pem
ip http secure server
!
end
iS5comm# c t
iS5comm(config)# ip http secure crypto key HttpsKey.pem cert HttpsCert.pem
% HTTPS service should be restarted for the changes to take effect
iS5comm(config)# exit
iS5comm# show ssl server-cert

 Certificate: HttpsCert.pem

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            d2:14:e5:2e:c5:51:7c:81
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CA, ST=ONTARIO, L=MISSISSAUGA, O=iS5 COMMUNICATION INC, OU=ENG
INEERING TEAM, CN=www.is5com.com
        Validity
            Not Before: May 19 18:45:24 2019 GMT
            Not After : May 18 18:45:24 2022 GMT
        Subject: C=CA, ST=ONTARIO, L=MISSISSAUGA, O=iS5 COMMUNICATION INC, OU=EN
GINEERING TEAM, CN=www.is5com.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c1:ce:26:a9:9f:2e:8a:9a:68:e0:0d:a4:0d:01:
                    f5:c6:94:d9:3e:23:53:71:3d:b2:57:0a:39:b8:73:
                    b8:9f:76:e5:d2:9e:92:c7:47:41:6a:93:be:f9:4d:
--More--
```

8.8. no crypto pki

This command is used to clear the certificates and keys from the device.

8.9. show crypto PKI

This command is used to list the certificates and keys on the device. It can also display the contents of individual certificate files.

show crypto pki

```
show crypto pki {name}
```

Parameters

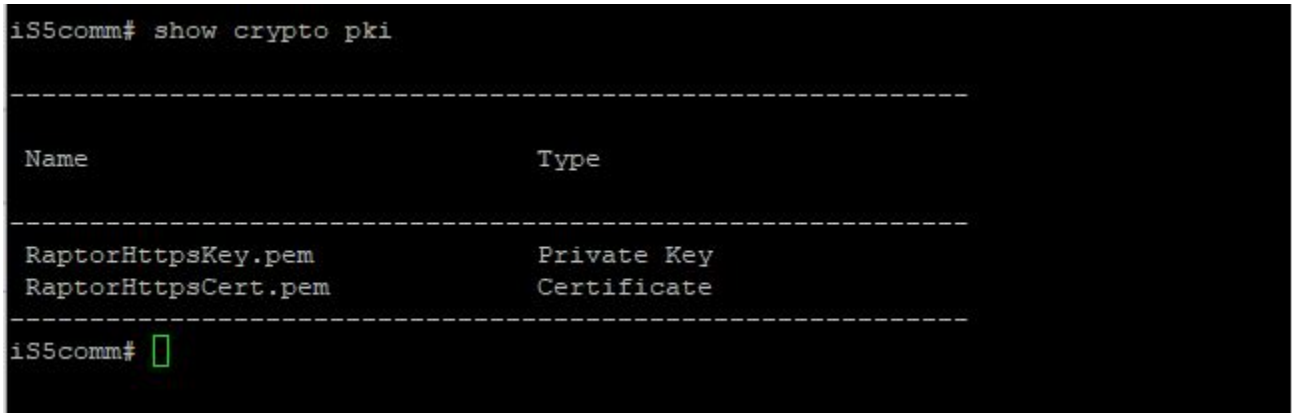
Parameter	Type	Description
name	string	The file name.

Mode

Privileged Exec Mode

Examples

iS5comm# show crypto pki



iS5comm# show crypto pki RaptorHttpsCert.pem

```
iS5comm# show crypto pki RaptorHttpsKey.pem

RaptorHttpsKey.pem: is not a SSL Certificate, CA Certificate or CSR
iS5comm# show crypto pki RaptorHttpsCert.pem

-----BEGIN CERTIFICATE-----
MIIDlTCCAn2gAwIBAgIJANsG4wyLk5zLMA0GCSqGSIb3DQEBCwUAMIGJMQswCQYD
VQQGEwJDQTEQMA4GA1UECAwHT05UQVJJTzEUMBIGA1UEBwwLTU1TU01TU0FVR0Ex
HjAcBgNVBAoMFW1TNSBDT01NVU5JQ0FUSU9OIE1OQzEZMBcGA1UECwwQRU5HSU5F
RVJJTkcgVEVBTTEXMBUGA1UEAwwOd3d3LmlzNWNvbS5jb20wHhcNMTkwNDI5MTc0
NjMyWhcNMjIwNDI4MTc0NjMyWjCBiTELMAkGA1UEBhMCQ0ExEDAOBgNVBAgMB09O
VEFSSU8xFDASBgNVBAcMC01JU1NJU1NBVUdBMR4wHAYDVQQKDBVpUzUgQ09NTVVO
SUNBVE1PTiBJTkMxGTAXBgNVBAsMEEVOR01ORUVSSU5HIFRFQU0xFzAVBgNVBAMM
Dnd3dy5pczVjb20uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
67gT9tSECUwmJCcEH8l/EMR9/vFENsqKoNj17u6jdlZ47mEN7mqJQxsBRMCyGF0S
uIPydzYmr0sFlxqh3UvbPWGjS9xBAcGE1A4009tuuH9x3gyeWey0UpwhmZ+zjJiY
q4Zul08LQ84Oh+/gAKstVTUP/goBeyB5fZFickfFXZ1tlrXgjz4h7/a9cz90BZCq
tBGxGfqgqbKwFjSr90DJoxHyXtwjiyK7AvN+EEkZkmlBPhK/K0xv5RdPqUuQVEue
OWh6KGYnZez5Kb+F2GHaTQV7O0FvEkDPcDlshsUGkRPyDaSoUILTIeDluUVeQIMe
tpNp7mESZH4dd5OAxubhPwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDCKZK0bafJ
WMco4pGbpvpceM/O5Tgfi+54U2E6FYSWcH6MeWH8gjtETWlptBnxWX1tj6lTzbSI
l32rSU4QlAdPWV4yUiHDy0njWQG7P/wBQos278Pjt3WEUMkCjcEhSl5lQaiV/HMO
rrUSCanfng8BXIsfAQmdhYglU46tWiRmwlbBpk6FT8yR8i/Jbe4m46Shl/EKh/i6
70VvebwaoDtskltwnLh83lfSjE8dDUAluKY7vvfofPwewLQETFLM/c2Wke3c7MV2
DYrdOAQnouLs5A5ZVb8zE65T7VNPDu/kKRaqo6+f+PhIRl3Hp3JZ5pXaB38nOAhK
OmxuyQMZhkZI
-----END CERTIFICATE-----
```

NOTE: The command also displays the certificate attributes which is not shown above.

SNTP

9. SNTP

The SNTP (Simple Network Time Protocol) is a simplified version or subnet of the NTP protocol. It is used to synchronize the time and date by contacting the SNTP Server. The administrator can choose whether to set the system clock manually or to enable SNTP. If SNTP is enabled, the SNTP implementation discovers the SNTP server and gets the time from the server. The SNTP implementation also has callouts to set the system time based on the time received from the SNTP server. It supports different time zones, where the user can set the required time zone.

9.1. sntp

To enter SNTP configuration mode which allows the user to execute all commands that support SNTP Configuration Mode, use the command **sntp** in Global Configuration Mode.

sntp

Mode

Global Configuration Mode

Examples

iS5comm (config)# sntp

iS5comm (config-sntp)#

9.2. set sntp

To configure in broadcast mode: SNTP delay time, SNTP broadcast mode status, and SNTP client poll interval; SNTP client module; in Manycast mode: SNTP client poll interval, Maximum retry poll count value, SNTP client poll timeout, and Server address; in Multicast mode: SNTP delay time, SNTP multicast group address, SNTP multicast mode status, and SNTP client poll interval; in Unicast mode: SNTP client maximum retry poll count, SNTP client maximum poll interval timeout, Unicast-poll-interval, and Unicast server related configuration, use the command **set sntp** in SNTP Configuration Mode. The no form of this command disables authentication and the Daylight Saving Time, resets the system time zone to GM, and

deletes the listening port for SNTP client and resets to the default value; for unicast server, it deletes the SNTP unicast server attributes and sets them to default values.

set sntp

```
set sntp {broadcast-delay-time [<value (1000-15000) microseconds>]

 | broadcast-mode send-request {enabled | disabled}

 | broadcast-poll-timeout [<value (1-30) seconds>]

 | client {addressing-mode {unicast | broadcast | multicast | manycast} |
authentication-key <key-id> md5 <key> | clock-format {ampm | hours} |
clock-summer-time <week-day-month,hh:mm (20)> | enabled | disabled | port
<port number(123|1025-65535)> | time-zone <random_str> | version {v1 | v2 |
v3 | v4}}

 | manycast-poll-interval [<value (16-16384) seconds>]

 | manycast-poll-retry-count [<value ((1-10)seconds>]

 | manycast-poll-timeout [<value ((1-30)seconds>]

 | manycast-server {broadcast | multicast {ipv4 [<mcast_addr>] | ipv6
[<ip6_addr>]

 | multicast-delay-time [<value (1000-15000) microseconds>]

 | multicast-group-address {ipv4 {A.B.C.D(<mcast_addr>) | default} | ipv6
{AAAA::BBBB(<ipv6_addr>) | default}}

 | multicast-mode send-request {enabled | disabled}

 | multicast-poll-timeout [<value (1-30) seconds>]

 | unicast-max-poll-retry <value (0-10) times>

 | unicast-max-poll-timeout <value (1-30) seconds>

 | unicast-poll-interval [<value (16-16384) seconds>]

 | unicast-server {ipv4 <ucast_addr> | ipv6 <ip6_addr> | domain-name <
dns_host_name>} [{primary | secondary}] [version {3 | 4} [port
<integer(1025-36564)>]}
```

no set sntp

```
no set sntp {client {authentication | clock-summer-time | port  | time-zone}
| unicast-server {ipv4 <ucast_addr> | ipv6 <ip6_addr> | domain-name <
dns_host_name>}
```

Parameters

Parameter	Type	Description
broadcast-mode		Enter to specify broadcast-mode.
send-request		Enter to specify that request packet is sent out to broadcast server
enabled		Enter to send the SNTP request packet to broadcast server to calculate the actual delay.
disabled		Enter to not send any SNTP request packet to broadcast server; instead the default value for the delay is taken. Disabled is default.
broadcast-delay-time		Enter to configure SNTP delay time or the time interval the SNTP client needs to wait for a response from the server
<value (1000-15000) microseconds>	Integer	Enter a value for delay time. This value ranges 1000 to 15000 microseconds.
broadcast-poll-timeout		Enter to configure SNTP client poll interval or the maximum interval to wait for a poll to be completed.
<value (1-30) seconds>	Integer	Enter a value for the maximum interval to wait for a poll to complete. This value ranges from 1 to 30 seconds. Default is 5.
client		Enter to set the addressing mode of SNTP client.
addressing-mode		Enter to configure the addressing mode of the SNTP client. The options are as follows. The default is Unicast.
unicast		Enter to configure the addressing mode of SNTP client as Unicast. A unicast client operates in a point-to-point fashion. It sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the round-trip delay and local clock offset relative to the server.
broadcast		Enter to configure the addressing mode of SNTP client as Broadcast. Broadcast operates in a point-to-multipoint fashion. The SNTP server uses an IP local broadcast address instead of a multicast address. The broadcast address is scoped to a single subnet, while a multicast address has Internet wide scope.
multicast		Enter to configure the addressing mode of SNTP client as Multicast. Multicast operates in point-to-multipoint fashion. The SNTP server uses a multicast group address to send unsolicited SNTP messages to clients. The client listens on this address and sends no requests for updates.

Parameter	Type	Description
manycast		Enter to configure addressing mode of SNTP client as Manycast. Manycast operates in a multipoint-to-point fashion. The SNTP client sends a request to a designated IPv4 or IPv6 local broadcast address or multicast group address. One or more manycast servers reply with their individual unicast addresses.
authentication-key		Enter to configure the authentication parameters for the key. Some SNTP severs requires authentication to be done before exchanging any data. This authentication key is used to authenticate the client to the SNTP server to which it tries to connect. By default, Authentication key ID is not set.
<key-id>	Integer	Enter a value for key identifier for providing authentication for the server and identifying the cryptographic key used to generate the message-authentication code. This value ranges from 1 to 65535.
md5		Enter to configure the authentication type as md5 (Message Digest-5) where data integrity is verified. MD5 is intended to be used with digital signature applications that require that large files are compressed by a secure method before being encrypted with a secret key under a public key cryptosystem.
<key>		Enter to configure the authentication code as a key value. This value is a string.
clock-format		Enter to configure the system clock as either am/ pm or hours format.
ampm		Enter to configure the system clock in am/ pm format
hours		Enter to configure the system clock in 24 hours format.
clock-summer-time		Enter to enable the DST (Daylight Saving Time). DST is a system of setting clocks ahead so that both sunrise and sunset occur at a later hour. The effect is additional daylight in the evening. The dates of DST may change from year to year.
<week-day-month,hh:mm (20)		Enter to configure the DST time. This value is a string of maximum size of 20. The input should be in the format listed below; • week—First, Second, Third, Fourth or Last week of month. • day—Sunday, Monday, Tuesday, Wednesday, Thursday, Friday or Saturday. • month—January, February, March, April, May, June, July, August, September, October, November or December. • hh:mm—time in hours and minutes.

Parameter	Type	Description
enabled		Enter to enable SNTP client module and sends a request to the host for time synchronization.
disabled		Enter to disable SNTP client module and no request is sent to the host for time synchronization.
port		Enter to modify the Client Port setting. It sets the listening port for SNTP client that refers to a port on a server awaiting a client connection. **NOTE:** Listening port for SNTP client should be 123 or greater than 1024, where the port below 1024 are reserved.
<port number (123|1025-65535)>	Integer	Enter a client port number value. This value is 123 or ranges from 1025 to 65535. Default is 123.
time-zone		Enter to configure the system time zone with respect to UTC.
<random_str>		Enter values as follows. The default is + 00: 00. • +/- —sets the client time zone as after or before UTC. Plus indicates forward time zone and minus indicates backward time zone. • UTC-offset value as —sets the UTC offset value in hours: – +00:00 to +14:00 – -00:00 to -12:00
version		Enter to configure the operating version of the SNTP for the client.
v1		Enter to configure the version of SNTP client as 1.
v2		Enter to configure the version of SNTP client as 2.
v3		Enter to configure the version of SNTP client as 3.
v4		Enter to configure the version of SNTP client as 4. This is default.
manycast-poll-interval		SNTP client poll interval which is the maximum interval between successive messages.
<value (16-16384) seconds>	Integer	Enter a value for the maximum interval between successive messages. The poll interval value ranges from 16 to 16384 seconds, where the poll interval value is expressed in exponent of two. The default is 64.
manycast-poll-retry-count		Enter to configure SNTP poll retries count which is the maximum number of unanswered polls that cause a slave to identify the server as dead.

Parameter	Type	Description
<value ((1-10) seconds>	Integer	Enter a value for poll retries before identifying a server as dead. This value ranges from 1 to 10 seconds. The default is 3.
manycast-poll-timeout		Enter to configure SNTP client poll timeout which is the maximum interval to wait for a poll to complete
<value ((1-30)seconds>	Integer	Enter a value for SNTP clientpoll timeout. This value ranges from 1 to 30 seconds. The default is 5.
manycast-server		Enter to configure SNTP multicast or broadcast server address in manycast mode.
broadcast		Enter to configure an SNTP broadcast server address in manycast mode.
multicast		Enter to configure an SNTP multicast server address in manycast mode.
ipv4		Enter to configure the multicast server address in IPv4.
<mcast_addr>	A.B.C.D	Enter a value for the multicast server address in IPv4.
ipv6		Enter to configure the multicast server address in IPv6.
<ip6_addr>	AAAA::BBBB	Enter a value for the multicast server address in IPv6.
multicast-delay-time		Enter to configure SNTP delay time in which there is no response from the multicast server.
<value (1000-15000) microseconds>	Integer	Enter to configure a value for the delay time with no response. This value ranges from 1000 to 15000 microseconds. The default is 8000.
multicast-group-addres		Enter to configure an SNTP multicast server address in multicast mode.
ipv4		Enter to configure the multicast server address in IPv4.
<mcast_addr>	A.B.C.D	Enter a value for the multicast server address in IPv4.
default		Enter for default value
ipv6		Enter to configure the multicast server address in IPv6.
<ip6_addr>	AAAA::BBBB	Enter a value for the multicast server address in IPv6.
default		Enter for default value
multicast-mode		Enter to configure the status of sending the request to the multicast server to calculate the delay time.

Parameter	Type	Description
send-request		Enter to specify sending the request.
enabled		Enter to send the SNTP request packet to multicast server to calculate the actual delay.
disabled		Enter for not sending any SNTP request packets to multicast server; instead the default value for the delay is taken. The default is Disabled.
multicast-poll-timeout		Enter to configure SNTP client poll interval in multicast mode which is the maximum interval to wait for the poll to complete.
<value (1-30) seconds>	Integer	Enter a value for the poll timeout interval. This value ranges from 1 to 30 seconds. The default value is 5.
unicast-max-poll-retry		Enter to configure SNTP client maximum retry poll count which is the maximum number of unanswered polls that cause a slave to identify the server as dead.
<value (0-10) times>	Integer	Enter a value for maximum poll retries before identifying a server as dead. This value ranges from 0 to 10 times. The default is 3.
unicast-max-poll-timeout		Enter to configure SNTP client maximum poll interval timeout which is the maximum interval to wait for the poll to complete.
<value (1-30) seconds>	Integer	Enter a value for maximum poll interval timeout. This value ranges from 1 to 30 seconds. The default is 5.
unicast-poll-interval		Enter to configure the SNTP unicast poll interval. The interval is the time between successive SNTP request transmissions in seconds
<value (16-16384) seconds>	Integer	Enter a value for the SNTP unicast poll interval. This value ranges from 16 to 16384 seconds and is expressed as exponent of two. The default is 64.
unicast-server		Enter to configure an SNTP unicast server.
ipv4		Enter to configure the address type of the unicast server as IPv4.
<ucast_addr>	A.B.C.D	Enter a valid IPv4 address. **NOTE:** One unicast server can be configured for an address type.
ipv6		Enter to configure the address type of the unicast server as IPv6.
<ip6_addr>		Enter a valid IPv6 address. **NOTE:** One unicast server can be configured for an address type.
domain-name		Enter to configure the domain name for the unicast server.

Parameter	Type	Description
< dns_host_name>		Enter a domain name. This value is a string with the maximum size as 255
primary		Enter to configure the unicast server type as primary server.
secondary		Enter to configure the unicast server type as secondary server.
version		Enter to configure the SNTP version.
3	Integer	Enter 3 to configure the SNTP version as 3.
4	Integer	Enter 4 to configure the SNTP version as 4. This is the default.
port		Enter to configure the port identifier for the selected server
<integer(1025-36564)>	Integer	Enter a value for port identifier. This value ranges from 1025 to 36564.

Mode

SNTP Configuration Mode

Examples

iS5comm(config)# sntp

iS5comm (config-sntp)# set sntp client enabled

iS5comm (config-sntp)# set sntp client version v3

iS5comm (config-sntp)# set sntp client addressing-mode unicast

iS5comm (config-sntp)# set sntp client port 1026

iS5comm (config-sntp)# set sntp client clock-format hours

iS5comm (config-sntp)# set sntp client time-zone +05:30

iS5comm (config-sntp)# set sntp client clock-summer-time First-Sun-Jan,12:12 Second-Sun-Mar,12:12

iS5comm (config-sntp)# set sntp client authentication-key 123 md5 iS5Com

iS5comm (config-sntp)# set sntp unicast-server auto-discovery enabled

iS5comm (config-sntp)# set sntp unicast-poll-interval 128

iS5comm (config-sntp)# set sntp unicast-max-poll-timeout 25

iS5comm (config-sntp)# set sntp unicast-max-poll-retry 10

iS5comm (config-sntp)# set sntp unicast-server ipv4 12.0.0.100 Primary version 3 port 1234

iS5comm (config-sntp)# set sntp broadcast-mode send-request enabled

iS5comm (config-sntp)# set sntp broadcast-poll-timeout 30

iS5comm (config-sntp)# set sntp broadcast-delay-time 2000

iS5comm (config-sntp)# set sntp multicast-mode send-request enabled

iS5comm (config-sntp)# set sntp multicast-poll-timeout 10

iS5comm (config-sntp)# set sntp multicast-delay-time 2000

iS5comm (config-sntp)# set sntp multicast-group-address ipv4 224.1.1.10

iS5comm (config-sntp)# set sntp manycast-poll-interval 256

iS5comm (config-sntp)# set sntp manycast-poll-timeout 10

iS5comm (config-sntp)# set sntp manycast-poll-retry-count 5

iS5comm (config-sntp)# set sntp manycast-server multicast ipv4 224.0.0.1

9.3. show sntp

To display the status of SNTP in broadcast, manycast, multicast, and unicast modes, the SNTP status, or show the current time, use the command **show sntp** in Privileged EXEC Mode.

show sntp

```
show sntp {broadcast-mode status | clock | manycast-mode status | multi-
cast-mode status | statistics | status | unicast-mode status}
```

Parameters

Parameter	Type	Description
broadcast-mode		Enter to display information about the broadcast mode.
status		Enter to display information about the broadcast mode.
clock		Enter to display the current time of the SNTP clock
manycast-mode		Enter to display information about the manycast mode.
status		Enter to display information about the manycast mode.
multicast-mode		Enter to display information about the multicast mode.
status		Enter to display information about the multicast mode.
statistics		Enter to display information about the statistics.
status		Enter to display information about the statistics.
unicast-mode		Enter to display information about the unicast mode.
status		Enter to display information about the unicast mode.

Mode

Privileged EXEC Mode

Examples

iS5comm # show sntp broadcast-mode status

```
send sntp request to server in broadcast mode is disabled
broadcast poll time out value is 5
broadcast delay time value is 8000
broadcast sntp server is 12.0.0.100
```

iS5comm# show sntp clock

```
current time : Mon Feb 03 2020 18:06:12.000 (UTC +00:00)
```

iS5comm# show sntp manycast-mode status

```
manycast poll interval value is 64
manycast max poll time out value is 5
manycast max retry time value is 3
manycast server type is  broadcast
primary server address is 12.0.0.100
```

iS5comm# show sntp multicast-mode status

```
send sntp request to server in multicast mode is disabled
multicast poll time out value is 5
multicast delay time value is 8000
multicast group address is 12.0.0.100
```

iS5comm# show sntp statistics

```
Number of SNTP server-reply Received       : 0
Number of SNTP client-request Transmitted  : 0
Number of SNTP Pkt InDiscards              : 0
```

iS5comm# show sntp status

```
sntp client is disabled
current sntp client version is v4
current sntp client addressing mode is unicast
sntp client port is 123
sntp client clock format is 24 hours
sntp client authentication key id not set
sntp client authentication algorithm is not set
sntp client auth Key is not set
sntp client time zone is  +00:00
sntp client dst start time is not set
sntp client dst end time is not set
```

iS5comm# show sntp unicast-mode status

```
auto discovery of sntp/ntp servers is disabled
unicast poll interval value is 64
unicast max poll time out value is 5
unicast max retry time value is 3
unicast current mode value is NOT RUNNING
```

9.4. debug sntp

To enable tracing in SNTP module for all debug levels, use the command **debug sntp** in Privileged EXEC Mode. The no form of the command disables the tracing in SNTP module as per the configured debug levels, or if the command is **no debug sntp all**, disables the tracing in SNTP module for all debug levels.

debug sntp

```
debug sntp {all | all-fail | buff | control | data-path | init-shut | mgmt |
resource}
```

no debug sntp

```
no debug sntp {all | all-fail | buff | control | data-path | init-shut |
mgmt | resource}
```

Parameters

Parameter	Type	Description
`all`		Enter to specify generating of debug statements for all possible messages.
`all-fail`		Enter to specify generating of debug statements for all failure traces.
`buff`		Enter to specify generating of debug statements for SNTP buffer related traces.
`control`		Enter to specify generating of debug statements for control path traces. This trace is generated during failure in modification or retrieving of SNTP entries.
`data-path`		Enter to specify generating of debug statements for data path traces. This trace is generated during failure in packet processing.
`init-shut`		Enter to specify generating of debug statements for init and shutdown traces. This trace is generated on failed initialization and shutting down of SNTP related entries
`mgmt`		Enter to specify generating debug statements for management traces. This trace is generated during failure in configuration of any of the SNTP features.
`resource`		Enter to specify generating debug statements for traces for allocation and freeing of all resource except the buffers.

Mode

Privileged EXEC Mode

Default

Debugging is disabled

Examples

iS5comm # debug sntp init-shutl

iS5comm# debug sntp all

iS5comm# no debug sntp all

PTP_CLI

10. PTP

The RAPTOR supports end-to-end and peer-to-peer transparent clocks.

End-to-end (E2E) transparent clocks forward PTP messages, measure the residence time of PTP event message at the transparent clock, and add this residence time to the correction field of the PTP messages. Transparent clock timestamps the event messages on ingress and egress port. The difference between these timestamps is the residence time within the transparent clock. End-to-end transparent clocks will not execute port state machine and BMC algorithm to select the state of the port.

End-to-end transparent clocks may be used as a network element, or they may be associated with application devices such as sensors or actuators if an ordinary clock is combined with the end-to-end transparent clock.

Peer-to-peer transparent clock differs from the end-to-end transparent clock in the way it corrects and handles the timing messages. End-to-end transparent clock time stamps all PTP timing messages; peer-to-peer transparent clock forwards only Sync and Follow-up messages.

Peer-to-peer transparent clock calculates the residence time of PTP messages in peer-to-peer transparent clock, measures the link delay of the ingress port of PTP messages, and adds this correction field in the PTP messages. Peer-to-peer transparent clock uses Pdelay request-response mechanism to measure the link delay. It uses rate estimation and control mechanism to avoid the residence time error.

The following sections describe all PTP CLI configuration commands including show and debug PTP.

10.1. ptp

To enter PTP configuration mode which allows the user to execute all commands that support PTP Configuration Mode, use the command **ptp** in Global Configuration Mode.

ptp

```
ptp
 {domain
 {(0-127) | <CR> | power-profile  {clear | exit | help | no | ptp
 {mode {e2etransparent | p2ptransparent} | transparent max-ports <id (0-24)>
| vlan {<id (1-4094)> | priority <id (0-7)>}}
 | profile
 DefaultE2E | DefaultP2P | PowerProfileV2 | Reset | UtilityProfile}
```

}

Mode

Global Configuration Mode

Parameters

Parameter	Type	Description
domain		Enter to configure a PTP domain related configuration information.
(0-127)	Integer	Enter a value for a PTP Domain ID. The range is from 1 to 127.
<CR>		Enter to create a PTP domain in a virtual context.
power-profile		Enter to select a PTP power profile as per IEEE C37.238-2017.
clear		Enter to clear the PTP power profile.
exit		Enter to exit the PTP power profile.
help		Enter for help on the commands for the PTP power profile.
no		Enter to delete the PTP power profile.
ptp		Enter to select to enable PTP on the PTP power profile.
mode		Enter to select the mode option.
e2etransparent		Enter to select the e2etransparent option which stands for end-to-end mode (E2E). Select it when the time taken for a PTP event message to transit the device is to be measured.
p2ptransparent		Enter to select the p2ptransparent option which stands for peer-to-peer (P2P)transparent mode. Select it when the link delay between two ports implementing link delay is to be measured.
transparent		Enter to select transparent clock.
max-ports		Enter to select the maximum ports option.
id (0-24)		Enter a value for the maximum ports number. The range is from 0 to 24. The maximum and default is 24.
vlan		PTP requests and responses can be sent over a specific VLAN on switch. Enter this option when VLAN configuration is to be implemented on a specific PTP domain.
id (1-4094)		Enter a value for VLAN ID. The range is from 1 to 4094.
priority		Enter to set the VLAN priority option.
id (0-7)		Enter a value for VLAN priority. The range is from 0 to 7.
profile		Enter PTP profile-related configuration option.
DefaultE2E		Enter to select Default End-to-End profile as per IEEE 1588-Annex J.
DefaultP2P		Enter to select Default P2P profile as per IEEE 1588-Annex J.

Parameter	Type	Description
PowerProfileV2		Enter to select C37-238-2017 Profile.
Reset		Enter to reset the profile.
UtilityProfile		Enter to select 61850-9-3:2016 compliant profile.

Examples

To globally enable PTP, type the following.

iS5comm(config)# no shutdown ptp

iS5comm (config)# ptp profile PowerProfileV2

iS5comm(config-ptp)# ptp vlan 10

iS5comm(config-ptp)# ptp vlan priority 4

iS5comm# show running-config ptp

```
#Building configuration...
!
!
no shutdown ptp
ptp domain power-profile
ptp vlan 10
ptp vlan priority 4
ptp mode p2ptransparent
!
interface  gigabitethernet 0/1
ptp enable
ptp min-pdelay-req-interval 2
!
end
```

Enter the following commands to remove VLAN 10

iS5comm(config)# ptp domain 0

iS5comm(config)# ptp domain power-profile

iS5comm(config-ptp)# no ptp vlan 10

or

iS5comm(config-ptp)# no ptp vlan

iS5comm(config-ptp)# no ptp vlan priority

10.2. ptp (interfaces)

To enter PTP configuration mode which allows the user to execute all commands that support PTP Configuration Mode at the interfaces, use the command **ptp**.

ptp

```
ptp {enable | min-pdelay-req-interval <exponent-Of-2-seconds (0-5)> |
port-statistcs-cnt-reset}
```

Mode

Interface Configuration Mode

Parameters

Parameter	Type	Description
enable		Enable PTP on a given interface
min-pdelay-req-interval		Configure the minimum pdelay request interval. This parameter is followed by a value in the range of 0-5. It represents the delay interval calculated from the equation 2^X in seconds.
exponent-Of-2-seconds (0-5)		Enter a value in the range of 0-5.
port-statistcs-cnt-reset		This command reset the statistics (counters) for the port.

Examples

S5comm (config)# int gigabitethernet 0/1

iS5comm (config-if)# ptp enable

iS5comm (config-if)# ptp port-statistics-cnt-reset

10.3. show ptp

To display the status of PTP, use the command **show ptp** in Privileged EXEC Mode.

show ptp

```
show ptp {clock | counters | global info | null-management | port | profile
| transparent max-ports}
```

Parameters

Parameter	Type	Description
clock		Enter this option for PTP clock related Information.
counters		Enter this option for PTP Port counter related Information.
global		Enter this option for PTP related global Information.
info		Enter this option for PTP global Information.
null-management		Enter this option for Management type.
port		Enter this option for PTP port properties Information. Specific ports or all port properties can be displayed.
profile		Enter this option for PTP profile related Information
transparent		Enter this option for transparent clock
max-ports		Enter this option for maximum ports supported in transparentclock.

Mode

Privileged EXEC Mode

Examples

iS5comm# show ptp clock

```
 PTP Clock Information
-------------------------Clock Identity               :
e8:e8:75:ff:fe:90:5f:82
 Clock Context               : 0
 Clock Domain                : 254
 Primary Domain              : 254
 Clock Mode                  : Transparent
 Type Of Clock               : One Step
 Delay Mechanism             : Peer to Peer
 Number of PTP ports         : 0
 Number of max PTP TS ports  : 24
```

iS5comm# show ptp counters

```
 PTP Interface Counters
 ----------------------
Interface  gigabitethernet 0/1:Number of modified Egress packet with
updated correction field:
```

```
Number of dropped Egress packets: 0
Number of saved time stamp Ingress packet: 0
Number of dropped Ingress packets: 0
Number of dropped Ingress packets (VLAN mismatch): 0
Number of dropped Egress packets (VLAN mismatch): 0
Number of dropped packets (Domain Mismatch) : 0
Number of received Sync packets: 0
Number of transmitted Sync packets: 0
Number of received Peer delay request packets: 0
Number of transmitted Peer delay request packets: 0
Number of received Peer delay response packets: 0
Number of transmitted Peer delay response packets: 0
Number of received Peer delay response Follow Up packets: 0
Number of transmitted Peer delay response Follow Up packets: 0
```

iS5comm# show ptp global info

```
 PTP System Status
-----------------
Global Status      : Enabled
Network Protocol   : IEEE 802.3
Domain             : 254
VlanId             : 10
Priority           : 4
```

iS5comm# show ptp null-management

```
Getting PTP Null Management DONE
Setting PTP Null Management DONE
Applying PTP Null Management DONE
```

iS5comm# show ptp port gigabitethernet 0/1

```
 PTP Transparent Port Properties
 -------------------------------
Record # 1       Interface            : Gi0/1       Faulty Flag
: 0       LogMinPdelayReqInterval: 2 (4 sec)       Status
: ENABLED        Clock Identity         : e8:e8:75:ff:fe:90:5f:82
Peer Mean Path Delay   : 0 nsec        Clock type             : P2P
TRANSPARENT        PhysicalAddress        : not specified        SW
revision            : V2
```

iS5comm# show ptp profile

```
PTP Profile
-----------
 Profile Name                        : PowerProfileV2 (C37.238-2017)
 Profile ID                          : 1c:12:9d:00:00:00
```

```
    Default Domain Number                 : 254
    VlanId                                : 10
    Priority                              : 4
    Default Min pDelay Request Interval   : 0
    Default Delay Mechanism               : Peer-to-Peer
```

iS5comm# show ptp transparent max-ports

```
    PTP TS max port number: 24
```

10.4. debug ptp

To enable tracing in PTP module for all debug levels, use the command **debug ptp all** in Privileged EXEC Mode. The no form of the command disables the tracing in PTP module as per the configured debug levels, or if the command is **no debug ptp all**, disables the tracing in PTP module for all debug levels.

debug ptp

```
debug ptp {all | critical | port}
```

no debug ptp

```
no debug ptp {all | critical | port}
```

Parameters

Parameter	Type	Description
`all`		All trace messages.
`critical`		Critical trace messages.
`port`		Port specific trace messages.

Mode

Privileged EXEC Mode

Default

Debugging is disabled

Examples

iS5comm # debug ptp all

iS5comm# no debug ptp all

SNMPv3

11. SNMPv3

SNMP (Simple Network Management Protocol) is the most widely-used network management protocol on TCP/IP-based networks.

SNMPv3 is designed mainly to overcome the security shortcomings of SNMPv1/v2. USM (User based Security Model) and VACM (View based Access Control Model) are the main features added as part of the SNMPv3 specification. USM provides both encryption and authentication of the SNMP PDUs (protocol data units), while VACM specifies a mechanism for defining access policies for different users with different MIB trees.

Also, SNMPv3 specifies a generic management framework, which is expandable for adding new Management Engines, Security Models, Access Control Models and so on. With SNMPv3, the SNMP communication is completely safe and secure.SNMPv3 is a multilingual agent supporting all three versions of SNMP (SNMPv1, SNMPv2c and SNMPv3) while conforming to the latest specifications. It is available as a portable source code product, which can be easily integrated to any platform (any OS and any Processor).

MIB integration is made simple with the aid of a tool called Middle Level Code Generator (MIDGEN), which is available along with SNMP. MIDGEN generates the interface stubs required for every object in the MIB for the SET, GET and GETNEXT operations.These stubs can be implemented by the respective modules supporting the MIB.

SNMP is provided as source code available for licensing to OEMs and VARs who wish to incorporate the multi-lingual SNMP functionality into their products.

11.1. SNMP Traps

This section describes the SNMP traps used on the switch.

Introduction

The switch supports a number of traps that indicate alarm or condition changes on the device. This section will list out those traps and describe how they are generated.

General SNMP configuration for TRAP Generation

This is applicable for all traps

```
iS5comm# configure terminal
iS5comm(config)# enable SnmpAgent
```

```
iS5comm(config)# snmp user snmpv3 auth md5 AUTHPASSWD
iS5comm(config)# snmp community index index3 name testv3 security snmpv3
iS5comm(config)# snmp group testv3 user snmpv3 security-model v3
nonvolatile
iS5comm(config)# snmp access testv3 v3 auth read iso write iso notify iso
iS5comm(config)# snmp targetaddr ht8 param pa8 5.0.0.5 taglist tg8
iS5comm(config)# snmp targetparams pa8 user snmpv3 security-model v3 auth
message-processing v3
iS5comm(config)# snmp notify testv3 tag tg8 type Trap
```

NOTE: *Commands to enable the alarm traps*

```
iS5comm(config)# alarm config-type switch relay enable
iS5comm(config)# alarm config-type switch LED enable
iS5comm(config)# alarm config-type chassis relay enable
iS5comm(config)# alarm config-type chassis LED enable
iS5comm(config)# alarm config-type protocol relay enable
iS5comm(config)# alarm config-type protocol LED enable
iS5comm(config)# alarm config-type service relay enable
iS5comm(config)# alarm config-type service LED enable
```

NOTE: *Commands to enable the authentication failure trap*

```
iS5comm(config)# snmp engineId 80.00.08.1c.04.46.54
iS5comm(config)# snmp user proxyuser1
iS5comm(config)# snmp group proxygroup user proxyuser1 security-model v2c
iS5comm(config)# snmp access proxygroup v2c read getview write getview
iS5comm(config)# snmp view getview 1 mask 1 included volatile
iS5comm(config)# snmp community index COMM2 name COMM2 security proxyuser1
contextengineid 80.00.08.1c.04.46.54
iS5comm(config)# exit
iS5comm#
```

NOTE: IP address 5.0.0.5, used above, is the IP through which the SNMP manager could be reached. This IP address is being used as an example only.

Line Module Trap

A Line Module TRAP will be generated, whenever a Line Module is inserted or Removed.Below are the corresponding MIB IDs that would be mentioned, in the generated TRAP.

- lineModuleNo - 1.3.6.1.4.1.41094.0.250.27.3.6
- lmInsertStatus - 1.3.6.1.4.1.41094.0.250.27.3.7

Steps to Generate the Line Module Trap

1) Remove a line module, to generate TRAP for Line Module Removal Event.
2) Insert the removed line module, to generate TRAP for Line Module Insertion Event.

Packet Capture

- **1.3.6.1.2.1.1.3.0**: 16600 ---> sysUpTime
  - Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
  - Value (Timeticks): 16600 ---> Total System UP Time in ticks
- **1.3.6.1.6.3.1.1.4.1.0**: 1.3.6.1.4.1.41094.0.250.27.3.6 (iso.3.6.1.4.1.41094.0.250.27.3.6)
  - Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0) --> snmpTrap OID
  - Value (OID): 1.3.6.1.4.1.41094.0.250.27.3.6 (iso.3.6.1.4.1.41094.0.250.27.3.6) -> Line module trap OID
- **1.3.6.1.4.1.41094.0.250.27.3.6**: ---> Line module Trap OID
  - Object Name: 1.3.6.1.4.1.41094.0.250.27.3.6 (iso.3.6.1.4.1.41094.0.250.27.3.6)
  - Value (Integer32): 1 -> Line module ID
- **1.3.6.1.4.1.41094.0.250.27.3.7**: --> Line module connect Status
  - Object Name: 1.3.6.1.4.1.41094.0.250.27.3.7 (iso.3.6.1.4.1.41094.0.250.27.3.7)
  - Value (Integer32): 2 ---> Connect Status as UP (1) or DOWN (2)
- **1.3.6.1.6.3.1.1.4.3.0**: 1.3.6.1.2.1.11 (iso.3.6.1.2.1.11) --> snmpTrapEnterprise
  - Object Name: 1.3.6.1.6.3.1.1.4.3.0 (iso.3.6.1.6.3.1.1.4.3.0)
  - Value (OID): 1.3.6.1.2.1.11 (iso.3.6.1.2.1.11) ---> snmp OID

Warm Start

The Warm Start TRAP will be generated, whenever “reload” command is issued.Below is the corresponding MIB ID that would be mentioned, with the TRAP generated.

- issWarmStart - 1.3.6.1.4.1.41094.0.250.2.120.11

Steps to generate the Warm Start trap

1) Execute “reload” command

Packet Capture

- **1.3.6.1.2.1.1.3.0**: 54887 ---> sysUpTime
  - Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
  - Value (Timeticks): 54887 ---> Total System UP Time in ticks
- **1.3.6.1.6.3.1.1.4.1.0**: 1.3.6.1.4.1.41094.0.250.2.120.11 (iso.3.6.1.4.1.41094.0.250.2.120.11)
  - Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0) --> snmpTrap OID
  - Value (OID): 1.3.6.1.4.1.41094.0.250.2.120.11 (iso.3.6.1.4.1.41094.0.250.2.120.11) --> Warm start MIB OID
- **1.3.6.1.4.1.41094.0.250.2.120.11**: --> Warm start MIB OID
  - Object Name: 1.3.6.1.4.1.41094.0.250.2.120.11 (iso.3.6.1.4.1.41094.0.250.2.120.11)
  - Value (Integer32): 1

- **1.3.6.1.6.3.1.1.4.3.0**: 1.3.6.1.2.1.11 (iso.3.6.1.2.1.11) --> snmpTrapEnterprise
  - Object Name: 1.3.6.1.6.3.1.1.4.3.0 (iso.3.6.1.6.3.1.1.4.3.0)
  - Value (OID): 1.3.6.1.2.1.11 (iso.3.6.1.2.1.11) ---> snmp OID

Alarm Trap

An Alarm TRAP will be generated, whenever any kind of alarm is generated. Here we validated the alarm module trap, with alarm generation for LINK UP and LINK DOWN event. Below are the corresponding MIB IDs that would be mentioned, with the TRAP generated.

- alarmTraps - 1.3.6.1.4.1.41094.0.250.258.3.1
- alarmId - 1.3.6.1.4.1.41094.0.250.258.2.1.1.2
- alarmDesc - 1.3.6.1.4.1.41094.0.250.258.2.1.1.4
- alarmTimeStr - 1.3.6.1.4.1.41094.0.250.258.2.1.1.5
- alarmPriority - 1.3.6.1.4.1.41094.0.250.258.2.1.1.6
- alarmGenModule - 1.3.6.1.4.1.41094.0.250.258.2.1.1.7

Steps to generate the Alarm trap

1) Bring up an interface to generate the LINK UP event
2) Bring down an interface to generate the LINK DOWN event

Packet Capture

- **1.3.6.1.2.1.1.3.0**: 43567 ---> sysUpTime
  - Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
  - Value (Timeticks): 43567 ---> Total System UP Time in ticks
- **1.3.6.1.6.3.1.1.4.1.0**: 1.3.6.1.4.1.41094.0.250.258.3.1 (iso.3.6.1.4.1.41094.0.250.258.3.1)
  - Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0) --> snmpTrap OID
  - Value (OID): 1.3.6.1.4.1.41094.0.250.258.3.1 (iso.3.6.1.4.1.41094.0.250.258.3.1) -> alarm-Traps MIB OID
- **1.3.6.1.4.1.41094.0.250.258.2.1.1.2**: --> alarmId
  - Object Name: 1.3.6.1.4.1.41094.0.250.258.2.1.1.2 (iso.3.6.1.4.1.41094.0.250.258.2.1.1.2)
  - Value (Integer32): 3000
- **1.3.6.1.4.1.41094.0.250.258.2.1.1.4:**4769302f3920496e7465726616365204c696e6b20537461...
  - Object Name: 1.3.6.1.4.1.41094.0.250.258.2.1.1.4 (iso.3.6.1.4.1.41094.0.250.258.2.1.1.4) ---> alarmDesc
  - Value (OctetString): 4769302f3920496e7465726616365204c696e6b20537461...
- **1.3.6.1.4.1.41094.0.250.258.2.1.1.5**: --> alarmTimeStr 4170722f31382f32333a33363a3533200000000000000000
  - Object Name: 1.3.6.1.4.1.41094.0.250.258.2.1.1.5 (iso.3.6.1.4.1.41094.0.250.258.2.1.1.5)
  - Value (OctetString): 4170722f31382f32333a33363a3533200000000000000000

- **1.3.6.1.4.1.41094.0.250.258.2.1.1.6**: --> alarmPriority
  - Object Name: 1.3.6.1.4.1.41094.0.250.258.2.1.1.6 (iso.3.6.1.4.1.41094.0.250.258.2.1.1.6)
  - Value (Integer32): 2
- **1.3.6.1.4.1.41094.0.250.258.2.1.1.7**: --> alarmGenModule
  - Object Name: 1.3.6.1.4.1.41094.0.250.258.2.1.1.7 (iso.3.6.1.4.1.41094.0.250.258.2.1.1.7)
  - Value (Integer32): 2
- **1.3.6.1.6.3.1.1.4.3.0**: 1.3.6.1.2.1.11 (iso.3.6.1.2.1.11) --> snmpTrapEnterprise
  - Object Name: 1.3.6.1.6.3.1.1.4.3.0 (iso.3.6.1.6.3.1.1.4.3.0)
  - Value (OID): 1.3.6.1.2.1.11 (iso.3.6.1.2.1.11) ---> snmp OID

Power Supply Trap

The Power supply TRAP will be generated, whenever a Power module is inserted or removed.Below are the corresponding MIB IDs that would be mentioned, with the TRAP generated.

- issTrapPowerSupply - 1.3.6.1.4.1.41094.0.250.2.120.6
- issPowerSupplyPresence - 1.3.6.1.4.1.41094.0.250.2.121.132
- issPowerSupplyActive - 1.3.6.1.4.1.41094.0.250.2.121.133

Steps to generate the Power Supply trap

1) Remove a power module to generate POWER module removal event
2) Insert a power module to generate POWER module insertion event

Packet Capture

- **1.3.6.1.2.1.1.3.0**: 129754 ---> sysUpTime
  - Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
  - Value (Timeticks): 129754 ---> Total System UP Time in ticks
- **1.3.6.1.6.3.1.1.4.1.0**: 1.3.6.1.4.1.41094.0.250.2.120.6 (iso.3.6.1.4.1.41094.0.250.2.120.6)
  - Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0) --> snmpTrap OID
  - Value (OID): 1.3.6.1.4.1.41094.0.250.2.120.6 (iso.3.6.1.4.1.41094.0.250.2.120.6) --> issTrap-PowerSupply
- **1.3.6.1.4.1.41094.0.250.2.121.132**: ---> issPowerSupplyPresence
  - Object Name: 1.3.6.1.4.1.41094.0.250.2.121.132 (iso.3.6.1.4.1.41094.0.250.2.121.132)
  - Value (Integer32): 0
- **1.3.6.1.4.1.41094.0.250.2.121.133**: ---> issPowerSupplyActive
  - Object Name: 1.3.6.1.4.1.41094.0.250.2.121.133 (iso.3.6.1.4.1.41094.0.250.2.121.133)
  - Value (Integer32): 0
- **1.3.6.1.6.3.1.1.4.3.0**: 1.3.6.1.2.1.11 (iso.3.6.1.2.1.11) --> snmpTrapEnterprise
  - Object Name: 1.3.6.1.6.3.1.1.4.3.0 (iso.3.6.1.6.3.1.1.4.3.0)

  - Value (OID): 1.3.6.1.2.1.11 (iso.3.6.1.2.1.11) ---> snmp OID

Cold Start Trap

The Cold Start TRAP will be generated, whenever the image is reloaded after doing SNMP configurations for TRAP and “write-startup” is done. Below is the corresponding MIB ID that would be mentioned, with the TRAP generated.

- coldStart - 1.3.6.1.6.3.1.1.5.1

Steps to generate the Cold Start trap

1) Execute “reload” command

Packet Capture

- **1.3.6.1.2.1.1.3.0**: 1419 ---> sysUpTime
  - Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
  - Value (Timeticks): 1419 ---> Total System UP Time in ticks
- **1.3.6.1.6.3.1.1.4.1.0**: 1.3.6.1.6.3.1.1.5.1 (iso.3.6.1.6.3.1.1.5.1)
  - Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0) --> snmpTrap OID
  - Value (OID): 1.3.6.1.6.3.1.1.5.1 (iso.3.6.1.6.3.1.1.5.1) ---> coldStart MIB OID
- **1.3.6.1.6.3.1.1.4.3.0**: 1.3.6.1.2.1.11 (iso.3.6.1.2.1.11) --> snmpTrapEnterprise
  - Object Name: 1.3.6.1.6.3.1.1.4.3.0 (iso.3.6.1.6.3.1.1.4.3.0)
  - Value (OID): 1.3.6.1.2.1.11 (iso.3.6.1.2.1.11) ---> snmp OID

Authentication Failure Trap

An Authentication failure TRAP will be generated, whenever the SNMP connectivity cannot be established due to Authentication failures. Below is the corresponding MIB ID that would be mentioned, with the TRAP generated.

- authenticationFailure - 1.3.6.1.6.3.1.1.5.5

Steps to generate the Authentication trap

1) Execute below command to enable Authentication trap
   - snmp-server enable traps snmp authentication
2) Execute below command from linux, to invoke error in authentication
   - snmpwalk -c COMM1 -v2c 7.0.0.1 iso

NOTE: *Here the community name configured is COMM2, but from LINUX, we are trying to authenticate with COMM1, which would cause a authentication failure.*

Packet Capture

- **1.3.6.1.2.1.1.3.0**: 1419 ---> sysUpTime
  - Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
  - Value (Timeticks): 1419 ---> Total System UP Time in ticks

- **1.3.6.1.6.3.1.1.4.1.0**: 1.3.6.1.6.3.1.1.5.5 (iso.3.6.1.6.3.1.1.5.5)
  - Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0) --> snmpTrap OID
  - Value (OID): 1.3.6.1.6.3.1.1.5.5 (iso.3.6.1.6.3.1.1.5.5) --> authenticationFailure OID
- **1.3.6.1.6.3.1.1.4.3.0**: 1.3.6.1.2.1.11 (iso.3.6.1.2.1.11) --> snmpTrapEnterprise
  - Object Name: 1.3.6.1.6.3.1.1.4.3.0 (iso.3.6.1.6.3.1.1.4.3.0)
  - Value (OID): 1.3.6.1.2.1.11 (iso.3.6.1.2.1.11) ---> snmp OID

Link UP / DOWN Trap

A LINK UP / LINK DOWN TRAP will be generated, whenever any interface is brought UP or DOWN. Below is the corresponding MIB ID that would be mentioned, with the TRAP generated.

- linkUp - 1.3.6.1.6.3.1.1.5.4
- linkDown - 1.3.6.1.6.3.1.1.5.3
- ifIndex - 1.3.6.1.2.1.2.2.1.1.<ifindex>
- ifAdminStatus - 1.3.6.1.2.1.2.2.1.7.<ifIndex
- ifOperStatus - 1.3.6.1.2.1.2.2.1.8.<ifIndex>

Steps to generate the Link UP/DOWN trap

1) Bring DOWN an active interface through command “shutdown”
2) Bring UP the same interface through command “no shutdown”

Packet Capture (for link UP)

- **1.3.6.1.2.1.1.3.0**: 136427
  - Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
  - Value (Timeticks): 136427
- **1.3.6.1.6.3.1.1.4.1.0**: 1.3.6.1.6.3.1.1.5.4 (iso.3.6.1.6.3.1.1.5.4)
  - Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0) --> snmpTrap OID
  - Value (OID): 1.3.6.1.6.3.1.1.5.4 (iso.3.6.1.6.3.1.1.5.4) --> linkup MIB OID
- **1.3.6.1.2.1.2.2.1.1.9**: --> ifIndex MIB OID
  - Object Name: 1.3.6.1.2.1.2.2.1.1.9 (iso.3.6.1.2.1.2.2.1.1.9)
  - Value (Integer32): 9
- **1.3.6.1.2.1.2.2.1.7.9**: --> ifAdminStatus MIB OID
  - Object Name: 1.3.6.1.2.1.2.2.1.7.9 (iso.3.6.1.2.1.2.2.1.7.9)
  - Value (Integer32): 1
- **1.3.6.1.2.1.2.2.1.8.9**: --> ifOperStatus MIB OID
  - Object Name: 1.3.6.1.2.1.2.2.1.8.9 (iso.3.6.1.2.1.2.2.1.8.9)
  - Value (Integer32): 1
- **1.3.6.1.6.3.1.1.4.3.0**: 1.3.6.1.2.1.11 (iso.3.6.1.2.1.11) --> snmpTrapEnterprise

  - Object Name: 1.3.6.1.6.3.1.1.4.3.0 (iso.3.6.1.6.3.1.1.4.3.0)
  - Value (OID): 1.3.6.1.2.1.11 (iso.3.6.1.2.1.11) ---> snmp OID

Spanning Tree Trap

The Spanning tree topology change trap is generated whenever we shut / no shut a port, change the priority of any bridge to invoke new root selection, new port role selection, etc.

Steps to generate the Spanning Tree trap

1) Change spanning priority to invoke New ROOT bridge selection
2) Bring DOWN an active interface through command “shutdown”
3) Bring UP the same interface through command “no shutdown”

Packet Capture

Below are the MIBs that will be mentioned for different kind of traps from PVRST.

- fsPvrstTopologyChgTrap - 1.3.6.1.4.1.41094.0.250.161.3.0.4
- fsPvrstBrgAddress - 1.3.6.1.4.1.41094.0.250.161.1.4
- fsPvrstInstTopChanges - 1.3.6.1.4.1.41094.0.250.161.1.14.1.11
- fsFuturePvrstTraps - 1.3.6.1.4.1.41094.0.250.161.3
- fsPvrstNewRootTrap - 1.3.6.1.4.1.41094.0.250.161.3.0.3
- fsPvrstInstDesignatedRoot - 1.3.6.1.4.1.41094.0.250.161.1.14.1.16
- fsPvrstNewPortRoleTrap - 1.3.6.1.4.1.41094.0.250.161.3.0.7
- fsPvrstOldRoleType - 1.3.6.1.4.1.41094.0.250.161.2.5.1.2
- fsPvrstPortRoleType - 1.3.6.1.4.1.41094.0.250.161.2.5.1.1

- data: sNMPv2-Trap (7)
  - sNMPv2-Trap
    - request-id: 1436813334
    - error-status: noError (0)
    - error-index: 0
    - variable-bindings: 5 items

Item #1

- name: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)
- valueType: value (0)
  - value: simple (4294967295)
  - value: simple (4294967295)
    - application-wide: timeticks-value (3): timeticks-value: 1120239

Item #2

- name: 1.3.6.1.6.3.1.1.4.1.0 (SNMPv2-MIB::snmpTrapOID.0)

- valueType: value (0)
  - value: simple (4294967295)
    - simple: objectID-value (2): Value: OID: SNMPv2-SMI::enterprises.41094.0.250.161.3.0.4

Item #3

- name: 1.3.6.1.4.1.41094.0.250.161.1.4 (SNMPv2-SMI::enterprises.41094.0.250.161.1.4)
- valueType: value (0)
  - value: simple (4294967295)
    - simple: string-value (1): Value: Hex-STRING: E8 E8 75 90 2B 01

Item #4

- name: 1.3.6.1.4.1.41094.0.250.161.1.14.1.11.1 (SNMPv2-SMI::enterprises.41094.0.250.161.1.14.1.11.1)
- valueType: value (0)
  - value: simple (4294967295)
    - simple: integer-value (0): Value: INTEGER: 6

Item #5

- name: 1.3.6.1.6.3.1.1.4.3.0 (SNMPv2-MIB::snmpTrapEnterprise.0)
- valueType: value (0)
  - value: simple (4294967295)
    - simple: objectID-value (2): Value: OID: SNMPv2-SMI::enterprises.41094.0.250.161.3

Temperature Trap

The temperature trap will be generated whenever the temperature of the hardware exceeds the High threshold limit or falls lesser than the minimum threshold limit. Below is the corresponding MIB ID that would be mentioned, with the TRAP generated.

- issTrapTemperature - 1.3.6.1.4.1.41094.0.250.2.120.4
- issSwitchMinThresholdTemperature - 1.3.6.1.4.1.41094.0.250.2.121.64
- issSwitchMaxThresholdTemperature - 1.3.6.1.4.1.41094.0.250.2.121.65
- issSwitchCurrentTemperature - 1.3.6.1.4.1.41094.0.250.2.121.66

Steps to generate the Temperature trap

1) Check the current temperature of the hardware using command “show env all”
2) Set the Max temperature threshold limit as lesser than the current temperature, to generate trap, using the below command.

```
set switch temperature max threshold <value>
```

Packet Capture

- data: sNMPv2-Trap (7)
  - sNMPv2-Trap
    - request-id: 1821105562

- error-status: noError (0)
- error-index: 0
- variable-bindings: 5 items

Item #1

- name: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)
- valueType: value (0)
  - value: simple (4294967295)
  - value: simple (4294967295)
    - application-wide: timeticks-value (3):timeticks-value: 7814

Item #2

- name: 1.3.6.1.6.3.1.1.4.1.0 (SNMPv2-MIB::snmpTrapOID.0)
- valueType: value (0)
  - value: simple (4294967295): simple: objectID-value (2)
    - Value: OID: SNMPv2-SMI::enterprises.41094.0.250.2.120.4 ---> issTrapTemperature

Item #3

- name: 1.3.6.1.4.1.41094.0.250.2.121.64 (SNMPv2-SMI::enterprises.41094.0.250.2.121.64) ---> issSwitchMinThresholdTemperature
- valueType: value (0)
  - value: simple (4294967295):simple: integer-value (0)
    - Value: INTEGER: -35

Item #4

- name: 1.3.6.1.4.1.41094.0.250.2.121.65 (SNMPv2-SMI::enterprises.41094.0.250.2.121.65) ---> issSwitchMaxThresholdTemperature
- valueType: value (0)
  - value: simple (4294967295):simple: integer-value (0)
    - Value: INTEGER: 40

Item #5

- name: 1.3.6.1.4.1.41094.0.250.2.121.66 (SNMPv2-SMI::enterprises.41094.0.250.2.121.66) ---> issSwitchCurrentTemperature
- valueType: value (0)
  - value: simple (4294967295):simple: integer-value (0)
    - Value: INTEGER: 41

Port Security Traps

Item #1

- ifSwitchPortSecRecoveryStatus OBJECT-TYPE
  - SYNTAX INTEGER { automatic(1), manual(2) }

  - MAX-ACCESS read-write
  - STATUS current
  - DESCRIPTION
    - specifies the recovery mode for the ports in the system, when port-violation mode configured with shut-down. The value 1 indicates authomatic, the port will bring-up after the user configured time or the default time. The value 2 indicates manual, The users have to do no shutdown to bring up the port.
  - DEFVAL { manual }
  - ::= { if 37 }

Item #2

- ifSwitchPortSecRecoveryTime OBJECT-TYPE
  - SYNTAX Integer32
  - MAX-ACCESS read-write
  - STATUS current
  - DESCRIPTION
    - The value indicates the the recovery time for a port, from shut-down state that occurred due to a port-security violation, to up-state, upon the mode configured as automatic in ifSwitchPortSecRecoveryStatus
  - DEFVAL { 5 }
  - ::= { if 38 }

Item #3

- dot1qFutureVlanPortUnicastMacLimitStatus OBJECT-TYPE
  - SYNTAX EnabledStatus
  - MAX-ACCESS read-write
  - STATUS current
  - DESCRIPTION
    - A truth value indicating the unicast MAC limit learning enabled/disabled status for this port
  - DEFVAL { enabled }
  - ::= { dot1qFutureVlanPortEntry 17 }

Item #4

- dot1qFutureVlanPortUnicastMacLimit OBJECT-TYPE
  - SYNTAX Unsigned32 (0..3000)
  - MAX-ACCESS read-write
  - STATUS current
  - DESCRIPTION

        - The limiting value on the number of distinct unicast MAC addresses learnt in a VLAN. The lower limit and upper limit value that can be SET for this object is determined by the underlying hardware.
    - ::= { dot1qFutureVlanPortEntry 18 }

Item #5

- dot1qFutureVlanPortSecureStatus OBJECT-TYPE
    - SYNTAX EnabledStatus
    - MAX-ACCESS read-write
    - STATUS current
    - DESCRIPTION
        - A truth value indicating the port-security status enabled/disabled status for this port. When port security is disabled, trusted MAC settings and MAC learn limit settings are not applicable.
    - DEFVAL { disabled }
    - ::= { dot1qFutureVlanPortEntry 19 }

Item #6

- dot1qFutureSwitchPortSecViolationTrap NOTIFICATION-TYPE
    - OBJECTS { dot1qFutureVlanPort }
    - STATUS current
    - DESCRIPTION
        - This trap is generated when Port security is enabled on the port and violation occurred for a configured number of times
    - ::= { dot1qVlanTraps 4 }

Item #7

- MIB for Trap-syslog status configuration
    - dot1qFutureVlanPortSecTrapSyslogStatus OBJECT-TYPE
    - MAX-ACCESS read-write
    - STATUS current
    - DESCRIPTION
        - A truth value indicating the trap and syslog status for port-security violation is enabled, and so traps and syslog will be generated when violations occur. When this status for port-secuirty violation is disabled, traps and syslogs will not be sent upon violation.
    - DEFVAL { disabled }
    - ::= { dot1qFutureVlan 10 }

Item #8

- MIB for Trap, syslog rate configuration
    - dot1qFutureVlanPortSecTrapSyslogRate OBJECT-TYPE
    - SYNTAX Integer32 (1..10)

- MAX-ACCESS read-write
- STATUS current
- DESCRIPTION
  - TrapSyslog rate is the value, for the Max no. of Traps and Syslog that could be sent in a second, with violation events. The range of trap syslog rate could be configured is from 1 to 10
- ::= { dot1qFutureVlan 11 }

11.2. disable snmpagent

To disable SNMP agent , use the command **disable snmpagent** in Global Configuration Mode.

disable

```
disable snmpagent
```

Parameters

Parameter	Type	Description
snmpagent		Enter to disable SNMP agent.

Mode

Global Configuration Mode

Examples

iS5comm (config)# disable snmpagent

11.3. enable snmpagent

To enable SNMP agent that provides an interface between a SNMP manager and a switch, use the command **enable snmpagent** in Global Configuration Mode.

enable

```
enable snmpagent
```

Parameters

Parameter	Type	Description
snmpagent		Enter to enable SNMP agent which provides an interface between a SNMP manager and a switch. The agent processes SNMP packets received from the manager, frames the appropriate response packets, and sends them to the manager. By default, the SNMP agent is enabled.

Mode

Global Configuration Mode

Default

SNMP agent is enabled

Examples

iS5comm (config)# enable snmpagent

11.4. show mib

To display the name of the corresponding MIB object identifier and the OID (Object Identifier) of the corresponding MIB object name, use the command **show mib** in Privileged Exec Mode.

show mib

```
show mib {name <name string (32)> | oid <oid string (32)>}
```

Parameters

Parameter	Type	Description
name		Enter to display the MIB object name.
<name string (32)>	String	Enter an MIB object name. This is a string value with maximum size of 32.
oid		Enter to display the MIB object identifier
<oid string (32)>	String	Enter an MIB object identifier. This is a string value with maximum size of 32.

Mode

Privileged Exec Mode

Examples

iS5comm# show mib oid fsbgp4PeerExtTable

```
MIB OID for fsbgp4PeerExtTable is 1.3.6.1.4.1.41094.0.250.41.2
```

11.5. show snmp

To display the status information of SNMP communications, use the command **show snmp** in Privileged EXEC Mode.

show snmp

```
show snmp [agentx {information | statistics}] [community] [engineid]
[filter] [group [access]] [inform statistics] [mibproxy] [notif] [proxy]
[proxy-udp-port] [targetaddr] [targetparam] [traps] [user] [viewtree]
```

Mode

Privileged EXEC Mode

Examples

iS5comm # show snmp agentx information

```
Agentx Subagent is enabled
TransportDomain   :TCP
Master IP Address :10.0.0.2
```

```
    Master PortNo     :705
```

iS5comm# show snmp agentx statistics

```
    Tx Statistics
    Transmitted Packets               :860
    Open PDU                          :1
    Index Allocate PDU                :0
    Index DeAllocate PDU              :0
    Register PDU                      :2
    Add Agent Capabilities PDU        :0
    Notify PDU                        :0
    Ping PDU                          :20
    Remove Agent Capabilities PDU     :0
    UnRegister PDU                    :0
    Close PDU                         :0
    Response PDU                      :837
    Rx Statistics
    Rx Packets                        :859
    Get PDU                           :1
    GetNext PDU                       :836
    GetBulk PDU                       :0
    TestSet PDU                       :0
    Commit PDU                        :0
    Cleanup PDU                       :0
    Undo PDU                          :0
    Dropped Packets                   :0
    Parse Drop Errors                 :1
    Open Fail Errors                  :0
    Close PDU                         :0
    Response PDU                      :2
```

iS5comm# show snmp community

```
    Community Index : NETMAN
    Community Name  : NETMAN
    Security Name   : none
    Context Name    :
    Context EngineID: 80.00.08.1c.04.46.53
    Transport Tag   :
    Storage Type    : Nonvolatile
    Row Status      : Active
    ------------------------------
    Community Index : PUBLIC
```

```
    Community Name  : PUBLIC
    Security Name   : none
    Context Name    :
    Context EngineID: 80.00.08.1c.04.46.53
    Transport Tag   :
    Storage Type    : Nonvolatile
    Row Status      : Active
```

iS5comm# show snmp filter

```
    Filter Name  : filter1
    Subtree OID  : 1.5
    Subtree Mask : 1.1
    Filter Type  : Included
    Storage Type : Non-volatile
    Row Status   : Active
    ------------------------------
```

iS5comm# show snmp engineID

```
    EngineId: 80.00.08.1c.04.46.53
```

iS5comm# show snmp group access

```
    Group Name   : iso
    Read View    : iso
    Write View   : iso
    Notify View  : iso
    Storage Type : Nonvolatile
    Row Status   : Active
    ------------------------------
    Group Name   : noAuthUser
    Read View    : restricted
    Write View   : restricted
    Notify View  : restricted
    Storage Type : Nonvolatile
    Row Status   : Active
```

iS5comm# show snmp inform statistics

```
    Target Address Name  : iS5Commanager
    IP Address           : 10.0.0.10
    Inform messages sent : 20
    Acknowledgement awaited for : 2 Inform messages
    Inform messages dropped : 0
    Acknowledgement failed for : 0 Inform messages
    Informs retransmitted: 0
```

```
    Inform responses received: 18
```

iS5comm# show snmp mibproxy

```
    Prop Proxy Name                : mibproxy1
    Prop MibID                     : 1
    Prop Proxy TargetParamIn       : param1
    Prop Proxy SingleTargetOut     : target2
    Prop Proxy MultipleTargetOut   :
    Prop Proxy Type                : Read
    Prop Storage Type              : Nonvolatile
    Prop Row Status                : Active
    -----------------------------------------------------
```

iS5comm# show snmp notif

```
    Notify Name: iS5Com
    Notify Tag: iS5Com
    Notify Type: trap
    Storage Type: volatile
    Row Status: active
    ---------------------------
    Notify Name: iS5Com1
    Notify Tag: iS5Com1
    Notify Type: trap
    Storage Type: volatile
    Row Status: active
```

iS5comm# show snmp proxy

```
    Proxy Name                : proxy1
    Proxy ContextEngineID     : 80.00.08.1c.04.46.53
    Proxy ContextName         :
    Proxy TargetParamIn       : param2
    Proxy SingleTargetOut     : target2
    Proxy MultipleTargetOut   :
    Proxy Type                : Write
    Storage Type              : Nonvolatile
    Row Status                : Active
    -----------------------------------------------------
```

iS5comm# show snmp proxy

```
    snmp-server proxy-udp-port : 162
```

iS5comm# show snmp targetaddr

```
    Target Address Name : ht231
    IP Address          : 12.0.0.100
```

```
Port                : 150
Tag List            : tg231
Parameters          : pa231
Storage Type        : Non-volatile
Row Status          : Active
------------------------------
```

iS5comm# show snmp targetparam

```
Target Parameter Name    : internet
Message Processing Model : v2c
Security Model           : v2c
Security Name            : none
Security Level           : No Authentication, No Privacy
Storage Type             : Nonvolatile
Row Status               : Active
Filter  Profile Name     : None
Row Status               : Active
```

iS5comm# show snmp tcp

```
snmp over tcp disabled
snmp trap over tcp disabled
snmp listen tcp port 161
Snmp listen tcp trap port 162
```

iS5comm# show snmp traps

```
Currently enabled traps:
------------------------
coldstart
```

iS5comm# show snmp user

```
Engine ID               : 80.00.08.1c.04.46.53
User                    : noAuthUser
Authentication Protocol : None
Privacy Protocol        : None
Storage Type            : Nonvolatile
Row Status              : Active
------------------------------
```

iS5comm# show snmp viewtree

```
View Name    : iso
Subtree OID  : 1
Subtree Mask : 1
View Type    : Included
Storage Type : Nonvolatile
```

```
Row Status   : Active
-----------------------------
View Name    : restricted
Subtree OID  : 1
Subtree Mask : 1
View Type    : Included
Storage Type : Nonvolatile
Row Status   : Active
-----------------------------
```

11.6. show snmp-server

To display the proxy UDP port number and the set of traps that are currently enabled, use the command **show snmp-server** in Privileged EXEC Mode.

show snmp-server

```
show snmp-server {proxy-udp-port | traps}
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show snmp-server proxy-udp-port

```
snmp-server proxy-udp-port : 162
```

iS5comm# show snmp-server traps

```
Currently enabled traps:
------------------------
coldstart
```

11.7. snmp

To configure the SNMP, use the command **snmp** in Global Configuration Mode. The no form of the command removes the SNMP configuration details.

Use the **snmp** command to configure the following:

- access—SNMP group access configuration
- agent—SNMP agent related configuration
- community—SNMP community configuration
- enable — Enables the feature

- engineid — SNMP engine ID configuration
- filter — Filter related Configuration
- filterprofile—SNMP notify filter table configuration
- group—SNMP group related configuration
- mib— Management Information Base related configuration
- mibproxy—SNMP MIB proxy related configuration
- notify— SNMP notification details configuration
- proxy— SNMP proxy related configuration
- targetaddr— SNMP target address configuration
- targetparams — SNMP target parameter related configuration
- trap—Trap related configuration
- user—SNMP user details configuration
- view—SNMP view related configuration

snmp

```
snmp {access <string(32)> {v1 | {v2c | v3 {auth | noauth | priv} [context
<string(32)>] [nonvolatile] [volatile] [notify <string(32)>] [read
<string(32)>] [write <string (32)>]}} | agent port <port number (1-65535)>

 | {community index <community index ID (string (32)> name <community name
string)> security <string(32)> [context <Name >] [{volatile | nonvolatile}]
[transporttag <TransportTagIdentifier | none>] [contextengineid <Contex-
tEngineID>]

 | enable traps {coldstart | snmp authentication}

 | engineid <engine ID (string)>

 | filter {<filter profile name string (32)> <object Id string> {excluded
[nonvolatile] [volatile] |included [nonvolatile] [volatile] | mask <OID mask
23 (string)> {excluded [nonvolatile] [volatile] |included [nonvolatile]
[volatile]} | {trap {name <mib OID name(string)> | oid <OID name(string)>
{excluded [nonvolatile] [volatile] |included [nonvolatile] [volatile] | mask
<OID mask 23 (string)>}

 | filterprofile {<filter profile name string (32)> <object Id string>
{excluded [nonvolatile] [volatile] |included [nonvolatile] [volatile] | mask
<OID mask(string)> {excluded [nonvolatile] [volatile] |included [nonvola-
tile] [volatile]}

 | group <Group name string(32)> user <user name string(32)> security-model
{v1 | v2c | v3 [nonvolatile] [volatile]}

 | mib name {<mib Object name (string)> | <proxy id string (32)> [count
<count value (1-100>] [proxytype {{inform | read | trap | write} mibid <MIB
ID string> targetparamsin <target ID string (32)> targetout <target ID string
(32)> [storagetype {nonvolatile |volatile}] [short] [value <mib object
(string)]
```

| mibproxy name {<mib Object name (string)> | <proxy id string (32)> [count <count value (1-100>] [proxytype {{inform | read | trap | write} mibid <MIB ID string> targetparamsin <target ID string (32)> targetout <target ID string (32)> [storagetype {nonvolatile |volatile}]

| notify <notification namestring(32)> tag <tag name string(32)>] type {Inform | Trap} [nonvolatile] [volatile]

| proxy name <proxy name (string (30))> proxytype {inform | read | trap | write} contextengineid <contextengine ID> targetparamsin <target ID string (32)> targetout <target ID string (32)> [contextname <ProxyContextName (string>] [storagetype {nonvolatile |volatile}] [contextname <context name string (32)>

| targetaddr <target address string (32)> param <SNMP param name string (32)> {<dns_host_name> | A.B.C.D (<ucast_addr>) | AAAA::BBBB <ipv6_addr>} [nonvolatile] [port <port number (1-65535)>] [retries <retry count value (1-3)>] [taglist <tag ID string (255)>] [timeout] <Timeout value (1-1500)>] [volatile]

| targetparams <SNMP param string (32)> user <user name string (32)> security-model {v1 | v2c | v3 {auth | noauth |priv} message-processing {v1 | v2c | v3 [filterprofile-name <filterprofile-name string (32)> [filter-storagetype {nonvolatile | volatile}] [nonvolatile [filterprofile-name <filterprofile-name string (32)>] [filter-storagetype {nonvolatile | volatile}]] [volatile [filterprofile-name <filterprofile-name string (32)>] [filter-storagetype {nonvolatile | volatile}]]

| trap {mst | pvst | rst | syslog-server-status}

| user <user name string (32)> [EngineId <EngineId string>] [auth {md5 | sha | sha256 | sha384 | sha512} <authent_password random_str(8-40)>] [nonvolatile [EngineId <EngineId string>]] [priv {AESCTR | AESCTR192 | AESCTR256 | AES_CFB128 | AES_CFB192 | AES_CFB256 | DES | None | TDES} <authent_password random_str(8-40)>] [volatile [EngineId <EngineId string>]]

| view {<view name string (32)> <object Id string> {excluded [nonvolatile] [volatile] |included [nonvolatile] [volatile] | mask <OID mask (string)> {excluded [nonvolatile] [volatile] | included [nonvolatile] [volatile]}

}

snmp

snmp {access | community | enable | engineid | filter | filterprofile | group | mibproxy | notify | proxy | targetaddr | targetparams | trap | user | view}

Parameters

Parameter	Type	Description
access		Enter to configure the SNMP group access details. To configure an SNMP access along with the group, a group must have already been created using the snmp group command.
<string (32)>	String	Enter a name for the group for which access is to be provided.
v1		Enter to configure the SNMP version as Version 1.
v2c	A.B.C.D	Enter to configure the SNMP version as Version 2. Note that the some of the parameters apply only for v1 and v2C, and not to v1
v3		Enter to configure the SNMP version as Version 3. This is the most secure model as it allows packet encryption with the priv key word
auth	Integer	Enter to enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication.
noauth		Enter to configure no authentication
priv		Enter to configure both authentication and privacy.
context		Enter to configure the name of the SNMP context.
<string (32)>	String	Enter a name of the context. The maximum length of the string is 32.
nonvolatile		Enter to configure the storage type as permanent. The configuration is saved on the system, and during restart, the saved configuration can be viewed.
volatile		Enter to configure the storage type as temporary. During restart of the system, the configuration setting are erased.
notify		Enter to configure the MIB view of the SNMP context to which notification access is authorized by this entry
<string (32)>	String	Enter a notification view identifier. The maximum length of the string is 32.
read		Enter to configure the MIB view of the SNMP context to which read access is authorized by this entry
<string (32)>	String	Enter a read view identifier. The maximum length of the string is 32.
write		Enter to configure the MIB view of the SNMP context to which write access is authorized by this entry

Parameter	Type	Description
<string (32)>	String	Enter a write view identifier. The maximum length of the string is 32.
agent		Enter to configure the agent port on which agent listens
port		Enter to configure an agent port on which agent listens.
<port number (1-65535)>	Integer	Enter a port number. The port number can be from 1 to 65535. The default is 161.
community		Enter to configure the SNMP community details.
index		Enter to configure a community index. The default Community Index - NETMAN/PUBLIC.
<community index ID (string (32)>	String	Enter a community index identifier which stores the index value of the row. This ID must be unique for every community name entry. The maximum length of the string is 32.
name		Enter for community name configuration.
<community name string>	String	Enter a community name string. The default Community name - NETMAN/PUBLIC.
security		Enter to store the security model of the corresponding Snmp community name
<string (32)>	String	Enter a security name. The maximum length of the string is 32. The default Security Name - None.
context		Enter to configure the context in which the management information is accessed when using the community string specified by the corresponding instance of snmp community name
<Name>		Enter a name for the context. The default ContextName - Null.
nonvolatile		Enter to configure the storage type as permanent. The configuration is saved on the system, and during restart, the saved configuration can be viewed. This is default.
volatile		Enter to configure the storage type as temporary. During restart of the system, the configuration setting are erased.
transporttag		Enter to configure a set of transport endpoints from which a command responder application can accept management request
TransportTagIdentifier		Enter a transport ID. The default Transport Tag - Null.
none		Enter for no transport ID.

Parameter	Type	Description
contextengineid		Enter to configure the location of the context through which the management information is accessed when using the community string specified by the corresponding instance of SNMP community name
<ContextEngineID>	A.B.C.D.E.F.G	Enter for context engine ID. The default Context EngineID - 80.00.08.1c.04.46.53.
enable		Enter to enable trap related configuration.
traps		Enter to configure trap related configuration.
coldstart		Enter to configure cold start trap.
snmp		Enter to configure SNMP related configuration.
authentication		Enter for authentication related configuration
engineid		Enter to configure the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to coordinate the exchange of messages between the source and the destination.
<engine ID (string)>		Enter a engine ID string. The default is 80.00.08.1c.04.46.53. The Engine ID must be given as octets in hexadecimal separated by dots and the allowed length is 5 to 32 octets. **NOTE:** SNMP engine ID is an administratively unique identifier. Changing the value of the SNMP engine ID has significant effects All user information will be updated automatically to reflect the change
filter		Enter to configure Notify filter Profile entry.
<filter profile name string (32)>	String	Enter a name of the filter profile. This is a string value with a maximum size as 32.
<object Id string>	String	Enter to configure the object Identifier.
excluded		Enter to configure that the family of subtrees defined by the OID and mask is excluded from the filter profile.
included		Enter to configure that the family of subtrees defined by the OID and mask is included in the filter profile.

Parameter	Type	Description
nonvolatile		Enter to configure the storage type as permanent. The configuration is saved on the system, and during restart, the saved configuration can be viewed.
volatile		Enter to configure the storage type as temporary. During restart of the system, the configuration setting are erased
mask		Enter to define a family of subtrees, in combination with the object identifier.
<OID mask 23 (string)>	String	Enter an OID mask string.
trap		Enter for Trap related configuration
name		Enter for Mib object name related configuration
<mib OID name(string)>	String	Enter a Mib object name or object identifier.
oid		Enter for Mib Object Identifier related configuration
<OID name (string)>	String	Enter OID name string.
filterprofile		Enter to configure Notify filter Profile entry
<filter profile name string (32)>	String	Enter a filter profile string.
group		Enter to configure the SNMP group details.
<group name string(32)>	String	Enter a name for an SNMP group.
user		Enter to set an user for the configured group.
<user name string(32)>	String	Enter an user name.
security-model		Enter to set the security model for SNMP
v1		Enter to configure the SNMP version as Version 1.
v2c		Enter to configure the SNMP version as Version 2.
v3		Enter to configure the SNMP version as Version 3. This is the most secure model.

Parameter	Type	Description
nonvolatile		Enter to configure the storage type as permanent. The configuration is saved on the system, and during restart, the saved configuration can be viewed.
volatile		Enter to configure the storage type as temporary. During restart of the system, the configuration setting are erased.
mib		Enter to set the SNMP MIB proxy name configuration.
name		Enter to set the SNMP MIB proxy name configuration.
{<mib Object name (string)>	String	Enter an SNMP MIB proxy name.
<proxy id string (32)>	String	Enter a Locally arbitrary and unique identifier representing name of proxy.
count		Enter to set number of entries.
<count value (1-100>	Integer	Enter a number of entries.
proxytype		Enter for SNMP proxy message type configuration.
inform		Enter to set that Inform type messages are forwarded using translation parameters
read		Enter to set that Read type messages are forwarded using translation parameters
trap		Enter to set that Trap type messages are forwarded using translation parameters
write		Enter to set that Write type messages are forwarded using translation parameters
mibid		Enter to set MIB ID string.
<MIB ID string>	String	Enter an MIB ID string.
targetparamsin		Enter to denote the row of snmpProxyTable to be used for forwarding received messages.
<target ID string (32)>	String	Enter a target Id string.
targetout		Enter to select management target defined in snmpTargetAddrTable
<target ID string (32)>	String	Enter a target Id string.

Parameter	Type	Description
storagetype		Enter to set storage type
nonvolatile		Enter to configure the storage type as permanent. The configuration is saved on the system, and during restart, the saved configuration can be viewed.
volatile		Enter to configure the storage type as temporary. During restart of the system, the configuration setting are erased.
short		Enter to display the value of MIB object of the given table, including the next object and the values of the MIB objects.
value		Enter for Value to be set for MIB object.
<MIB object string>	String	Enter a string that is to be set to the MIB Object.
mibproxy		Enter to configure the snmp proxy manager such that incoming request is routed to the given proxy address
notify		Enter to configure the SNMP notification details.
<notification namestring (32)>	String	Enter an unique identifier (notification name string) associated with the entry. The default Notify Name - iS5Com/iS5Com1.
tag		Enter to configure a notification tag, which selects the entries in the Target Address Table.
<tag name string(32)>]		Enter a notification tag name. The default Notify Tag - iS5Com/iS5Com1
type		Enter to set the notification type. The list is as follows.
Inform		Enter to Allows routers / switches to send inform requests (notifications) to SNMP managers
Trap		Enter to configure the SNMP notification details.
nonvolatile		Enter to configure the storage type as permanent. The configuration is saved on the system, and during restart, the saved configuration can be viewed.
volatile		Enter to configure the storage type as temporary. During restart of the system, the configuration setting are erased. This is default.
proxy		Enter to configure the proxy. This is a set of translation parameters used by a proxy forwarder application for forwarding SNMP messages
name		Enter to set the SNMP MIB proxy name configuration.

Parameter	Type	Description
<proxy id string (32)>	String	Enter an unique identifier for an entry in the proxy table. This value is a string of maximum size 32
proxytype		Enter for SNMP proxy message type configuration.
inform		Enter to set that Inform type messages are forwarded using translation parameters
read		Enter to set that Read type messages are forwarded using translation parameters
trap		Enter to set that Trap type messages are forwarded using translation parameters
write		Enter to set that Write type messages are forwarded using translation parameters
contextengineid		Enter to configure an context engine ID in messages that is forwarded using the translation parameters defined by the entry
<contextengine ID>	String	Enter a context engine ID.
targetparamsin		Enter to denote the row of snmpProxyTable to be used for forwarding received messages.
<target ID string (32)>	String	Enter a target Id string.
targetout		Enter to select management target defined in snmpTargetAddrTable. **NOTE:** For Single TargetOut—this is only used when selection of a single target is required (i.e. when forwarding an incoming read or write request). For Multiple Target Out—this is only used when selection of multiple targets is required (i.e. when forwarding an incoming notification.
<target ID string (32)>	String	Enter a target Id string.
contextname		Enter to set storage type
<ProxyContextName (string>)	String	Enter to configure the storage type as permanent. The configuration is saved on the system, and during restart, the saved configuration can be viewed.
storagetype		Enter to set storage type

Parameter	Type	Description
nonvolatile		Enter to configure the storage type as permanent. The configuration is saved on the system, and during restart, the saved configuration can be viewed. This is default.
volatile		Enter to configure the storage type as temporary. During restart of the system, the configuration setting are erased.
targetaddr		Enter to configure the SNMP target address. This is the transport address used in generation of SNMP messages. **NOTE:** This configuration is effective only if targetparams is configured.
<target address string (32)>	String	Enter an unique identifier of the Target. This value is a string of maximum size 32.
param		Enter to configure the parameters when generating messages to be sent to transport address.
<SNMP param name string (32)>	String	Enter an SNMP param name. This value is a string of maximum size 32.
<dns_host_name>	String	Enter to configure a target Host name to which the generated SNMP notifications are sent. This value is a sting of maximum size 255.
(<ucast_addr>)	A.B.C.D	Enter to configure a unicast target address to which the generated SNMP notifications are sent. The format of the IP addess is A.B.C.D
<ipv6_addr>}	AAAA::BBBB	Enter an IP6 target address to which the generated SNMP notifications are sent. The format is AAAA::BBBB.
nonvolatile		Enter to configure the storage type as permanent. The configuration is saved on the system, and during restart, the saved configuration can be viewed.
port		Enter to configure SNMP manager port for sending inform/trapmessages to SNMP manager.
<port number (1-65535)>	Integer	Enter a port number through which the generated SNMP notifications are sent to the target address. The value ranges from 1 to 65535.
retries		Enter to configure the default number of retries to be attempted when a response is not received for a generated message.
<retry count value (1-3)>	Integer	Enter a number for reties. This value ranges from 1 to 3. The default is 3.

Parameter	Type	Description
taglist		Enter to configure the tag identifier that selects the target address for the SNMP.
<tag ID string (255)>	String	Enter a tag identifier. This value is an octet string of maximum size 255.The tag ID can also be set as none using the none option.
timeout		Enter to configure the time for which the SNMP agent waits for a response from the SNMP Manager before retransmitting the Inform Request Message.
<Timeout value (1-1500)>	Integer	Enter a time for which the SNMP agent waits for a response. This value ranges from 1 to 1500 seconds. The default is 1500.
volatile		Enter to configure the storage type as temporary. During restart of the system, the configuration setting are erased.
targetparams		Enter to configure the SNMP group details. **NOTE:** User information should be configured prior to the configuration of SNMP target parameters. See snmp user.
<SNMP param string (32)>	String	Enter a name for an SNMP group.
user		Enter to set an user for the configured group. The default is UserName - Initial.
<user name string(32)>	String	Enter an user name.
security-model		Enter to set the security model for SNMP. **NOTE:** SNMP passwords are localized using the local SNMP engine ID.
v1		Enter to configure the SNMP version as Version 1.
v2c		Enter to configure the SNMP version as Version 2.
v3		Enter to configure the SNMP version as Version 3. This is the most secure model.
auth		Enter to enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication. The default Authentication Protocol is None.
noauth		Enter to configure no authentication
priv		Enter to configure both authentication and privacy. The default Privacy Protocol - None.

Parameter	Type	Description
message-processing		Enter to set the SNMP message processing model configuration.
v1		Enter to configure the SNMP version as Version 1.
v2c		Enter to configure the SNMP version as Version 2.
v3		Enter to configure the SNMP version as Version 3. This is the most secure model.
filterprofile-name		Enter to configure the profile name. his value is a string of maximum size 32
<filterprofile-name string (32)>	String	Enter a profile name.
filter-storagetype		Enter to set the required storage type for the filter profile.
nonvolatile		Enter to configure the storage type as permanent. The configuration is saved on the system, and during restart, the saved configuration can be viewed. This is default.
volatile		Enter to configure the storage type as temporary. During restart of the system, the configuration setting are erased.
mst		Enter to mst configuration
pvst		Enter to set Per-VLAN-Rapid Spanning Tree configuration
rst		Enter to set Rapid Spanning Tree configuration
syslog-server-status		Enter to set Syslog Server related configuration
user		Enter to set the SNMP user details.
<user name string(32)>	String	Enter an user name which is the User-based Security Model dependent security ID.
engineid		Enter to configure the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to coordinate the exchange of messages between the source and the destination
<engine ID (string)>	String	Enter a engine ID string.
auth		Enter to set an authentication Algorithm. Options are as follows

Parameter	Type	Description
md5		Enter to set the Message Digest 5 based authentication.
sha		Enter to set the Security Hash Algorithm based authentication.
sha256		Enter to set the Security Hash Algorithm as SHA 256
sha384		Enter to set the Security Hash Algorithm as SHA 384
sha512		Enter to set the Security Hash Algorithm as SHA 512
<authent_password random_str(8-40)>	String	Enter to set the authentication password that will be used for the configured authentication algorithm.
nonvolatile		Enter to configure the storage type as permanent. The configuration is saved on the system, and during restart, the saved configuration can be viewed.
engineid		Enter to configure the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to coordinate the exchange of messages between the source and the destination
<engine ID (string)>	String	Enter a engine ID string.
priv		Enter to set the DES encryption and also the password to be used for the encryption key. Options are as follows.
AESCTR		Enter for AES CTR128 related configuration
AESCTR192		Enter for AES CTR192 related configuration
AESCTR256		Enter for AES CTR256 related configuration
AES_CFB128		Enter for AES CFB128 related configuration
AES_CFB192		Enter for AES CFB192 related configuration
AES_CFB256		Enter for AES CFB256 related configuration
DES		Enter for DES encryption configuration
None		Enter for no encryption configuration
TDES		Enter for TDES encryption configuration

Parameter	Type	Description
<authent_password random_str(8-40)>	String	Enter to set the authentication password that will be used for the configured authentication algorithm.
volatile		Enter to configure the storage type as temporary. During restart of the system, the configuration setting are erased.
engineid		Enter to configure the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to coordinate the exchange of messages between the source and the destination
<engine ID (string)>	String	Enter a engine ID string.
view		Enter to configure the SNMP view.
<view name string (32)>	String	Enter a view name for which the view details are to be configured. This is a string value with maximum size as 32.
<OIDTree>		Enter to specify the sub tree value for the particular view. The default OIDTree is 1.
excluded		Enter to configure that the family of subtrees defined by the OID and mask is excluded from the filter profile.
included		Enter to configure that the family of subtrees defined by the OID and mask is included in the filter profile. This is default.
nonvolatile		Enter to configure the storage type as permanent. The configuration is saved on the system, and during restart, the saved configuration can be viewed. This is the default.
volatile		Enter to configure the storage type as temporary. During restart of the system, the configuration setting are erased
mask		Enter for AES CTR128 related configuration
<OIDMask>	String	Enter to specify the mask value for the particular view. The default OIDMask is 1.

Mode

Global Configuration Mode

Examples

SNMPv3 Configuration

iS5comm (config)# snmp access myv3group v1 read v2readview write v2writeview notify v2notifyview nonvolatile

iS5comm (config)# snmp community index myv3com name myv3com security xyz context myinst nonvolatile transporttag myv3tag

iS5comm (config)# snmp agent port 100

iS5comm (config)# snmp engineid 80.0.08.1c.04.5f.a9

iS5comm (config)# snmp proxy name proxy1 proxytype write contextengineid 80.0.08.1c.04.46.53 targetparamsin param2 targetout target2

iS5comm (config)# snmp mibproxy name mibproxy1 proxytype read mibid 1 targetparamsin param1 targetout target2 storagetype nonvolatile

iS5comm (config)# snmp view v2readview 12.0.0.1 mask 1.1.1.1 included nonvolatile

iS5comm (config)# snmp targetaddr ad1 param p1 10.3.21.3 timeout 1 volatile port 2

iS5comm (config)# snmp targetparams param1 user user1 security-model v3 noauth message-processing v3

iS5comm (config)# snmp user user1

iS5comm (config)# snmp notify note1 tag tag1 type Inform

iS5comm (config)# snmp filter trap name fsbgp4PeerExtTable

iS5comm (config)# snmp filterprofile filter1 1.5 mask 1.1 included nonvolatile

SNMP v2 Configuration

is5comm# configure terminal

is5comm (config)# snmp user testerv2

is5comm (config)# snmp community index public name public security testerv2

is5comm (config)# snmp group groupv2 user testerv2 security-model v2c

is5comm (config)# snmp access groupv2 v2c read iso write iso notify iso

is5comm (config)# snmp view iso 1.1 included

is5comm (config)# snmp targetaddr PC1 param paramlist1 192.168.10.254 taglist taglist1

is5comm (config)# snmp targetparams paramlist1 user testerv2 security-model v2c message-processing v2c

is5comm (config)# snmp notify PUBLIC tag taglist1 type Trap

11.8. snmpget mib

To get the value of the MIB object through SNMP agent, use the command **snmpget mib** in Global Configuration Mode.

snmpget mib

```
snmpget mib {name <name string (32)> | oid <oid string (32)>} [short]
```

Parameters

Parameter	Type	Description
name		Enter to get the MIB object name.
<name string (32)>	String	Enter an MIB object name. This is a string value with maximum size of 32.
oid		Enter to get the MIB object identifier
<oid string (32)>	String	Enter an MIB object identifier. This is a string value with maximum size of 32.
short		Enter to display the value of the MIB object.

Mode

Global Configuration Mode

Examples

iS5comm(config)# snmpget mib name fsbgp4PeerExtConfigurePeer.12.0.0.1 short

11.9. snmpgetnext mib

To get the next MIB object for the given object, use the command **snmpgetnext mib** in Global Configuration Mode.

snmpgetnext mib

```
snmpgetnext mib {name <value string (32)> | oid <oid string (32)> value
<value string (32)>} [short]
```

Parameters

Parameter	Type	Description
name		Enter to get the next MIB object name.
<value string (32)>	String	Enter a value for the next MIB object.This is a string value with maximum size of 32.
oid		Enter to get the next MIB object identifier
<value string (32)>	String	Enter a value for the next MIB object ID. This is a string value with maximum size of 32.
short		Enter to display the value of the MIB object.

Mode

Global Configuration Mode

Examples

iS5comm (config)# snmpgetnext mib name fsbgp4PeerExtTable short

11.10. snmp-server

To enable trap related configuration, and configure the TCP port, the UDP and the proxy UDP port over which the agent sends the trap, use the command **snmp-server** in Global Configuration Mode. The no form of the command disables generation of authentication traps and a coldstart trap, and configures the SNMP agent to send SNMP message on default TCP port or default UDP port.

snmp-server

```
snmp-server {enable traps {coldstart | snmp authentication} | trap
{proxy-udp-port <port number (1-65535)>} | {udp-port <port number
(1-65535)>}}
```

no snmp-server

```
no snmp-server {enable | trap}
```

Parameters

Parameter	Type	Description
enable		Enter to enable trap related configuration.
traps		Enter to configure trap related configuration.
coldstart		Enter to enable generation of a coldstart trap. A coldstart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.
snmp		Enter to enable generation of authentication traps from the SNMP agent (for all SNMPv1, SNMPv2 and SNMPv3)
authentication		Enter for authentication related configuration
trap		Enter to configure the TCP port over which agent sends the trap. TCP traps are not currently supported.
proxy-udp-port		Enter to configure the UDP port over which agent sends the trap to the proxy entity
<port number (1-65535)>	Integer	Enter a value for proxy UDP port number over which agent sends the trap. The format for port number is (1-65535). The default is 162.
udp-port		Enter to specify the context name used during snmp subagent registration process. SNMP subagent is not supported and this option will be removed from a future release.
<port number (1-65535)>	Integer	Enter to configure the UDP port over which agent sends the trap. The format for port number is (1-65535).

Mode

Global Configuration Mode

Default

snmp-server is disabled

Examples

iS5comm (config)# snmp-server enable traps snmp authentication

iS5comm (config)# snmp-server enable traps coldstart

iS5comm (config)# snmp-server trap udp-port 1234

iS5comm (config)# snmp-server trap proxy-udp-port 162

11.11. snmpset mib

To set the value of the MIB object through SNMP agent., use the command **snmpset mib** in Global Configuration Mode.

snmpset mib

```
snmpset mib {name <name string (32)> value <value string (32)> | oid <oid
string (32)> value <value string (32)>} [short] [input <input value>]
```

Parameters

Parameter	Type	Description
name		Enter to set the MIB object name.
<name string (32)>	String	Enter an MIB object name. This is a string value with maximum size of 32.
value		Enter set the value for the MIB object.
<value string (32)>	String	Enter a value for the MIB object.This is a string value with maximum size of 32.
oid		Enter to set the MIB object identifier
<oid string (32)>	String	Enter an MIB object identifier. This is a string value with maximum size of 32.
value		Enter set the value for the MIB object.
<value string (32)>	String	Enter a value for the MIB object identifier. This is a string value with maximum size of 32.
short		Enter to display the value of the MIB object.
input		Enter to set the specified data type for the MIB object.
<input value>	String	Enter data type for the MIB object. The data types are • i—sets the integer value for the MIB object. • s—sets the string value for the MIB object. • o—sets the Octet string value for the MIB object. • x—sets the hexa string value for the MIB object.

Mode

Global Configuration Mode

Examples

iS5comm (config)# snmpset mib name snmpListenTcpPort.0 value 145 short 1

11.12. snmpwalk mib

To get the next MIB object for the given object, use the command **snmpwalk mib** in Global Configuration Mode.

snmpwalk mib

```
snmpwalk mib {name <value string (32)> | oid <oid string (32)> value <value string (32)>} [count <integer(1-100)>] [short]
```

Parameters

Parameter	Type	Description
name		Enter to get the next MIB object name.
<value string (32)>	String	Enter a value for the next MIB object.This is a string value with maximum size of 32.
oid		Enter to get the next MIB object identifier
<value string (32)>	String	Enter a value for the next MIB object ID. This is a string value with maximum size of 32.
count		Enter to set the number of entries to be displayed in the MIB objec
<integer(1-100)>		Enter a number of entries to be displayed in the MIB object. This value ranges from 1 to 100.
short		Enter to display the value of the MIB object.

Mode

Global Configuration Mode

Examples

iS5comm (config)# snmpwalk mib name fsbgp4PeerExtTable

iS5comm # snmpwalk mib name fsbgp4PeerExtTable count 1 short1

Syslog

12. Syslog

System Log (Syslog) is an RFC 3164 compliant protocol. The syslog protocol provides a transport to allow a machine to send event notification messages across IP networks to event message collectors (aka syslog servers). A Syslog message is any IP packet sent via Syslog protocol using UDP port 514 (by default). These messages are generated instantly as and when an event (e.g. Interface UP/DOWN, login/logout, save and restore config, max temperature threshold) occurs during the device's operation.

System Log (Syslog) is an RFC 3164 compliant protocol. The Syslog protocol provides a transport to allow a machine to send event notification messages across IP networks to event message collectors (aka syslog servers). A Syslog message is any IP packet sent via Syslog protocol using UDP port 514 (by default). These messages are generated instantly as and when an event (e.g. Interface UP/DOWN, login/logout, save and restore config, max temperature threshold) occurs during device's operation.

The full format of a syslog message seen on the wire has three discernable parts. The first part is called the PRI, the second part is the header, and the third part is the MSG. The total length of the packet must be 1024 bytes or less. RAPTOR ensures that each syslog message do not exceed 1024 bytes.

In its first PRI part, every syslog message contains a Priority value which represents both the Facility and Severity. The HEADER consists of VERSION, TIMESTAMP, HOSTNAME (or IPv4 or IPv6 address), APP-NAME, PROCID, and MSGID. The TIMESTAMP field is the local time and is in the format of "Mmm dd hh:mm:ss" (without the quote marks) value in "mmm dd hh:mm:ss" format.

RAPTOR allows administrator to direct the log messages to local storage (RAM/Flash) or to remote Syslog server which runs in any Linux/Windows machine. In case of remote logging, RAPTOR uses IP-based communication to log message to remote server. Syslog client in RAPTOR can also send the same message to different collector if configured by the administrator. One of the fundamental tenets of the syslog protocol and process is its simplicity. The transmission of syslog messages may be started on a device without a receiver being configured, or even actually physically present. This simplicity has greatly aided the acceptance and deployment of syslog.

12.1. Severity

Each message Priority has a decimal Severity level indicator between 0 – 7. The lower the value, the higher the priority. RAPTOR's Software is provisioned with more than 1500 SYSLOG messages covering errors, alerts, and major events. *Table 1* shows the list of all severity levels along with their numerical values.

Table 1: Severity Levels

Value	Severity	Keyword	Description	Condition
0	Emergency	emerg	System is unusable	A panic condition
1	Alert	alert	Action must be taken immediately	A condition that should be corrected immediately, such as corrupted system database.
2	Critical	crit	Critical conditions	Hard device errors.
3	Error	err	Error conditions	Specified any error condition happened in the system operation.
4	Warning	warning	Warning conditions	Specified any abnormalities happening in the system operation.
5	Notice	notice	Normal but significant conditions	Conditions that are not error conditions, but that may require special handling.
6	Informational	info	Informational messages	Information to users.
7	Debug	debug	Debug-level messages	Messages that contain information normally of use only when debugging a program.

12.2. Priority

Each syslog message includes a priority value in the beginning of the text message. The priority value ranges between 0 to 191 and it made up of facility and severity values. The priority is enclosed with in “<>” delimiters. The formula for calculating the priority value is:

Priority Value = Facility Level Numerical Value + Severity Value

For example, for a local4 message (Facility level value 160) with a Severity of Notice (Severity=5), the Priority would have a Priority value of 165.

12.3. Facility

Facility code is used to specify the type of program logging the message. Messages with different facilities can be handled differently. This term comes into picture when we start using remote logging mechanism. There are total of 8 facility levels ranging between local0 and local7. Each facility level has a value assigned to it—local0 (128), local1 (136), local2 (144), local3(152), local4(160), local5(168), local6(176), and local7 (184). Raptor is configured with default facility level (local0) and all messages are sent with

this facility level unless configured to use different facility level. The idea of the facility level configuration is to differentiate and filter logs.

12.4. Example of Valid Syslog Message

```
<165>1 2003-08-24T05:14:15.000003-07:00 192.0.2.1 su 8710 ID47 BOM 'su
root' failed for lonvick on /dev/pts/8
```

- <165> stands for Priority value indicating a locally defined facility (local4) with a severity of Notice 5 (11.1.3).
- The HEADER part has VERSION 1, a TIMESTAMP field in the message "24 August 2003 at 5:14:15am,with a -7 hour offset from UTC, 3 microseconds into the next second" , iPv4—"192.0.2.1"; APP-NAME is "su", the PROCID is "8710" (for example, this could be the UNIX PID), and the MSGID is "ID47".
- The MSG is " 'su root' failed for lonvick", encoded in UTF-8. The encoding is defined by the BOM

This example of valid syslog messages is based on section 6.5 Examples of RFC 5425.

12.5. Factory Default Syslog Configuration Values

Shown below is the list of factory default values configured after a clean start.

- Local logging in RAM is enabled by default
- Default number of syslog messages stored in RAM is 200
- Default severity level is Critical
- Default facility level is local0.
- Default flash file size is 1MB in case that flash logging is configured.

12.6. Logging Mechanisms Types and Default Configuration

There are two types of local logging mechanisms. Mechanism 1 is stored in RAM and 2 is stored in Flash memory.

12.7. Local Logging Mechanism 1

In this mechanism, the Syslog messages are stored in RAM. Syslog client in Raptor can store 200 messages (default) at a time which can be configured to maximum of 4096 messages. Once the maximum level is reached, it rolls on i.e. the latest messages will be displayed and the oldest messages will be erased.

There is a rule in local logging mechanism as per which all levels below the configured reference severity level are automatically logged. For example, if *critical* is the default level with priority value of 2, the levels below are *alert* with a value of 1 and *emergency* (level 0). Both below levels are automatically

logged. Therefore, there will be no need for configuration needed if the administrator needs to log only critical and levels below messages. If we had configured the logging severity as *debugging* whose value is 7 (the maximum), in that case, all severity levels (7-0) would have been logged automatically

12.8. CLI Commands for Local Logging Method 1

Table 2: CLI Commands for Local Logging Method 1

Command Syntax	Description
logging local buffered 4096	Configures maximum storage capability to 4096. Default value is 200.
logging severity debugging	Sets the reference severity level to debugging. Default value is “Critical”.
syslog localstorage	Enables the syslog local storage capability. This command is enabledwith the help of init script during Raptor boot up.
no logging severity	This will revert back the reference severity level back to default, which is Critical severity level.
no logging buffered	This will reset the buffer level back to default value 200.
no syslog localstorage	
show logging	Displays the syslog messages stored in RAM.
clear logs	Deletes all the captured syslog messages in RAM

From the above shown CLI commands, the logging severity level is configured as debugging, and hence the priority value below 7 (emergency/alert/critical/error/warning/notice/info/debug) is automatically logged in RAM.

The “show logging” command lists all captured syslog messages in RAM. It displays the latest collected logs and deletes the oldest messages. The buffer size is set to max 4096 and the facility level configured is local0 (see below).

```
System Log Information
----------------------
Syslog logging : enabled(Number of messages 127)
Console logging : disabled(Number of messages 0)
TimeStamp option : enabled
Severity logging : Critical
Facility : local1
Buffered size : 4096 Entries
```

12.9. Local Logging Mechanism 2

This second local logging method is storing syslog messages in flash memory. We can set a file name of user choice in a flash and redirect all syslog messages to the created file. First, we create a file name and next associate the messages (based on severity) to the log file.

Each created file can accommodate 4 MB of data. Once the 4 MB data quota is reached, the log messages will be moved to the same file name with a .bk extension and a new file will be created (with the same name) in which the live logging will continue. This process is a repeating cycle, as each time 4 MB of data is reached, the old logs are moved to a .bk file and the live logging takes place in a new file. So, the flash consumption is restricted to max of 8MB (4 MB for. bk file which has the old log messages and 4 MB where the current live logging takes place).

There is CLI command to set the flash file size and its threshold limit at run time. This option helps user to maximize the file storage size from default 4 MB up to 10 MB. The CLI configuration is:

12.10. CLI Commands for Setting Flash Size and Threshold Limit

Table 3: CLI Commands for Setting Flash Size and Threshold Limit

Command Syntax	Description
logging filesize <integer 1-10>	Sets logging Flash file size between 1 – 10 MB. Default is 1 MB
logsize-threshold <integer (1-99)>	This command sets the threshold limit of the logging file size as well as the flash usage. It serves two purposes.

A maximum of 3 files can be created. The CLI commands for configuring the files are shown in the table below.

Table 4: Syslog CLI Configurations for Local Logging

Command Syntax	Description
syslog filename-one is5	A flash file with a name is5 is created.
syslog filename-two two	A flash file with a name two is created.
syslog filename-three three	A flash file with a name three is created.

12.11. Logging to Flash Files CLI Commands

The original command provided was as shown in Table 6. In the original command, the user had to provide the priority value between 0-191. It is a bit tedious process to choose the value as the user had

to do some calculation of the priority based on the numerical values of facility and severity level of the syslog message that needs to be logged on.

Therefore, the command had been simplified as shown in *Table 6*. The user does not need to provide the hard coded value but rather just specify the severity of the message that needs to be logged into the file.

Table 5: Old Logging-file CLI Command

Command Syntax	Description
logging-file <short (0-191)> <string (32)>	0-191 is the priority value that user should provide and the string is the file name.

Table 6: New & Modified Logging to File CLI Command

Command Syntax	Description
logging local {buffered [<short (1-4096)>]| flash {{{alerts | critical | debugging |emergencies | errors | informational|notification | warnings} file <string(32)>} | size <integer (1-10)> }}	Simplified command which logs based on severity level specified by user. At backend, we calculate the associated priority.
logging local flash debugging file is5	Redirects debugging severity to flash file “is5”
logging local flash critical file two	Redirects critical severity to flash file “two”
logging local flash alert file three	Redirects alert severity to flash file “three”
no logging local flash debugging file is5	Unconfigures the local flash logging for debugging severity for flash file “is5”
no logging local flash critical file two	Unconfigures the local flash logging for criticalseverity for file named “two”.
no logging local flash alert file three	Unconfigures the local flash logging for alertseverity for file name “three”.

12.12. Flash Space Restriction Mechanisms

All Syslog and other log files (fsir.log.xxx & audit log) are created and stored under /mnt/log flash folder. The capacity of the log folder is 118 MB. To prevent the flash log folder getting fully occupied, a restriction mechanism had been devised.

12.13. Warning Messages

When the usage of this folder reaches the threshold, in the console prompt, a warning message such as the one shown below is generated for the user. The warning will appear every time when there is an attempt for a syslog message to be logged in a flash file and until space in the flash file is freed.

```
Warning: Syslog flash storage crossed its threshold limit. Do you want to
erase logs (Y/N) [N]?
```

If an user presses **Yes**, all log files in the flash log directory will be deleted.

If an user selects **No** or just presses **Enter** (i.e. the default option which is **No** is activated), the console prompt is returned to normal operation. The administrator can later transfer the log messages from the flash directory to an external Windows / Linux machine and erase the logs to save space. The CLI configuration commands to do the same are outlined in *Table 7*.

Table 7: Copy and Erase Flash Log CLI Commands

Command Syntax	Description
copy flash log threetftp://192.168.10.66/three	Copies flash file “three” to remote machine
copy flash log threetftp://192.168.10.66/syslog	The source file and the destination file don’t need to be same.
erase flash log three	This CLI command deletes the specific log file in flash named “three”

12.14. Error Messages

When the flash is occupied to its maximum capacity of 118 MB, a second level of restriction mechanism is activated, and an error message as captured below is generated. The user will be prevented from creating new file.

```
iS5Comm <config># syslog filename-two <string(32)>
ERROR: Flash space exhausted. Please delete log files and then try again
iS5Comm <config>#
```

12.15. USB Option for Copying Logs to External USB Flash Drive

There will be a new CLI command added for copying the Syslog file from internal flash to external USB flash drive. The command is outlines in the table below.

Table 8: Copy Logs to External USB Flash Drive CLI Commands

Command Syntax	Description
copy flash log three usb three	Copies internal flash (source) file named “three” to USB drive with destination name as given by the user.
copy flash log three usb syslog	The source file and destination file don’t need to be same.

12.16. CLI Command for Listing File Contents of Flash

Table 9: Listing File Contents of Flash CLI Commands

Command Syntax	Description
show flash logs	This command is executed in global execution mode which lists the flash contents.

12.17. Example configuration for Local (Flash) Logging

```
iS5Comm <config># logging severity debugging
iS5Comm <config># syslog filename-one one
iS5Comm <config># syslog filename-two two
iS5Comm <config># syslog filename-three three
iS5Comm <config># logging local flash debugging file one
iS5Comm <config># logging local flash alert file two
iS5Comm <config># logging local flash critical file three
iS5Comm <config># end
```

As per the example configuration shown above, the above set of configurations creates flash file named “one”, “two”, and “three” in the flash directory /mnt/log/ and the debugging severity messages are directed to file “one”, alert severity messages are directed to “two”, and critical severity messages are directed to “three”.

For instance, if file “one” has reached its quota 4 MB, the log messages in file “one” is backed up in a new file named “one.bk” and the newly generated messages are still logged to file “one” as a new file. This cycle is repeated every time 4 MB is reached.

12.18. Remote Logging

The remote logging is transferring the Syslog messages to syslog remote server running in any Windows/Linux machine. These messages are transferred instantly when an event (e.g. Link up/down, attaining max temperature threshold) occurs in RAPTOR via a UDP socket. These messages can be filtered based on the severity & facility level.

For the remote logging to take place, first we need to set the reference severity, and then configure which severity to be logged to the remote syslog server. The default logging severity is Critical (3). So, when an event occurs the SYSLOG client application first check if the severity level of the message is less that or equal to reference severity level, and second, it checks if there is any remote server configured for that severity. Only if both conditions are satisfied, the log will be transferred to the remote server.

12.19. Remote Logging Syslog CLI Command

The original CLI command for logging the message to remote server is shown in Table 10. In a similar manner as the logging-file CLI command, this command also requires a user to specify the priority value between 0-191. loggingfile CLI command had been replaced with a CLI commands for remote logging which uses severity levels instead of priority levels. The new CLI commands for remote logging are displayed in *Table 11*.

Table 10: Remote Logging Old CLI Command

Command Syntax	Description
logging-server <short (0-191)> {ipv4<ucast_addr> |ipv6 <ip6_addr>|<dns_host_name>} [port <integer (1- 65535)>]	0-191 is the priority value that Raptor requiresthe user to configure.

Table 11: Remote Logging Modified CLI Commands (Sheet 1 of 2)

Command Syntax	Description
logging remote {alerts | critical | debugging| emergencies | errors | informational |notification | warnings} {ipv4 <ucast_addr> |ipv6 <ip6_addr> | <dns_host_name>} [port<integer (1-65535)>] [{udp | tcp | beep}]	Simplified command for setting the remote logging severity based on the severity rather than priority. At backend we calculate theassociated priority.
logging remote alerts ipv4 < syslog-server IPaddress>	Logs alert level messages
logging remote critical ipv4 < syslog-serverIP address>	Logs critical level messages
logging remote debugging ipv4 < syslog-serverIP address>	Logs debugging level messages
logging remote emergencies ipv4 < syslogserver IP address>	Logs emergency level messages
logging remote errors ipv4 <syslog-server IPaddress>	Logs error level messages
logging remote informational ipv4 <syslogserver IP address>	Logs informational level messages
logging remote notification ipv4 <syslogserver IP address>	Logs notification level messages
logging remote warnings ipv4 <syslog-server IP address>	Logs warning level messages

Table 11: Remote Logging Modified CLI Commands (Continued) (Sheet 2 of 2)

Command Syntax	Description
no logging remote alerts ipv4 <syslog-server IP address>	Unconfigures the remote logging server for alerts severity level.
no logging remote critical ipv4 <syslog-server IP address>	Unconfigures the remote logging server for critical severity level

We can have maximum of seven different syslog server IP address configurations, and ideally each severity level (total 0 - 7) can be logged to eight different servers.

12.20. Remote Logging Syslog Facility Level Configuration

There are eight facility levels in total which can be configured. The purpose of these commands is to differentiate and filter syslog messages in the external syslog severs. The default facility is Local0.

Table 12: Remote Logging Syslog Facility Level CLI Commands

Command Syntax	Description
logging severity debugging	Sets the reference severity level
logging facility local1	Sets the logging facility aslocal1
logging remote critical ipv4 < syslog-serverIP address>	Logs critical level messages
logging remote debugging ipv4 < syslog-serverIP address>	Logs debugging level messages
logging remote emergencies ipv4 < syslogserver IP address>	Logs emergency level messages

12.21. Example 1 for Configuration for Remote Logging

```
iS5Comm <config># logging severity debugging
iS5Comm <config># logging remote debugging ipv4 192.168.10.67
iS5Comm <config># remote critical ipv4 192.168.10.68
iS5Comm <config># end
```

The above set of configurations logs debugging severity messages under facility level local1. Facility level is a onetime configuration. Once it is set, all message generation will follow the same facility level, i.e. severity cannot be set to different facility level.

12.22. Example 2 for Configuration for Remote Logging

```
iS5Comm <config># logging severity debugging
iS5Comm <config># logging facility local1
iS5Comm <config># logging remote debugging ipv4 192.168.10.67
iS5Comm <config># end
```

The above set of configurations logs debugging severity messages under facility level local1. Facility level is a onetime configuration, and once it is set, all message generation will follow the same facility level, i.e. severity cannot be set with different facility level.

12.23. Syslog List

What follows is a list of the Syslogs supported by the RAPTOR.

Table 13: List of Syslogs (Sheet 1 of 12)

Module	Syslog Message	Severity Level
STP-RSTP	Total number of ports in switch exceeds 4094,STP can run only on ports upto 4094. Hence this port will not be participating in the spanning tree	Alert
STP-RSTP	Setting of port state failed in hardware	Alert
VLAN	SBP oper Status is [UP / Down] for SCID-SVID (<port no> - <port no>) on the UAP port	Informational
VLAN	Not owned context exists: vlan_curr_context_thread	Critical
VLAN	Context owned by vlan_curr_context_thread not owned by current thread	Critical
VLAN	VLAN: Source relearning has Occurred for Mac Address from one port to another port	Informational
VLAN	Failed to program MAC address during creation/deletion/updating the unicast entry from the peer node	Error
VLAN	MAC learning limit has reached for VLAN ID	Error
Link Aggregation	LaEnqueueControlFrame: Ctrl Mesg ALLOC_MEM_BLOCK FAILED	Critical
Link Aggregation	Reason for Recovery is Threadhold Exceed for Port	Critical
Link Aggregation	Reason for Recovery is Port Defaulted for Port	Critical

Table 13: List of Syslogs (Continued) (Sheet 2 of 12)

Module	Syslog Message	Severity Level
Link Aggregation	Reason for Recovery is H/w Failure for Port	Critical
Link Aggregation	Recovery trigger for Port has exceeded the threshold.Performing admin down action	Critical
Link Aggregation	Recovery trigger for Port has exceeded the threshold.Performing no action	Critical
Link Aggregation	LaCreatePort: Intf Mesg ALLOC_MEM_BLOCK FAILED	Critical
Link Aggregation	LaMapPort: Intf Mesg ALLOC_MEM_BLOCK FAILED	Critical
Link Aggregation	LaDeletePort: Intf Mesg ALLOC_MEM_BLOCK FAILED	Critical
Link Aggregation	LaUnmapPort: Intf Mesg ALLOC_MEM_BLOCK FAILED	Critical
Link Aggregation	LaUpdatePortStatus: Intf Mesg ALLOC_MEM_BLOCK FAILED	Critical
Link Aggregation	LaAsyncNpUpdateStatus:Intf Msg ALLOC_MEM_BLOCK FAILED	Critical
Link Aggregation	Reason for Error Recovery timer Start is Threadhold Exceed for Port	Critical
Link Aggregation	Reason for Error Recovery timer Start is Port Defaulted for Port	Critical
Link Aggregation	Reason for Error Recovery timer Start is H/w Failure for Port	Critical
Link Aggregation	[NP-FAULT - LA] operation has failed	Critical
Link Aggregation	LaEnqueueControlFrame: Ctrl Mesg ALLOC_MEM_BLOCK FAILED	Critical
PNAC	Allocate mem block for Pnac Configuration Message failed	Critical
PNAC	Allocate mem block for Pnac Interface Message failed	Critical
PNAC	PAE: PnacSetPnacPortAuthMode Allocate mem block for Pnac Interface Message failed	Critical

Table 13: List of Syslogs (Continued) (Sheet 3 of 12)

Module	Syslog Message	Severity Level
PNAC	PAE: PnacSetPnacPortAuthControl Allocate mem block for Pnac Interface Message failed	Critical
PNAC	Memory Allocation for PnacCallBackEvent Message failed	Critical
PNAC	Allocate mem block for Pnac Interface Message failed	Critical
PNAC	[NP-FAULT] errors	Alert
WEBNM	Firmware upgrade successful	Notice
WEBNM	WEBNM: Improper realm in HTTP Digest Authentication scheme	Alert
WEBNM	WEBNM: HTTPS session established successfully from <IP address>	Informational
WEBNM	WEBNM: User is blocked, Login Not Allowed	Alert
WEBNM	WEBNM: The RequestDigest sent by the client is INVALID	Alert
WEBNM	WEBNM: Attempt to block the user failed	Alert
WEBNM	WEBNM: Attempt to login with wrong credentials	Alert
WEBNM	WEBNM: User requires password change, redirecting.	Alert
WEBNM	WEBNM: Successfully logged as User	Alert
WEBNM	WEBNM: User successfuly logged out	Informational
WEBNM	WEBNM: Attempt to Login with Wrong Password	Alert
WEBNM	WEBNM: Session logout Idle timer expired for web	Alert
DHCP_SRV	Pool utilization exceeded threshold level	Alert
SNTP	Displaying info of old time, new time, server IP address	Informational
SNTP	No Server Found. Stopping further requests…	Informational
SNTP	Server is not responding. Stopping further requests to this server...	Informational
SNTP	primary server is not responding	Informational

Table 13: List of Syslogs (Continued) (Sheet 4 of 12)

Module	Syslog Message	Severity Level
SNTP	secondary server is not responding	Informational
SNTP	Unable to reach Primary and Secondary Server	Informational
SNTP	Displaying info of old time, new time, server IP address	Informational
LLDP	LldpVlndbNotifyVlnInfoChgForPort Intf Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpVlndbNotifyVlanInfoChg Intf Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpApiNotifyIfCreate: Port <port no>: Intf creation Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpApiNotifyIfMap: Port <port no> : Intf mapping Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpApiNotifyIfDelete: Port <port no> : Intf Deletion Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpApiNotifyIfUnMap: Port<port no> : Intf Unmapping Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpApiNotifyIfAlias: Port <port no> : Intf Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpApiNotifyAgentCircuitId: Port <port no> : Intf Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpApiNotifyIfOperStatusChg: Port <port no> : Intf Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpApiEnqIncomingFrame: Port <port no> : MemAlloc Failed for RxPduQPoolId	Critical
LLDP	LLDPNotifyPortVlanId: Port <port no> : Intf Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpApiNotifyProtoVlanStatus: Port <port no> : Intf Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpApiNotifyProtoVlanId: Port <port no> : Intf Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpApiNotifyPortAggCapability: Port <port no> : Intf Msg ALLOC_MEM_BLOCK FAILED	Critical

Table 13: List of Syslogs (Continued) (Sheet 5 of 12)

Module	Syslog Message	Severity Level
LLDP	LldpApiNotifyResetAggCapability Intf Msg ALLOC_MEM_BLOCK FAILED"	Critical
LLDP	LldpApiNotifyAggStatus: Port <port no> : Intf Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpApiNotifySysName : Mem Allocation Failed for QMsgPoolId while Notifying System Name change	Critical
LLDP	LldpApiNotifySysDesc : Mem Allocation Failed for QMsgPoolId while Notifying System Desc change	Critical
LLDP	LldpApiNotifyIpv6IfStatusChange : Failed to allocate memory for the QMsgPoolId	Critical
LLDP	"LldpApiApplPortReg: Port <port no> : Appln Reg. Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpApiApplPortReg: Port <port no> : Appln TLV Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpApiSetDstMac: Port <port no> : Appln Reg Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	LldpApiNotifyPortDesc : Mem Allocation Failed for QMsgPoolId while Notifying Port Desc change	Critical
LLDP	LldpApiNotifyIfCreate: Port <port no> : Intf creation Msg ALLOC_MEM_BLOCK FAILED	Critical
LLDP	Mempool Allocation Failure for New RemManAddr Node	Critical
LLDP	LldpTlvUpdtUnrecogOrgDefTlv : Mempool Allocation Failure for New Unrecog Org Spec TLV Node - But returning SUCCESS as it is not required to store application TLVS in LLDP"	Critical
LLDP	Mempool Allocation Failure for New RemUnknownTlv Node	Critical
LLDP	LldpIfCreate: Alloc mem block for port FAILED	Critical
LLDP	LldpIfCreate: Alloc mem block for lldp agent mapping FAILED	Critical
LLDP	LldpIfCreate: RBTree add for lldp agent mapping FAILED	Critical

Table 13: List of Syslogs (Continued) (Sheet 6 of 12)

Module	Syslog Message	Severity Level
LLDP	LldpIfCreate: Alloc mem block FAILED	Critical
LLDP	LldpTxUtlAddIpv4Addr : Failed to allocate memory for Local ManAddr Node	Critical
LLDP	(LldpTxUtlAddIpv6Addr) - Failed to allocate memory for Local ManAddr Node	Critical
LLDP	LldpTxUtlAddProtoVlanEntry: Memory allocation failed!!	Critical
LLDP	LldpDot3TlvUpdtOrgSpecTlv: Mempool Allocation Failure for New RemManAddr Node	Critical
LLDP	LldpDot1TlvUpdtProtoVlanIdTlv; Mempool Allocation Failure for New Protocol Vlan Node	Critical
LLDP	LldpDot1TlvUpdtVlanNameTlv: Mempool Allocation Failure for New Vlan Name Node	Critical
LLDP	LldpDot3TlvUpdtOrgSpecTlv: Mempool Allocation Failure for New RemManAddr Node	Critical
PTP1588	No change in profile	Informational
PTP1588	PTP Profile change failed (Domain switch to <domain no> failed)	Error
PTP1588	PTP Profile changed to <profile name>	Informational
PTP1588	printing error	Error
OSPF	Max LSA limit reached for size	Critical
OSPF	LSA Alloc Failure	Critical
OSPF	DDP Processing Stopped Due To LRQ Alloc Failure	Critical
VRRP	Error Observed for VrId <vr id > Address Type <type> with reason	Error
VRRP	Not Master for VRID %d Address Type	Notice
VRRP	Track IP address <ip addr> is DOWN	Informational
VRRP	Track IP address <IP addr> is UP/Restored	Informational
VRRP	Entering VrrpRedInitGlobalInfo	Informational
IGMP	Summarised GroupList Record already exists	Error

Table 13: List of Syslogs (Continued) (Sheet 7 of 12)

Module	Syslog Message	Severity Level
IGMP	Entering IgmpMatchGroupList	Informational
IGMP	Exiting IgmpMatchGroupList	Informational
IGMP	Entering IgmpCheckForLimit	Informational
IGMP	Membership report for group <address> is ignored as Global Limit Reached	Error
IGMP	Membership report for group <address> is ignored as Interface Limit Reached	Error
IGMP	Exiting IgmpCheckForLimit	Informational
IGMP	Entering IgmpMgmtUtilNmhTestv2FsIgmpInterfaceGroupListId	Informational
IGMP	Interfacenode not exist with ifindex	Error
IGMP	Exiting IgmpMgmtUtilNmhTestv2FsIgmpInterfaceGroupListId	Informational
IGMP	Limit should be less than <value>	Error
IGMP	Group List Id should not be zero	Error
IGMP	Group List IP is not in multicast range	Error
IGMP	Inconistent maks is not in multicast range	Error
IGMP	Entry exists	Error
IGMP	Summarised GroupList Record already exists	Error
IGMP	No entry exists with <grplistID>,<grpIP>,<PrefixLen>	Error
IGMP	Limit should be less than MAX_IGMP_MCAST_GRPS	Error
IGMP	Igmp not enabled globally	Error
IGMP	IGMP SSM Mapping should be globally enabled	Error
IGMP	Invalid IGMP SSM Mapping Start Group address	Error
IGMP	Invalid IGMP SSM Mapping End Group address	Error
IGMP	Invalid IGMP SSM Mapping Source address	Error

Table 13: List of Syslogs (Continued) (Sheet 8 of 12)

Module	Syslog Message	Severity Level
IGMP	Starting multicast group range is greater than ending multicast group range	Error
IGMP	IGMP SSM Mapping for the given range of group address is a superset of already configured range	Error
IGMP	IGMP SSM Mapping for the given range of group address to the source address already exists	Error
IGMP	IGMP SSM Mapping Source-List is full for the given range of group address	Error
IGMP	IGMP SSM Mapping for the given range of group address overlaps with already configured range	Error
IGMP	IGMP SSM Mapping for the given range of group address to the source address does not exist	Error
Watchdog	Reading status of <taskname> as NOT ACTIVE	Alert
Watchdog	Generating core dump	Alert
Watchdog	Timer expired but associted registered task does NOT exists	Alert
Snooping	Memory allocation for group entry failed	Critical
Snooping	[NP-FAULT]	Alert
Snooping	Memory alloc for ASM Host entry failed	Critical
Snooping	Memory allocation for port entry for group failed	Critical
Snooping	Memory alloc for Host entry for group failed	Critical
Snooping	Memory allocation for SSM host source bitmap failed	Critical
Snooping	Memory allocation for SSM port entry for group failed	Critical
Snooping	Memory allocation for SSM port source bitmap failed	Critical
Snooping	Memory allocation for Host entry for group failed	Critical
Snooping	Memory allocation for SSM host source bitmap failed	Critical

Table 13: List of Syslogs (Continued) (Sheet 9 of 12)

Module	Syslog Message	Severity Level
Snooping	Memory allocation for consolidated group entry failed	Critical
Opensource/SSH	Failed to Establish Connection with client,max session exceeded	Alert
Opensource/SSH	Bad protocol version identification	Alert
Opensource/SSH	SSL ssl23_read_bytes: No data or Invalid data/port from <IP>	Alert
CFA2	CFA updated status to watchdog as ACTIVE Failed	Alert
CFA2	<intf> Link Status [DOWN/UP]	Alert
CFA2	IP Address change in Default vlan interface	Notice
System	Physical Index Validation Failed	Critical
System	Physical Contained In Get Operation Failed	Critical
System	Physical Class Get Operation Failed	Critical
System	Physical Parent Relative Position Get Operation Failed	Critical
System	Physical Name Get Operation Failed	Critical
System	Physical Hardware Revision Get Operation Failed	Critical
System	Physical Firmware Revision Get Operation Failed	Critical
System	Physical Software Revision Get Operation Failed	Critical
System	Physical Serial Number Get Operation Failed	Critical
System	Physical component Manufacturer's Name Get Operation Failed	Critical
System	Physical component's Model Name Get Operation Failed	Critical
System	Physical component's Alias Name Get Operation Failed	Critical
System	Physical component's Asset Id Get Operation Failed	Critical
System	Physical component's FRU status Get Operation Failed	Critical

Table 13: List of Syslogs (Continued) (Sheet 10 of 12)

Module	Syslog Message	Severity Level
System	Physical component's Mfg Date Get Operation Failed	Critical
System	Physical component's Uris Name Get Operation Failed	Critical
System	Physical component's Serial Num Set Operation Failed	Critical
System	Physical component's Serial Number Set Operation Failed	Critical
System	Physical component's Alias Name Set Operation Failed	Critical
System	Physical component's Asset Id Set Operation Failed	Critical
System	Physical component's Uris Id Set Operation Failed	Critical
System	Logical Index Validation Failed	Critical
System	Logical Component's Community Get Operation Failed	Critical
System	Logical Component's Context Name Get Operation Failed	Critical
System	Logical Component's Context Name Get Operation Failed	Critical
System	LP Mapping Validation Failed	Critical
System	Alias Mapping Validation Failed	Critical
System	Physical Contains Table validation Failed	Critical
System	Firmware upgrade successful ..	Notice
System	Saved configuration to USB successfully!	Informational
System	Firmware switch partition cancelled..!	Debug
System	Firmware switch partition successful	Notice
System	Factory reset cancelled.	Debug
System	Factory reset initiated..	Debug
System	Factory reset Failed.	Debug
System	Factory reset users cancelled.	Debug

Table 13: List of Syslogs (Continued) (Sheet 11 of 12)

Module	Syslog Message	Severity Level
System	Factory reset users initiated.	Debug
System	Factory reset users Failed.	Debug
System	Reload operation cancelled	Debug
System	Saved configuration to FLASH successfully	Informational
System	Saved configuration to remote(TFTP) successfully	Informational
System	Saved configuration to remote(SFTP) successfully!	Informational
System	Firmware upgrade successful	Notice
CLI	Attempt to login as <user details> via telnet from <IP> Succeeded	Alert
CLI	Attempt to login as <user name> via console Succeeded	Alert
CLI	User <username> logged in via <CLI_mode>	Informational
CLI	User <user name> <IP> <cli_mode>logged out from	Informational
CLI	User <user name> <IP> <cli_mode> forcefully logged out from	Informational
CLI	Password expired for user <username>	Alert
CLI	Password credentials updated successfully for User <username>	Alert
CLI	Password must be reset for user <user name>	Alert
CLI	Attempt to login as <username > via telnet <IP>	Alert
CLI	Attempt to login as <username > via SSH <IP>	Alert
CLI	Attempt to block the user <username> failed	Alert
CLI	Login failed : Login incorrect <username> via <CLI_mode> <IP>	Informational
FSAP2	Displaying ISS status	Critical
FSAP2	Displaying error reason	Critical
FSAP2	Displaying MempoolErr ID	Critical
FSAP2	Displaying MempoolErr ID owner	Critical

Table 13: List of Syslogs (Continued) (Sheet 12 of 12)

Module	Syslog Message	Severity Level
TCP	No MD5 digest from <srcAddr,port> to <DstAddr,port>	Informational
TCP	Bad MD5 digest from <srcAddr,port> to <DstAddr,port>	Informational
TCP	Multiple TCP-AO option in one segment from <srcAddr,port> to <DstAddr,port>	Informational
TCP	TCP-AO & TCP MD5 option in one segment from <srcAddr,port> to <DstAddr,port>	Informational
TCP	TCP-AO MAC from <srcAddr,port> to <DstAddr,port> No MKT Match Discard Packet	Informational
TCP	TCP-AO not expected but found, silent accept from <srcAddr,port> to <DstAddr,port>	Informational
TCP	No TCP-AO MAC from <srcAddr,port> to <DstAddr,port>	Informational
TCP	TCP-AO MAC MKT mismatch from <srcAddr,port> to <DstAddr,port>	Informational
TCP	Bad TCP-AO MAC from <srcAddr,port> to <DstAddr,port>	Informational
TCP	Connection attempt to closed/non-active TCP port. Possible Replay attack. <srcAddr,port> to <DstAddr,port>	Warning
TCP	Invalid segment of data received Possible Replay attack. <srcAddr,port> to <DstAddr,port>	Warning

12.24. logging

To enable the Syslog server and configure Syslog related parameters, use the command **logging** in Global Configuration Mode. The no form of the command disables syslog server and resets the configured parameters. The existing syslog buffers will not be cleared and none of the configured options will be changed, when the Syslog feature is disabled.

The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or Syslog server.

The log file is stored in ASCII text format. The Privileged EXEC command is used to display its contents.

logging

```
logging {console

 | facility {local0 | local2 | local3 | local4 | local5 | local6 | local7} |
local {buffered <buffer size integer (1-4096)> | {flash {alerts | critical |
debugging | emergencies | errors | informational | notification | warnings}
file <file name string (32)>}

 | on

 | remote {alerts | critical | debugging | emergencies | errors | informa-
tional | notification | warnings} {<dns_host_name> | ipv4 <ucast_addr> |
ipv6 <ipv6_addr>} [ port < integer(1-65535) > ] [ { udp | tcp | beep | tls } ]

 | severity [<level value (0-7)>] [alerts] [critical] [debugging] [emergen-
cies] [errors] [informational] [notification] [warnings]}
```

no logging

```
no logging {buffered | console | facility | local | on | remote | severity}
```

Parameters

Parameter	Type	Description
`console`		Enter to enable Syslog server and configure the Syslog server IP address, the log-level and other Syslog related parameters.
`facility`		Enter to configure facility code level. Messages with different facilities can be handled differently. There are total of 8 facility levels ranging between local0 and local7. Each facility level has a value assigned to it—local0 (128), local1 (136), local2 (144), local3(152), local4(160), local5(168), local6(176), and local7 (184). The idea of the facility level configuration is to differentiate and filter logs.
`local0`		Enter to have facility is set as local0. Default facility level is local0.
`local1`		Enter to have facility is set as local1.
`local2`		Enter to have facility is set as local2.
`local3`		Enter to have facility is set as local3.
`local4`		Enter to have facility is set as local4.
`local5`		Enter to have facility is set as local5.
`local6`		Enter to have facility is set as local6.
`local7`		Enter to have facility is set as local7.
`<file size integer (1-10>`	Integer	Enter a number for the maximum size (in MB) of the log file.
`local`		Enter to enable local logging.
`buffered`		Enter to configure the limit for the Syslog messages displayed from an internal buffer.
`<buffer size integer 1-4096)>`		Enter a number of entries for buffer size. The default size is 200 entries.
`flash`		Enter to enable local logging. The severity is as follows.
`alerts`		Enter to configure logging when immediate action must be taken. For example, a condition that should be corrected immediately, such as a corrupted system database.
`critical`		Enter to configure logging for Critical conditions. For example, hard device errors.

Parameter	Type	Description
debugging		Enter to configure logging of Debug-level messages. For example, messages that contain information normally of use only when debugging a program
emergencies		Enter to configure logging of panic conditions e.g. unstable system.
errors		Enter to configure logging of error conditions. This can be any error condition happened in the system operation.
informational		Enter to configure logging of informational messages.
notification		Enter to configure logging of normal but significant messages. Examples are conditions that are not error conditions, but that may require special handling.
warnings		Enter to configure logging of warning conditions. For example, any specified abnormalities happening in the system operation.
file		Enter to configure the flash file name.
<file name string (32)	String	Enter a flash file name. This is a string value with a maximum size as 32.
on		Enter to enable Syslog server and the Syslog server IP address, the log-level and other Syslog related parameters.
remote		Enter to enable remote logging.
<dns_host_name>		Enter a host domain name.
ipv4		Enter to configure an IPv4 address
<ucast_addr>	A.B.C.D	Enter an IPv4 address
ipv6		Enter to configure an IPv4 address
<ucast_addr>	AAAA::BBBB	Enter an IPv6 address
severity		Enter to configure severity for the messages.
<level value integer (0-7)>	Integer	Enter a number for severity level.
port	Integer	The port range can be 1 - 65535.

Parameter	Type	Description
{udp|tcp|beep|tls}		Transport mode is set to either udp, tcp, beep, TLS

Mode

Global Configuration Mode

Examples

iS5comm (config)# logging local buffered 200

iS5comm(config)# logging facility local1

iS5comm(config)# logging remote alerts ipv4 192.168.20.77 port 15010 tls

iS5comm(config)# no logging remote alerts ipv4 192.168.20.77

iS5comm(config)# logging remote alerts ipv4 192.168.20.77 tls

12.25. syslog format

This command sets the format of the syslogs to either RFC3164 or RFC5424.

syslog format

```
syslog format { rfc3164 | rfc5424 }
```

Parameters

Parameter	Type	Description
rfc3164		RFC3164 is the old format and the default mode.
rfc5424		RFC5424 is the advanced format with high precision timings and extra fields.

Mode

Global Configuration Mode

Examples

iS5comm(config)# syslog format rfc5424

NOTE: Changing the syslog format will erase the local/remote logging configurations.

12.26. secure logging crypto key

This CLI helps to configure the certificates required for secure syslog communication over TLS. We need three files, certificate signed by CA, private key and a root CA. This is a global settings and there is no unconfigure command. User can just overwrite the file name if he needs to use a different certificate.

secure logging crypto key

```
secure logging crypto key < string(100) > cert < string(100) > ca-cert <
string(100) >
```

Description

This CLI helps to configure the certificates required for secure syslog communication over TLS. We need three files, certificate signed by CA, private key and a root CA. This is a global settings and there is no unconfigure command. User can just overwrite the file name if he needs to use a different certificate.

These key and certificates will take effect only when user configures his transport mode as TLS.

These certificates are generated/imported using crypto PKI infrastructure.

This command execution will throw error when the corresponding certificate or key file is not already generated or imported using PKI tool.

Parameters

Parameter	Type	Description
key <string(100)>	string	Private key for switch client.
cert <string(100)>	string	Certificate for switch client.
ca-cert <string(100)	string	Root CA, which has signed both the server and client node certificates.

Mode

Global Configuration Mode

Examples

iS5comm(config)# secure logging crypto key r1Key.pem cert r1Cert.pem ca-cert CA.pem

Related Commands:

iS5comm# show crypto pki

Other related command:

crypto pki keygen <file-prefix(32)> {RSA2048 | RSA4096} { default | <country(2)> <state(100)>

<locality(100)> <organization(100)> <organizational-unit(100)> <common-name(100)> | current}

12.27. mail-server

To configures the mail server address used for sending email alert messages, use the command **mail-server** in Global Configuration Mode. The no form of the command deletes the mail server address from the mail table.

mail-server

```
mail-server <short(0-191)> {ipv4 <ucast_addr> | ipv6 <ip6_addr> |
<dns_host_name>} <string(50)> [user <user_name> password <password>]
```

no mail-server

```
no mail-server <short(0-191)> {ipv4 <ucast_addr> | ipv6 <ip6_addr> |
<dns_host_name>}
```

Parameters

Parameter	Type	Description
<short(0-191)>	Integer	Enter to set the priority for that particular mail-server configuration. This value ranges from 0 to 191.
ipv4	A.B.C.D	Enter to configure the ipv4 destination address for the syslog mail server.
<ucast_addr>		Enter the ipv4 destination address for the syslog mail server. The format for the Mail server ID is a string of size 50
ipv6	AAAA:BBBB.	Enter to configure the ipv6 destination address for the syslog mail server.
<ip6_addr>		Enter the ipv6 destination address for the syslog mail server. The format for IPv6 address is AAAA:BBBB.
<dns_host_name>		Enter to configure the DNS host name for the syslog mail server. This value is a string of size 255.
<string(50)>		Enter to specify the receiver mail id in which the email alert messages are received and logged. This value is a string of maximum size 50.
user		Enter to configure the user name of the account in the mail server to which the mails is to be sent. The user name is used only if a valid authentication method is configured for the system.
<user_name>		Enter the user name of the account in the mail server to which the mails is to be sent. This value is a string of maximum size 64.
password		Enter a valid email address for the sender.
<password>		Enter to set the password to authenticate the user name in the mail server. The password is used only if a valid authentication method is configured for the system. This value is a string of maximum size 64.

Mode

Global Configuration Mode

Examples

iS5comm(config)# mail-server 190 ipv4 23.78.67.89 support@iS5Com.com

12.28. sender

To set the sender mail id from which the email alert messages are sent, use the command **sender** in Global Configuration Mode. The no form of the command deletes the configured sender mail id.

sender

```
sender mail-id <mail-id string(100)>
```

no sender

```
no sender mail-id
```

Parameters

Parameter	Type	Description
`mail-id`		Enter to configure mail id for the sender.
`<mail-id string(100)>`		Enter a valid email address for the sender.

Mode

Global Configuration Mode

Default

syslog@iS5Com.com

Prerequisites

This command can be executed only if the mail server is configured.

Examples

iS5comm(config)# sender mail-id plabinik@iS5Com.com

12.29. cmdbuffs

To configure the number of syslog buffers for a particular user, use the command **cmdbuffs** in Global Configuration Mode.

cmdbuffs

```
cmdbuffs <user name> <no.of buffers (1-200)>
```

Parameters

Parameter	Type	Description
<user name>		Enter an user name
<no.of buffers (1-200)>	Integer	Enter the number of log buffers to be allocated in the system. This is an integer with a maximum length of 200.

Mode

Global Configuration Mode

Default

50

Examples

iS5comm(config)# cmdbuffs iS5Com 50

12.30. clear logs

To clear the system syslog buffers, use the command **clear logs** in Global Configuration Mode or Privileged EXEC Mode.

clear logs

```
clear logs
```

Mode

Privileged EXEC Mode / Global Configuration Mode

Examples

iS5comm(config)# cmdbuffs iS5Com 50

12.31. syslog

To configure the first file, the second, and third file to store the syslog messages locally, enable the syslog file storage to log the status in the local storage path, enable the syslog mail storage in the system, set the profile for reliable syslog, change the syslog role from device to relay, set the Syslog relay transport type either as UDP or TCP, use the command **syslog** in Global Configuration Mode. By enabling syslog mail storage, the device sends the syslog messages as mail messages to the mail-server configured in the system. The no form of command disables the syslog mail storage, the mail option in syslog, sets the profile to default (raw), changes the syslog role from relay to device, and Set the Syslog Port to default port 514.

syslog

```
syslog {filename-one <filename <string(32)> | filename-two <filename
<string(32)> | filename-three <filename <string(32)> localstorage | mail |
profile {raw |cooked} | relay [<port number (0-65535)>] [transport type {tcp
| udp} | relay-port <port number (0-65535)>}
```

no syslog

```
no syslog {localstorage | mail | profile | relay | relay-port}
```

Parameters

Parameter	Type	Description
filename-one		Enter to configure a first file to store the syslog messages locally. **NOTE:** This command is executed only if syslog local storage is enabled.
<filename <string(32)>	String	Enter a name for the first file. The maximum size of the file name is 32 characters.
filename-two		Enter to configure a second file to store the syslog messages locally **NOTE:** This command is executed only if syslog local storage is enabled.
<filename <string(32)>	String	Enter a name for the second file. The maximum size of the file name is 32 characters.
filename-three		Enter to configure a third file to store the syslog messages locally. **NOTE:** This command is executed only if syslog local storage is enabled.
<filename <string(32)>	String	Enter a name for the third file. The maximum size of the file name is 32 characters.
localstorage		Enter to enable the syslog file storage to log the status in the local storage path.
mail		Enter to enable the syslog mail storage in the system. By enabling syslog mail storage, the device sends the syslog messages as mail messages to the mail-server configured in the system.
profile		Enter to set the profile for reliable syslog.
raw		Enter to set the syslog profile as raw which is the profile for the transport type beep. This is the default option.
cooked		Enter to set the syslog profile as cooked.
relay		Enter to change the syslog role from device to relay. **NOTE:** This command is executed only if syslog local storage is enabled.
<port number (0-65535)>	Integer	Enter a port number through which syslog messages are received. The default port is 514.
transport		Enter to configure the Syslog transport/
type		Enter to configure the Syslog transport type.
tcp		Enter to configure the Syslog transport type as TCP.
udp		Enter to configure the Syslog transport type as UDP.
relay-port		Enter to setsthe syslog port through which the relay receives the syslog messages irrespective of the transport type

Parameter	Type	Description
<port number (0-65535)>	Integer	Enter a port number through which syslog messages are received. The default port is 514.

Mode

Global Configuration Mode

Examples

iS5comm (config)# syslog filename-one iS5Com1

iS5comm (config)# syslog filename-two iS5Com2

iS5comm (config)# syslog filename-three iS5Com3

iS5comm (config)# syslog localstorage

iS5comm (config)# syslog mail

iS5comm (config)# syslog profile raw

iS5comm (config)# syslog relay

iS5comm (config)# syslog relay transport type udp

12.32. show logging

To display all logging status and configuration information, use the command **show logging** in Privileged EXEC Mode.

show logging

Mode

Privileged EXEC Mode

Examples

iS5comm# show logging

```
System Log Information
----------------------
Syslog logging   : enabled(Number of messages 159)
Console logging  : disabled(Number of messages 0)
TimeStamp option : enabled
```

```
Severity logging     : Critical
Facility         : Default (local0)
Buffered size    : 200 Entries

LogBuffer(164 Entries, 169248 bytes)
<129>Jun  6 19:19:40 ISS CFA DOWN
<129>Jun  6 19:19:40 ISS CFA DOWN
<129>Jun  6 19:19:43 ISS NPAPI Slot0/9 Link Status [UP]
<129>Jun  6 19:19:43 ISS CFA vlan1 Link Status [UP]
<129>Jun  6 19:19:43 ISS CFA vlan1 Link Status [UP]
<129>Jun  6 19:19:50 ISS FM [FM - SYS] : PowerSupply: 0 volts exceeds
the limit. Max power supply is 240 volts and Min power supply is 100
volts
```

12.33. show flash logs

To display the flash contents, use the command **show flash logs** in Privileged EXEC Mode.

show flash logs

Mode

Privileged EXEC Mode

Examples

iS5comm # show flash logs

```
Name: fsir.log.2452   ,  Size: 4630       ,  Updated: Mon Aug  6
04:14:23 2018Name: fsir.log.2424   ,  Size: 208        ,  Updated: Mon
Nov  5 00:14:18 2018Name: fsir.log.2421   ,  Size: 81         ,
Updated: Mon Nov  5 00:44:10 2018
```

12.34. show email alerts

To display configurations related to email alerts, use the command **show email alerts** in Privileged EXEC Mode.

show email alerts

Mode

Privileged EXEC Mode

Prerequisites

This command is executed only if mail server is configured.

Examples

iS5comm(config)# show email alerts

```
    Sender email-id   : support@iS5Com.com
```

12.35. show syslog

To display all file names for Syslog local storage, the status of consolidated syslog log information, syslog local storage Syslog role, status of the mail option, the Syslog profile, Syslog relay transport type, and Syslog role, use the command **show syslog** in Privileged EXEC Mode.

show syslog

```
show syslog {file-name | information | localstorage | mail | profile | relay
[transport type] | relay-port | role}
```

Parameters

Parameter	Type	Description
file-name		Enter to display all file names for Syslog local storage.
information		Enter to display the status of consolidated syslog log information.
localstorage		Enter to display the Syslog local storage.
mail		Enter to status of the mail option.
profile		Enter to display the Syslog profile.
relay		Enter to display the Syslog relay transport type.
transport		Enter to display the Syslog relay transport type.
type		Enter to display the Syslog relay transport type.
relay-port		Enter to display the relay port related configuration.
role		Enter to display the Syslog role.

Mode

Privileged EXEC Mode

Examples

iS5comm(config)# show syslog file-name

```
Syslog File Name
----------------------
Syslog File-One :is5
Syslog File-Two :
Syslog File-Three :
```

iS5comm# show syslog information

```
System Log Information
----------------------
Syslog Localstorage   : Enabled
Syslog Mail Option    : Disabled
Syslog Port    : 514
Syslog Role    : Relay
Smtp Authentication   : None
```

iS5comm# show syslog localstorage

```
Syslog Localstorage: Enabled
```

iS5comm# show syslog mail

```
Syslog Mail Option    : Enabled
```

iS5comm# show syslog profile

```
Syslog Profile    : raw
```

iS5comm# show syslog relay transport type

```
Syslog Relay Transport type udp
```

iS5comm# show syslog relay-port

```
Syslog Port    : 514
```

iS5comm# show syslog role

```
Syslog Role    : Relay
```

12.36. show logging-server

To display the information about the Syslog logging server table, use the command **show logging-server** in Privileged EXEC Mode.

show logging-server

Mode

Privileged EXEC Mode

Examples

iS5comm# show logging-server

```
Syslog Forward Table Information
--------------------------------
Priority  Address-Type   IP Address Port   Trans-Type
--------  ------------   --------- ----   ----------
1         host           abc.com 2      tcp
129       ipv4           12.0.0.2 514    udp
191       ipv6           1111::2222 514    udp
```

12.37. show logging-file

To display the priority and file name of all three files configured in the syslog file table, use the command **show logging-file** in Privileged EXEC Mode.

show logging-file

Mode

Privileged EXEC Mode

Examples

iS5comm# show logging-file

```
Syslog File Table Information
-----------------------------
Priority    File-Name
--------    ----------
128          is5
129          is5
```

12.38. show mail-server

To display the information about the Syslog mail server table, use the command **show mail-server** in Privileged EXEC Mode.

show mail-server

Mode

Privileged EXEC Mode

Examples

iS5comm# show mail-server

```
    Syslog Mail Table Information
    -----------------------------

    Priority  Address-Type   IP Address       Receiver Mail-Id  User Name
    --------  ------------   ---------       ----------------  --------
    0         host           abc.com  mail@yahoo.com  user1

    1         ipv4           15.0.0.100  mail1@example.com  user2

    2         ipv6           1111::2222  mail2@example.com
```

12.39. smtp authentication

To set the Simple Mail Transfer Protocol (SMTP) authentication method while sending E-mail alerts to the mail server configured, use the command **smtp authentication** in Global Configuration Mode. The no form of the command resets the authentication method to send email alerts with any authentication.

smtp authentication

```
smtp authentication {auth-login | auth-plain | cram-md5 | digest-md}
```

no smtp authentication

```
no smtp authentication
```

Parameters

Parameter	Type	Description
auth-login		Enter to set the smtp authentication method as auth-login in which both the user name and password are BASE64 encoded.
auth-plain		Enter to set the smtp authentication method as auth-plain in which the user name and password used for authentication are combined to one string and BASE64 encoded
cram-md5		Enter to set the BASE64 encoded user name and 16-byte digest in hexadecimal notation. The digest is generated using HMAC calculation with password as secret key and SMTP server original challenge as the message.
digest-md		Enter to set the smtp authentication method as digest-md5 in which the BASE64 encoded MD5 digest response string that is calculated using the user name, password, realm string and nonce string.

Mode

Global Configuration Mode

Examples

iS5comm(config)# smtp authentication auth-login

12.40. logsize

To set the threshold limit of the logging file size, use the command **logsize** in Global Configuration Mode.

logsize

```
logsize <log size integer (1-95)>
```

Parameters

Parameter	Type	Description
<log size integer (1-95)	Integer	Enter a threshold value. It is in percents.

Mode

Global Configuration Mode

Examples

iS5comm(config)# logsize 95

Serial

13. Serial

Serial support in the device software includes Modbus Client and Server modes as well as Raw Socket mode. This chapter describes the CLI commands needed to enable these capabilities.

13.1. CLI Serial Command Modes

Depending on the CLI mode, iS5comm prompt will be specific. This cannot be changed by the end user. For example, when the command mode is Global Configuration, the prompt display will be `iS5comm(config)#`.

The hierarchical structure of the command modes used for serial interface is as shown on the figure below.

Figure 1: CLI Command Modes

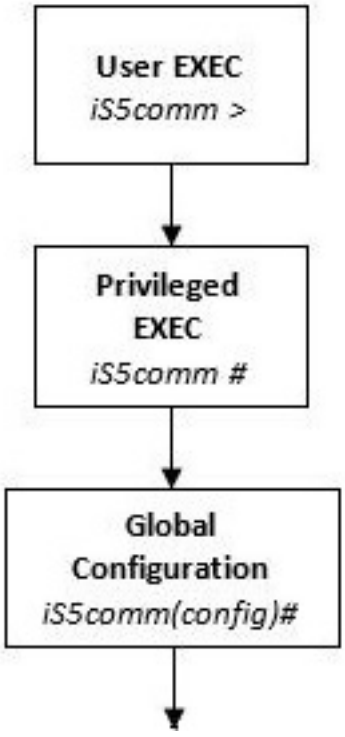
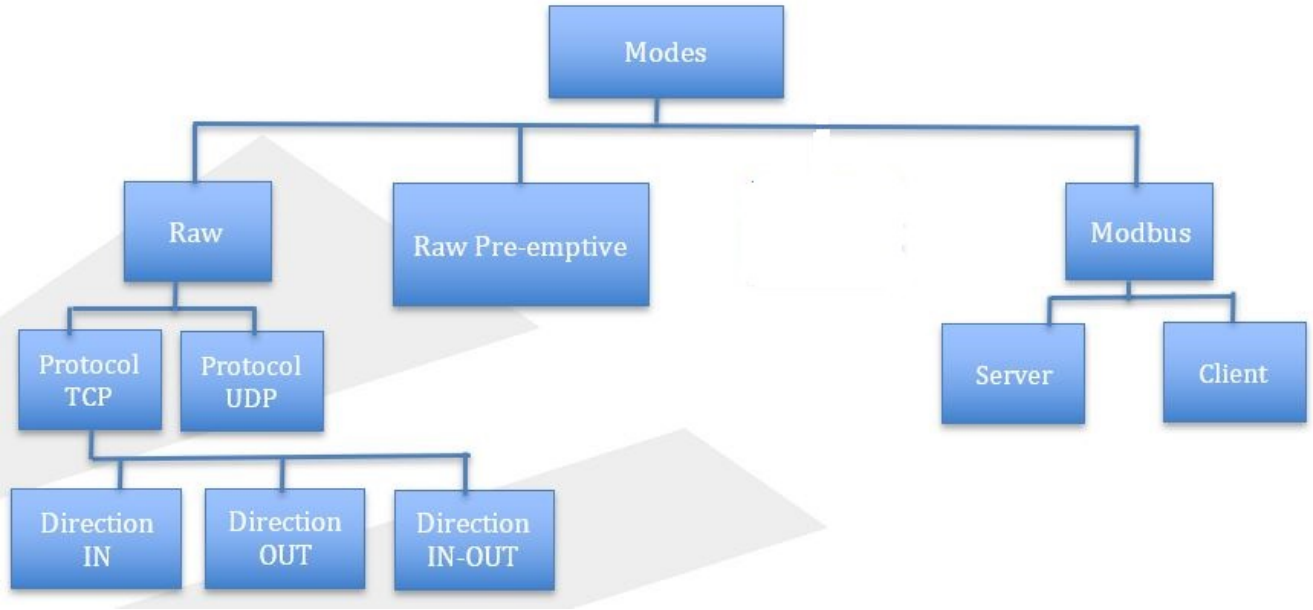


Figure 2: Serial Module only CLI Command Modes


Modes
Raw
Raw Pre-emptive
Modbus
Protocol TCP
Protocol UDP
Server
Client
Direction IN
Direction OUT
Direction IN-OUT

User Exec Mode

Prompt	Access method	Exit Method
`iS5comm>`	This is the initial mode to start a session.	logout

Privileged Exec Mode

Prompt	Access method	Exit Method
`iS5comm#`	The User EXEC mode command `enable` is used to enter the Privileged EXEC Mode	To return from the Privileged EXEC Mode to User EXEC mode, the command `disable` is used.

Global Configuration Mode

Prompt	Access method	Exit Method
`iS5comm(config)#`	The Privileged EXEC mode command `configure terminal` is used to enter the Global Configuration Mode.	To return from the Global Configuration Mode to Privileged Mode, the command `exit` is used.

Serial Interface Configuration Mode

Prompt	Access method	Exit Method
`iS5comm(config-serial-if)#`	The Global Configuration mode command `iS5comm(config)# interface serial 0/9` is used to enter the Serial Interface Configuration Mode.	To return from the Interface Configuration mode to Global Configuration Mode, the command `exit` is used. To exit from the Interface Configuration mode to Privileged EXEC Mode, the command `end` is used.

Serial Profile Mode (Raw Socket)

Prompt	Access method	Exit Method
`iS5comm(raw-p1)#`	The Global Configuration mode command `iS5comm(config)# serial connection-type raw profile p1` is used to enter the Serial Profile Mode.	To return from the Serial Profile mode to Global Configuration Mode, the command `exit` is used. To exit from the VLAN Interface Configuration mode to Privileged EXEC Mode, the command `end` is used.

Serial Profile Mode (Preemptive-raw)

Prompt	Access method	Exit Method
`iS5comm(preemptive-p2)#`	The Global Configuration Mode command **`iS5comm(config)# serial connection-type preemptive-raw profile p2`** is used to enter the Profile Mode (Preemptive).	To exit from the Serial Profile Mode (Preemptive) to Privileged EXEC Mode, the command `end` is used.

Serial Profile Mode (UDP)

Prompt	Access method	Exit Method
`iS5comm(raw-udp)#`	The Global Configuration Mode command **`iS5comm(config)# serial connection-type raw profile udp`** is used to enter the Profile Mode (UDP).	To exit from the Serial Profile Mode (UDP) to Privileged EXEC Mode, the command `end` is used.

Serial Profile Mode (TCP)

Prompt	Access method	Exit Method
`iS5comm(raw-tcp)#`	The Global Configuration Mode command **`iS5comm(config)# serial connection-type raw profile tcp`** is used to enter the Profile Mode (TCP).	To exit from the Serial Profile Mode (UDP) to Privileged EXEC Mode, the command `end` is used.

Serial Profile Mode (Modbus)

Prompt	Access method	Exit Method
`iS5comm(modbus-m1)#`	The Global Configuration Mode command **`iS5comm(config)# serial connection-type modbus profile m1`** is used to enter the Profile Mode (Modbus).	To exit from the Serial Profile Mode (Modbus) to Privileged EXEC Mode, the command `end` is used.

Transport Protocol TCP Mode

Prompt	Access method	Exit Method
`iS5comm(raw-tcp-TCP)#`	The Serial Profile mode command `iS5comm (raw-tcp)# transport protocol tcp` is used to enter the Transport Protocol TCP Mode.	To exit from the Transport Protocol Mode to Privileged EXEC Mode, the command `end` is used.

Transport Protocol UDP Mode

Prompt	Access method	Exit Method
`iS5comm (raw-udp-UDP)#`	The Serial Profile mode command `iS5comm (raw-p1)# transport protocol udp` is used to enter the Transport Protocol UDP Mode.	To exit from the Transport Protocol Mode to Privileged EXEC Mode, the command `end` is used.

Direction (In) Mode (Raw)

Prompt	Access method	Exit Method
`iS5comm(raw-p1-TCP-in)#`	The Transport Protocol mode command **`iS5comm(serial-p1-TCP)# direction in`** is used to enter the Direction IN Mode (Raw Socket).	To exit from the Direction Mode (Raw Socket) to Privileged EXEC Mode, the command `end` is used.

Direction (Out) Mode (Raw)

Prompt	Access method	Exit Method
`iS5comm(raw-p1-TCP-out)#`	The Transport Protocol mode command **`iS5comm(serial-p1-TCP)# direction out`** is used to enter the Direction OUT Mode (Raw Socket).	To exit from the Direction Mode (Raw Socket) to Privileged EXEC Mode, the command `end` is used.

Direction (IN-OUT) Mode (Raw)

Prompt	Access method	Exit Method
`iS5comm(raw-p1-TCP-InOut)#`	The Transport Protocol mode command **`iS5comm(serial-p1-TCP)# direction in-out`** is used to enter the Direction IN-OUT Mode (Raw Socket).	To exit from the Direction Mode (Raw Socket) to Privileged EXEC Mode, the command `end` is used.

Role Mode (Modbus server)

Prompt	Access method	Exit Method
`iS5comm(modbus-m1-server)#`	The Transport Protocol mode command **`iS5comm(config)# serial connection-type modbus profile m1;iS5comm(modbus-m1)# role server`** is used to enter the Role Mode (Modbus server).	To exit from the Role Mode (Modbus) to Privileged EXEC Mode, the command `end` is used.

Role Mode (Modbus client)

Prompt	Access method	Exit Method
`iS5comm(modbus-m1-client)#`	The Transport Protocol mode command **`iS5comm(config)# serial connection-type modbus profile m1;iS5comm(modbus-m1)# role client`** is used to enter the Role Mode (Modbus server).	To exit from the Role Mode (Modbus) to Privileged EXEC Mode, the command `end` is used.

13.2. add slave-id

To define the MODBUS profile to act either as server or client, use the **add slave-id** command in Role Mode. Modbus is a stateless client-server (master -slave) protocol. A transaction consist of two

messages: a request (issued by the client) and a response (issued by the server).

Each MODBUS server or client are uniquely identified by a slave ID. The MODBUS server slave IDs are bound to an interface, whereas MODBUS client slave IDs is bound to a profile. This is because a MODBUS server can support multiple interface to be mapped to same profile. Each interface can be mapped to a set of slave IDs.

Each profile can support 247 slave IDs and its range is between 1 - 247.

add slave-id

```
MODBUS server
 add slave-id
 <ids> interface serial <interface-id>
 remove slave-id
 <ids> interface serial <interface-id>

 MODBUS client
 add slave-id
 <ids>
 remove slave-id
 <ids>
```

Parameters

Parameter	Type	Description
ids (1-247)	Integer	Enter an ID number.

13.3. add udp-host

To add an UDP remote host with which the device to communicate, use the **add udp-host** command in Transport Protocol UDP Mode. By this command, we can restrict the device to allow data transfer to only selected remote host / clients.

add udp-host

```
add udp-host
 {<IpAddress> port <integer(1-65535)>
```

Parameters

Parameter	Type	Description
<IpAddress>	A.B.C.D	Unicast IP address of the remote host.
port		Enter for a port of the UDP remote host.
<integer(1-65535)>		Enter a port number of the remote host.

Mode

Transport Protocol UDP Mode

Examples

iS5comm(config)# serial connection-type raw profile udp

iS5comm(raw-udp)# transport protocol udp

iS5comm(raw-udp-UDP)# add udp-host 192.168.20.66 port 35478

iS5comm(raw-udp-UDP)# end

13.4. baud-rate

To define the baud rate, use the **baud rate** command in Interface Configuration Mode. The baud rate is the rate at which information is transferred in a serial communication channel. In the serial port context, "9600 baud" means that the serial port is capable of transferring a maximum of 9600 bits per second.

baud-rate

```
baud-rate
 <integer>
```

no baud-rate

```
no baud-rate
```

Parameters

Parameter	Type	Description
integer	Integer	Enter a number that represent the baud-rate setting. The available values are: • 1200 baudrate of 1200 bps • 2400 baudrate of 2400 bps • 4800 baudrate of 4800 bps • 9600 baudrate of 9600 bps • 14400 baudrate of 14400 bps • 19200 baudrate of 19200 bps • 38400 baudrate of 38400 bps • 57600 baudrate of 57600 bps • 115200 baudrate of 115200 bps • 230400 baudrate of 230400 bps

Mode

Serial Interface Configuration Mode

Examples

iS5comm(config)# configure terminal

iS5comm(config)# interface serial 0/9

iS5comm(config-serial-if)# baud-rate 115200

iS5comm(config-if)# no baud-rate

NOTE: “no baud-rate” will revert back the baud rate settings to the default value which is 9600.

13.5. clear serial config

To erase all serial profile configurations from the system, use the **clear serial config** command in Global Configuration Mode.

clear serial config

```
clear serial config
 [MODBUS] [RAW_SOCKET]
```

Parameters

Parameter	Type	Description
MODBUS		When selected, it clears only MODBUS configuration.
RAW_SOCKET		When selected, it clears only Raw Socket configuration.

Mode

Global Configuration Mode

Examples

iS5comm(config)# clear serial config ?

```
<CR>                                Erase all serial profile
configurations from the system
MODBUS                              MODBUS configurations
RAW_SOCKET                        RAW_SOCKET configurations
```

iS5comm(modbus-m20)# clear serial config

```
Note:  "clear serial config" will erase entire serial profile
configurations...

Are you sure you want to clear it? (Y/N) [N]? y
Erasing configurations ...
```

iS5comm(config)# clear serial config MODBUS

```
Note:  "clear serial config" will erase entire MODBUS
configurations...

Are you sure you want to clear it? (Y/N) [N]? y
Erasing configurations ...
iS5comm(config)#
```

iS5comm(config)# clear serial config RAW_SOCKET

```
Note:  "clear serial config" will erase entire raw socket
configurations...

Are you sure you want to clear it? (Y/N) [N]? y
Erasing configurations ...
iS5comm(config)#
```

13.6. clear serial counters

To clear application level serial profile counters, use the **clear serial counters** command in Global Configuration Mode. There are three options available: clearing of interface level, profile level, or all serial profile counters.

clear serial counters

```
clear serial counters
 [interface serial <interface-id>] [profile <string(64)>]
```

Parameters

Parameter	Type	Description
interface		Enter to select interface.
serial		Enter to select serial interface.
interface-id (<0>/<9-16>)		Enter a value for serial interface ID. 0/9-0/12 or 0/9-0/16
profile		Enter to select serial interface.
<string(64)>		Enter a value for profile name.

Mode

Global Configuration Mode

Examples

iS5comm(config)# clear serial counters

iS5comm(config)# clear serial counters interface serial 0/9 profile p1

iS5comm(config)# clear serial counter profile p1

13.7. connection-map interface

To map the profile to an physical serial interface, use the **connection-map interface** command in Serial Profile Mode. The profile gets activated with this operation.

connection-map interface

```
connection-map interface
 serial (<0>/<9-16>)
```

no connection-map

```
no connection-map
```

Parameters

Parameter	Type	Description
<0>/<9-16>	Integer	Enter a slot number / port number for serial interface.

Mode

Serial Profile Mode (Raw)

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# connection-map interface serial 0/9

iS5comm(raw-p1)# no connection-map

13.8. data-bits

To determine the number of bits for the port to operate with, use the **data-bits** command in Interface Configuration Mode.

data-bits

```
data-bits
 <integer (7-8)>
```

Parameters

Parameter	Type	Description
integer (7-8)	Integer	Enter a number of bits for the port to operate with. The default is 8. Binary data is typically transmitted as eight bits, and text-based data is transmitted as seven bits or eight bits. If the data is based on the ASCII character set, then a minimum of seven bits is required because there are 27 or 128 distinct characters. If an eighth bit is used, it must have a value of

Mode

Serial Interface Configuration Mode

Examples

iS5comm(config)# configure terminal

iS5comm(config-serial-if)# data-bits 7

iS5comm(config-serial-if)# data-bits 8

13.9. debug serial

To the debug traces for the serial line module, use the **debug serial** command Global Configuration Mode.

There are several severity available:

- Critical level enables all the failure traces.
- Info level enables all traces related to information to end user.
- Trace level helps the software team to see the code flow.
- Data level includes info and critical level debugs.

debug serial

```
debug serial
 {all | |trace | data |info |critical none}
```

Parameters

Parameter	Type	Description
all		Enter to enable debugging for all severity levels available.
trace		Enter to enable debugging for trace level debugging.
data		Enter to enable debugging for data level debugging.
info		Enter to enable debugging for info level debugging.
critical		Enter to enable debugging for critical level debugging.
none		Enter to disable debugging.

Mode

Global Execution Mode

Examples

iS5comm# debug serial critical

```
    [SER_IP_DBG] : DBG Critical 2
```

iS5comm# debug serial none

```
    [SER_IP_DBG] : nmhSetSerialIpDebug() i4SetValSerialIpDebug 0
```

iS5comm#

13.10. description

To assign a name to a serial interface, use the **description** command in Serial Interface Configuration Mode.

description

```
description
 <string(127)>
```

no description

Parameters

Parameter	Type	Description
`string (127)`		Enter a description of the interface.

Mode

Serial Interface Configuration Mode

Examples

iS5comm(config)# configure terminal

iS5comm(config)# interface serial 0/9

iS5comm(config-serial-if)# description AB_interface

13.11. direction

To define the direction for a serial protocol, use the **direction** command in Transport Protocol Mode. There are IN, OUT, and IN-OUT directions. When the device acts as a server, IN direction is configured. The device acts as a client in OUT direction, and as both server and client in IN-OUT direction. For UDP transport protocol, the default direction is IN-OUT.

direction

```
direction
 {in | out | in-out}
```

Parameters

Parameter	Type	Description
`in`		Enter for IN direction for server mode.
`out`		Enter for OUT direction for client mode
`in-out`		Enter for IN-OUT direction for TCP connection.

Mode

Transport Protocol Mode

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol tcp

iS5comm(serial-p1-TCP)# direction in

iS5comm(raw-p1-TCP-in)# end

iS5comm# configure terminal

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol tcp

iS5comm(raw-p1-TCP)# direction out

iS5comm(raw-p1-TCP-Out)# end

iS5comm# configure terminal

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol tcp

iS5comm(raw-p1-TCP!)# direction in-out

iS5comm(raw-p1-TCP-InOut)# end

NOTE: There is no need to configure direction for UDP connection. In a case of UDP connection, the default direction is IN-OUT, and the software assigns it without need for configuration by the user.

13.12. DSCP

To define the Differentiated service code point (DSCP) which is set in the IP header for the outgoing packets, use the **DSCP** command in Role Mode (Modbus Client).

DSCP

```
DSCP
 <integer(0-63)>
```

no DSCP

```
no DSCP
```

Parameters

Parameter	Type	Description
<integer(0-63)>	Integer	Enter a decimal value for the Differentiated service code point (DSCP). The default is OFF.

Mode

Role Mode (Modbus Client)

Examples

iS5comm(config)# serial connection-type modbus profile m1

iS5comm(modbus-m1)# role client

iS5comm(modbus-m1-client)# DSCP 44

iS5comm(modbus-p1-client)# no DSCP

NOTE: As per RFC5865, DSCP with decimal value f 44 stands for VOICE-ADMIT. Refer to https://www.iana.org/assignments/dscp-registry/dscp-registry.xhtml

13.13. dynamic idle-timeout

To configure the time delay for auto disconnection, use the **dynamic idle-timeout** command in Serial Profile Mode (Preemptive). In case of no activity for the specified period of time, the socket will be disconnected automatically.

dynamic idle-timeout

```
dynamic idle-timeout
 <integer(10-3600)>
```

no dynamic idle-timeout

```
no dynamic idle-timeout
```

Parameters

Parameter	Type	Description
<integer(10-3600)>	Integer	Enter a number for idle time. The default is 10 seconds.

Mode

Serial Profile Mode (Preemptive)

Examples

iS5comm(config)# serial connection-type preemptive-raw profile p2

iS5comm(preemptive-p2)# dynamic idle-timeout 45

iS5comm(preemptive-p2)# no dynamic idle-timeout

13.14. dynamic packet timeout

To configure the time delay for auto disconnection of the dynamic client, use the **dynamic packet timeout** command in Serial Profile Mode (Preemptive). A dynamic client denotes a temporary client that connects to the preemptive raw profile.

dynamic packet timeout

```
dynamic packet timeout
 <integer(0-10000)>
```

no dynamic packet timeout

```
no dynamic packet timeout
```

Prerequisites

To set the dynamic packet timeout in Serial Profile Mode (Preemptive), the dynamic packet character trigger should be off.

```
iS5comm(preempt-p2)# dynamic packet char off
```

Parameters

Parameter	Type	Description
<integer(0-10000)>	Integer	Enter a number for dynamic packet timeout. The default is 10 milliseconds.

Mode

Serial Profile Mode (Preemptive)

Examples

iS5comm(config)# serial connection-type preemptive-raw profile p2

iS5comm(preemptive-p2)# dynamic packet char off

iS5comm(preemptive-p2)# dynamic packet timeout 100

iS5comm(preemptive-p2)# no dynamic packet timeout

iS5comm(preemptive-p2)# packetizing enable

13.15. dynamic packet char

To demarcate the packets sent out of a dynamic client, use the **dynamic packet char** command in Serial Profile Mode (Preemptive). A dynamic client denotes a temporary client that connects to the preemptive raw profile.

dynamic packet char

```
dynamic packet char
 (off | <integer(0 - 255)>)
```

Prerequisites

To set the dynamic packet character, the dynamic packet timeout command has to be disabled.

```
iS5comm(preemptive-p2)# packetizing enable
iS5comm(preemptive-p2)# dynamic packet timeout 0
```

Parameters

Parameter	Type	Description
`off`		Enter to disable the dynamic packet char command. By default, the dynamic character trigger is OFF.
`<integer(0 - 255)>`	Integer	Enter a number for the dynamic packet character. Its range is between 0 and 255.

Mode

Serial Profile Mode (Preemptive)

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type preemptive-raw profile p2

iS5comm(preemptive-p2)# packetizing enable

iS5comm(preemptive-p2)# dynamic packet timeout 0

iS5comm(preemptive-p2)# dynamic packet char 39

13.16. flow-control

To enable or disable hardware and software flow control, use the **flow-control** command in Serial Interface Configuration Mode. Flow control provides extra signaling to inform the transmitter that it should stop (pause) or start (resume) the transmission.

There is a hardware and software flow control.

For RS-232, the hardware method uses the RTS / CTS outputs. If the transmitter is ready to send data, then it sets the signal on the RTS line. If the receiver is ready to receive data, it sets the signal on the CTS line. If one of the signals is not set, no data transfer will occur.

The software method uses the Xon and Xoff characters (in the ASCII characters set: Xon = 17, Xoff = 19) which are transmitted using the same TXD / RXD communication lines as the main data instead of the pins. If the data cannot be received, the receiver transmits the Xoff symbol. To resume data transmission, the Xon symbol is sent.

flow-control

```
flow-control
 {hardware | none | software}
```

Parameters

Parameter	Type	Description
`hardware`		Enter this option to enable hardware flow control.
`none`		Enter this option for no flow control.
`software`		Enter this option to enable software flow control.

Mode

Serial Interface Configuration Mode

Examples

iS5comm(config)# configure terminal

iS5comm(config)# interface serial 0/9

iS5comm(config-serial-if)# flow-control hardware

iS5comm(config-serial-if)# flow-control software

iS5comm(config-serial-if)# flow-control none

13.17. force half-duplex

To enable or disable half duplex mode of operation, use the **force half-duplex** command in Serial Interface Configuration Mode. While sending data out of the serial port, all received data is ignored. This mode of operation is available only on ports that operate in full duplex mode.

force half-duplex

```
force half-duplex
 {on | off}
```

Parameters

Parameter	Type	Description
on		Enter this option to enable half duplex mode. Half duplex is to be used while the interface is either transmit ting or receiving, while in full duplex mode, data can be received and transmitted simultaneously.
off		Enter this option to disable half duplex mode. This is default.

Mode

Serial Interface Configuration Mode

Examples

iS5comm(config)# configure terminal

iS5comm(config)# interface serial 0/1

iS5comm(config-serial-if)# force half-duplex on

iS5comm(config-serial-if)# force half-duplex off

13.18. forward-exception

To enable / disable forwarding TCP exception, use the **forward-exception** command in Role Mode.

forward-exception

```
MODBUS client
 forward-exception
 {enable | disable}
```

Parameters

Parameter	Type	Description
`enable`		Enter this option to enable forwarding TCP exception. Default is enabled which is numerically denoted as 1.
`disable`		Enter this option to disable forwarding TCP exception. The numerical notation for disabled is 0.

Mode

Role Mode (Modbus Client)

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type modbus profile m1

iS5comm(modbus-m1)# role client

iS5comm(modbus-m1-client)# forward-exception enable

13.19. hold-time

To define the maximum amount of time that the serial packet can be held in the queue before being sent to the serial line, use the **hold-time** command in Serial Interface Configuration Mode. Time is measured from the moment the packet is received from the IP Layer.

hold-time

```
hold-time
 <integer (0-15000)>
```

Parameters

Parameter	Type	Description
`integer (0-15000)`	Integer	Enter a value, in milliseconds, for the delay time after which UART start listening to Rx line. The default is 0 ms.

Mode

Serial Interface Configuration Mode

Examples

iS5comm(config)# configure terminal

iS5comm(config)# interface serial 0/9

iS5comm(config-serial-if)# hold-time 500

iS5comm(config-serial-if)# hold-time 0

13.20. interface serial

To help end users to select the serial interface in config mode, use the **interface serial** command Global Configuration Mode. They can make it administratively up and can configure all the serial parameters like baud rate, flow control, stop, parity, data bits, etc.

interface serial

```
interface serial
 <integer (<0>/<9-16>)>
```

Parameters

Parameter	Type	Description
`integer (<0>/<9-16>)`	Integer	Enter a number that represent a serial interface number which a range between 9 through 16 or 0.

Mode

Global Configuration Mode

Examples

iS5comm(config)# configure terminal

iS5comm(config)# interface serial 0/9

iS5comm(config-serial-if)# baud-rate 115200

iS5comm(config-serial-if)# force half-duplex on

iS5comm(config-serial-if)# hardware flow-control enable

iS5comm(config-serial-if)# hold-time 1234

iS5comm(config-serial-if)# post-tx delay 12

iS5comm(config-serial-if)# rx-to-tx delay 500

iS5comm(config-serial-if)# software flow-control enable

iS5comm(config-serial-if)# stop-bits 2

iS5comm(config-serial-if)# turnaround delay 300

iS5comm(config-serial-if)# parity even

iS5comm(config-serial-if)# end

iS5comm# show interfaces serial

```
    Interface name          : serial 9
    Admin status            : Up
    Interface baudrate      : 115200
    Interface stopbits      : 2
    HW Flow ctl             : Enabled
    SE Flow ctl             : Enabled
    IfForceHD               : Enabled
    IfParity                : Even
    IfDataBits              : 8
    IfTurnAroundDelay       : 300 secs
    IfHoldTime              : 1234 secs
    IfPostTxDelay           : 12 secs
    IfRxToTxDelay           : 500 secs
```

iS5comm(config)# configure terminal

iS5comm(config)# interface serial 0/9

iS5comm(config-serial-if)# shutdown

iS5comm(config-serial-if)# end

iS5comm# show interfaces serial

```
    Interface name          : serial 9
```

```
Admin status            : Down
Interface baudrate      : 115200
Interface stopbits      : 2HW
Flow ctl              : Enabled
SE Flow ctl             : Enabled
IfForceHD               : Enabled
IfParity                : Even
IfDataBits              : 8
IfTurnAroundDelay       : 300 secs
IfHoldTime              : 1234 secs
IfPostTxDelay           : 12 secs
IfRxToTxDelay           : 500 secs
```

13.21. keep-alive

To perform a TCP alive check time, use the **keep-alive** command in Direction Mode (Raw Socket) and Role Mode (Modbus). The time specifies how long the device will wait for a response to keep alive packets sent before terminating the TCP connection. If the remote host does not respond to the keep alive packet within the specified time, the device will force the existing TCP connection to close. This command is applicable for TCP connections and for raw as well as MODBUS modes.

keep-alive timeout

```
keep-alive timeout
 <integer(60-600)>
```

no keep-alive timeout

```
no keep-alive timeout
```

Parameters

Parameter	Type	Description
<integer(60-600)>	Integer	Enter a keep-alive timeout range in seconds. The default is 240 seconds.

Mode

Direction Mode (Raw Socket)

Role Mode (Modbus Server/Client)

Examples

iS5comm# configure terminal
iS5comm(config)# serial connection-type raw profile p1
iS5comm(raw-p1)# transport protocol tcp
iS5comm(raw-p1-TCP)# direction in
iS5comm(raw-p1-TCP-in)# keep-alive timeout 5

iS5comm# configure terminal
iS5comm(config)# serial connection-type raw profile p1
iS5comm(raw-p1)# transport protocol tcp
iS5comm(raw-p1-TCP)# direction in
iS5comm(raw-p1-TCP-in)# no keep-alive timeout

iS5comm# configure terminal
iS5comm(config)# serial connection-type modbus profile m1
iS5comm(modbus-m1)# role server
iS5comm(modbus-m1-server)# keep-alive timeout 70
iS5comm(modbus-m1-server)# no keep-alive timeout

iS5comm# configure terminal
iS5comm(config)# serial connection-type modbus profile m2
iS5comm(modbus-m2)# role client
iS5comm(modbus-m2-client)# keep-alive timeout 70
iS5comm(modbus-m1-client)# no keep-alive timeout

13.22. local client port

To the local client port when the device acts in a client mode both in Raw Socket and MODBUS connection types, use the **local client port** command Global Configuration Mode.

local client port

```
Raw socket:
 local client port <integer(15010-15110)>
 MODBUS Client:
```

```
local client port {modbus | <integer(15010-15110)>}
```

Parameters

Parameter	Type	Description
`modbus`		Enter to select Modbus. The TCP port number is 502. Software internally assigns 502 if an user configures Modbus as its port.
`integer (15010-15110)`		Enter a value for local client port ID. Port numbers range between 15010 to 15110.

Mode

Direction mode (Raw)

Role mode (Modbus Client)

Examples

S5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol tcp

iS5comm(raw-p1-TCP)# direction out

iS5comm(raw-p1-TCP-Out)# local client port 15010

iS5comm(raw-p1-TCP-Out)# remote ipv4 address 192.168.20.66 port 15023

iS5comm(raw-p1-TCP-Out)# !

iS5comm(raw-p1-TCP)# !

iS5comm(raw-p1)# connection-map interface serial 0/12

iS5comm(raw-p1)# end

iS5comm(config)# serial connection-type modbus profile m1

iS5comm(modbus-m1)# role client

iS5comm(modbus-m1-client)# local client port modbus

13.23. local server

To configure the local server port in use while listening for the incoming TCP or UDP connection, use the **local server** command in Direction Mode (Raw Socket) and Role Mode (Modbus). This command is also applicable to MODBUS server mode.

local server

```
Raw socket:
 local server
 port <integer(15010-15110)>

 MODBUS:
 local server
 port {modbus | <integer(15010-15110)> }
```

no local server port

```
no local server port
```

Parameters

Parameter	Type	Description
port		Enter for a port to listen.
<integer(15010-15110)>	Integer	Enter a port range. The range is between 15010 to 15110.
modbus		Enter for Modbus mode.

Mode

Direction Mode (Raw)

Role Mode (Modbus Server)

Examples

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol tcp

iS5comm(serial-p1-TCP)# direction in

iS5comm(raw-p1-TCP-in)# local server port 15010

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol tcp

iS5comm(serial-p1-TCP)# direction in

iS5comm(raw-p1-TCP-in)# no local server port

For MODBUS connection-type:

iS5iS5comm(config)# serial connection-type modbus profile m1

iS5comm(modbus-m1)# role server

iS5comm(modbus-m1-server)# local server port modbus

iS5comm(modbus-m1-server)# no local server port

13.24. loopback local

To enables loopback on a serial interface, use the command **loopback local** in Serial Interface Configuration Mode. The no form of this command disables the loopback on a physical interface.

loopback local

no loopback local

Mode

Serial Interface Configuration Mode

Examples

iS5comm(config)# configure terminal

iS5comm(config)# interface serial 0/9

iS5comm (config-serial-if)# loopback local

13.25. max client connections

To establish the maximum number of clients supported by MODBUS server, use the **max client connections** command in Role (server) Mode.

max client connections

```
max client connections
 <integer(1-64)>
```

no max client connections

```
no max client connections
```

Parameters

Parameter	Type	Description
<integer(1-64)>	Integer	Enter a maximum number of clients supported by MODBUS server. The default is 64.

Mode

Role Mode (Modbus Server)

Examples

iS5comm(config)# serial connection-type modbus profile m1

iS5comm(modbus-m1)# role server

iS5comm(modbus-m1-server)# max client connections 45

13.26. max connections

For configurations using TCP, to configure the maximum number of allowed incoming TCP connections, use the **max connections** command in Direction Mode. This is applicable when the device acts as a server (IN and IN-OUT direction).

max connections

```
max connections
 <integer(1-64)>
```

no max connection

```
no max connection
```

Parameters

Parameter	Type	Description
<integer(1-64)>	Integer	Enter a maximum number of allowed incoming TCP connections. The default is 1.

Mode

Direction Mode (Raw)

Examples

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol tcp

iS5comm(raw-p1-TCP)# direction in

iS5comm(raw-p1-TCP-in)# max connections 25

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol tcp

iS5comm(raw-p1-TCP)# direction in

iS5comm(raw-p1-TCP-in)# no max connections

13.27. max pending messages

For a maximum number of messages that Modbus server can handle from different clients, use the **max pending messages** command in Role Mode (Modbus server).

max pending messages

```
max pending messages
 <integer(0-16)>
```

no max pending messages

```
no max pending messages
```

Parameters

Parameter	Type	Description
<integer(0-16)>	Integer	Enter a maximum number of messages that Modbus server can handle from different clients. The default is 16.

Mode

Role Mode (Modbus server)

Examples

iS5comm(config)# serial connection-type modbus profile m20

iS5comm(modbus-m20)# role server

iS5comm(modbus-m20-server)# max pending messages 10

iS5comm(modbus-m20-server)# no max pending messages

13.28. max udp connections

To establish the maximum number of UDP host/client to connect with, use the **max udp connections** command in Transport Protocol UDP Mode.

max udp connections

```
max udp connections
 <integer(1-64)>
```

Parameters

Parameter	Type	Description
<integer(1-64)>	Integer	Enter a UDP connections with which the device can connect with. The default is 64.

Mode

Transport Protocol UDP Mode

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type raw profile udp

iS5comm(raw-udp)# transport protocol udp

S5comm(raw-udp-UDP)# max udp connections 55

iS5comm(raw-udp-UDP)# end

13.29. mtu

To configure the Maximum Transmission Unit (MTU) frame size for all frames transmitted and received on a serial interface, use the command **mtu** in Serial Interface Configuration Mode. The no form of this command sets the maximum transmission unit to the default value in all interfaces.

mtu

```
mtu <frame-size(46-9216)>
```

Parameters

Parameter	Type	Description
<frame-size (46-9216)>	Integer	Enter a size of the MTU frame. The value ranges from 46 to 9216 and defines the largest PDU that can be passed by the interface without any need for fragmentation. This value is shown to the higher interface sub-layer and should not include size of the encapsulation or header added by the interface. This value represents the IP MTU over the interface, if IP is operating over the interface. Default is 1500.

Mode

Serial Interface Configuration Mode

Examples

iS5comm (config-serial-if)# mtu 900

13.30. packet char

To demarcate the packets sent out of serial interface, use the **packet char** command in Direction Mode or Serial Profile Mode. A specified character by this command will trigger packetizing and force forward the accumulated serial data to the network. The character length may range between 0 - 255.

packet char

```
packet char
 (off | <integer(0 - 255)>)
```

Prerequisites

To set the packet character, packetizing has to be enabled and packet timeout has to be set as 0.

```
iS5comm(raw-p1-TCP-out)# packetizing enable
iS5comm(raw-p1-TCP-Out)# packet timeout 0
```

Parameters

Parameter	Type	Description
`off`		Enter to disable packet char command. By default, the character trigger is OFF.
`<integer(0 - 255)>`	Integer	Enter a value for a packet character. Its range is between 0 and 255.

Mode

Direction Mode (Raw)

Serial Profile Mode (Raw Preemptive)

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol tcp

iS5comm(raw-p1-TCP)# direction out

iS5comm(raw-p1-TCP-Out)# packetizing enable

iS5comm(raw-p1-TCP-Out)# packet char 240

% Make sure packet timeout is 0 for profile p1 and retry !

iS5comm(raw-p1-TCP-Out)# packet timeout 0

iS5comm(raw-p1-TCP-Out)# packet char 240

iS5comm(raw-p1-TCP-Out)# packet char off

iS5comm(raw-p1-TCP-Out)# ex

iS5comm(raw-p1-TCP)# direction in

iS5comm(raw-p1-TCP-in)# packetizing enable

iS5comm(raw-p1-TCP-in# packet char 240

iS5comm# configure terminal

iS5comm(config)# serial connection-type preemptive-raw profile p2

iS5comm(preempt-p2)# packetizing enable

iS5comm(preempt-p2)# packet timeout 0

iS5comm(preempt-p2)# packet char 39

iS5comm(preempt-p2)# end

13.31. packet size

For the server to packetize based on packet size, use the **packet size** command in Direction Mode or Serial Profile Mode. The server packetizes and forwards the packet when the number of bytes reaches the configured value.

packet size

```
packet size
 <integer(16 - 1400)>
```

no packet size

```
no packet size
```

Prerequisites

To set the packet size in Direction Mode (Raw), packetizing has to be enabled.

```
iS5comm(raw-p1-TCP-in)# packetizing enable
```

Parameters

Parameter	Type	Description
<integer(16 - 1400)>	Integer	Enter a value for packet size. The default value is 1400.

Mode

Direction Mode (Raw)

Serial Profile Mode (Raw Preemptive)

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol tcp

iS5comm(raw-p1-TCP)# direction in

iS5comm(raw-p1-TCP-in)# packet size 1340

iS5comm(raw-p1-TCP-in)# no packet size

iS5comm(config)# serial connection-type preemptive-raw profile p2

iS5comm(preempt-p2)# packetizing enable

iS5comm(preempt-p2)# packet size 19

iS5comm(preempt-p2)# no packet size

13.32. packet timeout

To define the delay between the packets sent from serial ports, use the **packet timeout** command in Direction Mode or Serial Profile Mode (Raw).

packet timeout

```
packet timeout
 <integer(0-1000)>
```

no packet timeout

```
no packet timeout
```

Prerequisites

To set the packet timeout in Direction Mode (Raw), packetizing has to be enabled and packet char should be off.

```
iS5comm(raw-p1-TCP-in)# packetizing enable
iS5comm(raw-p1-TCP-in)# packetizing char off
```

Parameters

Parameter	Type	Description
<integer(0-1000)>	Integer	Enter a timeout value in milliseconds. The default is 10 ms.

Mode

Direction Mode (Raw)

Serial Profile Mode (Raw Preemptive)

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol tcp

iS5comm(raw-p1-TCP)# direction in-out

iS5comm(raw-p1-TCP-InOut)# packetizing enable

```
    Error: Cannot set packet timer for profile  p1
    Check if packet char is off for profile p1 !
```

iS5comm(raw-p1-TCP-InOut)# packet char off

iS5comm(raw-p1-TCP-InOut)# packet timeout 500

iS5comm(preempt-p2)# packet char off

iS5comm(raw-p1-TCP-InOut)# end

iS5comm# configure terminal

iS5comm(config)# serial connection-type preemptive-raw profile p2

iS5comm(preempt-p2)# packetizing enable

iS5comm(preempt-p2)# packet timeout 600

iS5comm(preempt-p2)# end

iS5comm# configure terminal

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol tcp

iS5comm(raw-p1-TCP)# direction in-out

iS5comm(raw-p1-TCP-InOut)# no packet timeout

iS5comm(raw-p1-TCP-InOut)# end

iS5comm# configure terminal

iS5comm(config)# serial connection-type preemptive-raw profile p2

iS5comm(preempt-p2)# packetizing enable

iS5comm(preempt-p2)# no packet timeout

iS5comm(preempt-p2)# end

13.33. packetizing

For enable or disable packetizing, use the **packetizing** command in Direction Mode. Packetizing is a feature of Raw Socket which uses the TCP as its transport protocol. Only if this is enabled, the packet timer, packet size, and packet char can be set.

packetizing

```
packetizing
 {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enter this option to enable packetizing.
disable		Enter this option to disable packetizing.This is the default option.

Mode

Direction Mode (Raw)

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol tcp

iS5comm(raw-p1-TCP)# direction in

iS5comm(raw-p1-TCP-in)# packetizing enable

iS5comm(raw-p1-TCP-in)# packetizing disable

13.34. parity

To detect errors in transmission, use the **parity** command in Serial Interface Configuration Mode. When parity is used with a serial port, an extra data bit is sent with each data character and is arranged so that the number of 1 bits in each character, including the parity bit, is always odd or always even. If a byte is received with the wrong number of 1s, then, it must have been corrupted. However, an even number of errors can pass the parity check.

parity

```
parity
 {none | even | odd}
```

Parameters

Parameter	Type	Description
none		Enter this option for no error checking mechanism. This is default.
even		Enter this option for the number of 1's in the data plus parity to be an even number.
odd		Enter this option for the number of 1's in the data plus parity to be an odd number.

Mode

Serial Interface Configuration Mode

Examples

iS5comm(config)# configure terminal

iS5comm(config)# interface serial 0/1

iS5comm(config-serial-if)# parity even

iS5comm(config-serial-if)# parity odd

iS5comm(config-serial-if)# parity none

13.35. permanent-client

To configure the permanent client for preemptive mode, use the **permanent-client** command in Serial Profile Mode (Preemptive Raw).

In Preemptive mode, the device acts as a server and can support maximum of two clients (one can be active at any point of time). One is a permanent client (permanent master), and another is a dynamic client or dynamic master. The dynamic client can preempt the existing permanent client connection and can start data transfer with the device (acting as a server). After a certain period of idle time, the connection with the dynamic client is discontinued, and the permanent client resumes control.

permanent-client

```
permanent-client
 ipv4 address <IpAddress>
```

no permanent-client

```
no permanent-client
```

Parameters

Parameter	Type	Description
`ipv4 address`		Enter to specify unicast IP address to be defined.
`<IpAddress>`	A.B.C.D	Enter the unicast IP address of the client which is connected to the server permanently.

Mode

Serial Profile Mode (Preemptive Raw)

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type preemptive-raw profile p2

iS5comm(preempt-p2)# permanent-client ipv4 address 192.168.20.66

iS5comm(preempt-p2)# no permanent-client

13.36. post-tx delay

To define the delay after transmitting a packet, use the **post-tx delay** command in Serial Interface Configuration Mode. This is the dead time after transmitting a packet.

post-tx delay

```
post-tx delay
 <integer (0-15)>
```

Parameters

Parameter	Type	Description
`integer (0-15)`	Integer	Enter a value (in seconds) for the delay after transmitting a packet.

Mode

Serial Interface Configuration Mode

Examples

iS5comm(config)# configure terminal

iS5comm(config)# interface serial 0/9

iS5comm(config-serial-if)# post-tx delay 12

13.37. re-connect timeout

For configurations enabling the device to perform reconnection attempts, use the **re-connect timeout** command in Direction Mode (Raw Socket) or Role Mode (Modbus Client). This is applicable when the device acts as a client attempting to connect an external server. This configuration also applies to a MODBUS client as well.

re-connect timeout

```
re-connect timeout
 <integer(60-300)>
```

no re-connect timeout

```
no re-connect timeout
```

Parameters

Parameter	Type	Description
<integer(60-300)>	Integer	Enter a maximum time for attempting to connect to an external server. The range is between 60 to 300 seconds, with a default of 120 seconds.

Mode

Direction Mode (Raw Socket)

Role Mode (Modbus Client)

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type raw profile p2

iS5comm(raw-p2)# transport protocol tcp

iS5comm(raw-p2-TCP)# direction out

iS5comm(raw-p2-TCP-Out)# re-connect timeout 299

iS5comm# configure terminal

iS5comm(config)# serial connection-type raw profile p2

iS5comm(raw-p2)# transport protocol tcp

iS5comm(raw-p2-TCP)# direction out

iS5comm(raw-p2-TCP-Out)# no re-connect timeout

Modbus client

iS5comm(config)# serial connection-type modbus profile m1

iS5comm(modbus-m1)# role client

iS5comm(modbus-m1-client)# re-connect timeout 75

iS5comm(modbus-m1-client)# no re-connect timeout

13.38. remote ipv4 address

To configure the remote IP and port for the device to communicate as a client, use the **remote ipv4 address** command in Direction Mode. The port “modbus” comes into picture for configuring Modbus.

remote ipv4 address

```
Raw socket:
 remote ipv4 address <IpAddress> port <integer(1-65535)>
 MODBUS:
 remote ipv4 address
 <IpAddress> port {modbus | <integer(1-65535)>
```

no remote ipv4 address port

```
no remote ipv4 address port
```

Parameters

Parameter	Type	Description
`<IpAddress>`	A.B.C.D	Enter an Unicast IPv4 address.
`port`		Enter for a port to listen.
`<integer(1-65535)>`	Integer	Enter a number in the port range. The range is between 1-65535.
`modbus`		Enter for Modbus. The TCP port number for Modbus is 502. Software internally assigns 502 if user configures Modbus.

Mode

Direction Mode (Raw Socket)

Role Mode (Modbus client)

Examples

iS5comm(config)# serial connection-type raw profile p1

S5comm(raw-p1)# transport protocol tcp

iS5comm(raw-p1-TCP)# direction out

iS5comm(raw-p1-TCP-out)# remote ipv4 address 192.168.20.66 port 650

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol tcp

iS5comm(raw-p1-TCP)# direction out

iS5comm(raw-p1-TCP-out)# no remote ipv4 address port

iS5comm# configure terminal

iS5comm(config)# serial connection-type modbus profile m1

iS5comm(modbus-m1)# role client

iS5comm(modbus-m1-client)# remote ipv4 address 192.168.20.66 port modbus

13.39. remove slave-id

To delete the MODBUS profile identification (its slave-id), use the **remove slave-id** command in Role Mode.

remove slave-id

```
MODBUS server
 remove slave-id
 <ids> interface serial <interface-id>

 MODBUS client
 remove slave-id
 <ids>
```

Parameters

Parameter	Type	Description
`ids (1-247)`	Integer	Enter a value for the slave ID. The format is comma separated integer values with a maximum of 10 slave IDs per command.
`interface serial`		Enter this option for the interface to be defined.
`interface-id (<0>/<9-16>)`	Integer	Enter a value for the interface ID range. The serial interface ranges between 0/9-16. **NOTE:** Interface mapping is applicable only to server.

Mode

Role Mode (Server /Client)

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type modbus profile m1

iS5comm(modbus-m1)# role server

iS5comm(modbus-m1-server)# add slave-id 1,2,3,4,5,6,7,8,9,10 interface serial 0/9

iS5comm(modbus-m1-server)# remove slave-id 1,2,3,4,5,6,7,8,9,10 interface serial 0/9

iS5comm(modbus-m1-server)# exit

iS5comm(modbus-m1)# role client

iS5comm(modbus-m1-client)# remove slave-id

iS5comm(modbus-m1)# exit

13.40. remove udp-host

To remove an UDP remote host from the raw socket profile, use the **remove udp-host** command in Transport Protocol UDP Mode. By this command we can restrict the device to allow data transfer to only selected remote host / clients.

remove udp-host

```
remove udp-host
 {<IpAddress> port <integer(1-65535)>
```

Parameters

Parameter	Type	Description
<IpAddress>	A.B.C.D	Unicast IP address of the remote host.
port		Enter for a port of the UDP remote host.
<integer(1-65535)>		Enter a port number of the remote host.

Mode

Transport Protocol UDP Mode

Examples

iS5comm(config)# serial connection-type raw profile udp

iS5comm(raw-udp)# transport protocol udp

iS5comm(raw-udp-UDP)# remove udp-host 192.168.20.66 port 35478

iS5comm(raw-udp-UDP)# end

13.41. response-timeout

To define the response time of a serial port, use the **response-timeout** command in Role Mode (Modbus).

Response time is the time to wait for a response from a serial port.

Same as for slave IDs, response time configuration is bound to:

- an interface for MODBUS servers, or
- a profile for MODBUS clients

response-timeout

```
MODBUS server
 response-timeout
 <integer(50-10000)> interface serial <interface-id>
 no response-timeout
 <ids> interface serial <interface-id>

 MODBUS client
 response-timeout
 <integer(50-10000)>
 no response-timeout
```

Parameters

Parameter	Type	Description
`<integer(50-10000)>`	Integer	Enter a value for the response timeout in milliseconds. The default is 2000 ms.
`interface serial`		Enter this option for the interface to be defined.
`<interface-id (0/9-16)>`	Integer	Enter a value for the interface id range. The serial interface range is between 0/9-16. **NOTE:** Interface mapping is applicable only to server.

Mode

Role Mode (Modbus Server / Client)

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type modbus profile m1

iS5comm(modbus-m1)# role server

iS5comm(modbus-m1-server)# response-timeout 50 interface serial 0/9

iS5comm(modbus-m1-server)# exit

iS5comm(modbus-m1)# role client

iS5comm(modbus-m1-client)# response-timeout 300

13.42. role

To define the MODBUS profile to act either as a server or a client, use the **role** command in Profile Mode.

role

```
role
 {server | client}
```

Parameters

Parameter	Type	Description
server		Enter this option for the MODBUS profile to act as a server.
client		Enter this option for the MODBUS profile to act as a client.

Mode

Serial Profile Mode (Server / Client)

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type modbus profile m1

iS5comm(modbus-m1)# role server

iS5comm(modbus-m1-server)# exit

iS5comm(modbus-m1)# role client

iS5comm(modbus-m1-client)# exit

13.43. rx-to-tx delay

To define the delay between Receive mode and Transmit mode, use the **rx-to-tx delay** command in Serial Interface Configuration Mode.

rx-to-tx delay

```
rx-to-tx delay
 <integer (0-1000)>
```

Parameters

Parameter	Type	Description
integer (0-1000)	Integer	Enter a value for request to transmit delay (in seconds).

Mode

Serial Interface Configuration Mode

Examples

iS5comm(config)# configure terminal

iS5comm(config)# interface serial 0/9

iS5comm(config-serial-if)# rx-to-tx delay 500

13.44. serial connection-type

To define a profile name and its connection type, use the **serial connection-type** command in Global Configuration Mode. There are three modes available: raw, raw-preemptive, and Modbus. The profile is created by this command and is not activated until a serial interface is mapped to it.

serial connection-type

```
serial connection-type
 {raw | preemptive-raw | modbus} profile <string(64)>
```

no serial profile

```
no serial profile <string(64)>
```

Parameters

Parameter	Type	Description
raw		Enter for raw mode. User can configure a simple raw mode for TCP or UDP communication.
raw-preemptive		Enter for preemptive mode. The device acts as a server in preemptive mode. In this mode, direction and protocol are implicitly set as IN and TCP. Any dynamic client can preempt the permanent client and start communicating with the device for specified period of time
modbus		Enter for Modbus mode.
profile		Enter for profile name definition.
<string(64)>	string	Enter a string for an user defined profile name

Mode

Global Configuration Mode

Examples

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# exit

iS5comm(config)# serial connection-type preemptive-raw profile p2

iS5comm(preempt-p2)# exit

iS5comm(config)# serial connection-type modbus profile p3

iS5comm(modbus-p3)# exit

iS5comm(config)# no serial profile profile1

iS5comm(config)# no serial profile profile2

iS5comm(config)# no serialprofile profile3

13.45. show interfaces serial

To display the serial profile configuration, use the command **show interfaces serial** in Privileged EXEC Mode.

show interfaces serial

```
show interfaces serial
```

```
<interface-id> <0>/<9-16>
```

Parameters

Parameter	Type	Description
`interface serial`		Enter to display the serial interface details.
`<interface-id>`		Enter to display a specific slot number / port number. The format is <0>/<9-16> without spaces between Slot Number/Port Number. For example, 0/9.

Mode

Privileged EXEC Mode

Examples

iS5comm# show interfaces serial 0/9

```
    Interface name          : serial 0/9
    Admin status            : Up
    Baudrate                : 9600
    Data bits               : 8
    Parity                  : Even
    Stop bits               : 2
    Flow control            : None
    Interface type          : rs232
    Termination resistor    : Disabled
    Force HD                : Enabled
    Turn around delay       : 0 secs
    Hold time               : 0 secs
    Post Tx delay           : 12 secs
    Rx to Tx delay          : 500 secs
```

13.46. show serial profile

To display the serial profile configuration and display both the active and inactive profiles, use the command **show serial profile** in Privileged EXEC Mode.

show serial profile

```
show serial profile
```

```
 {all | active | inactive | name <string(64)> | interface serial <inter-
face-id> <0>/<9-16>}
```

Parameters

Parameter	Type	Description
all		Enter to display all profiles no matter active or inactive.
active		Enter to display all active profiles. Active profiles are the these with a serial interface mapped to them.
inactive		Enter to display all inactive profiles. Inactive profiles are the these with no serial interface mapped to them.
name		Enter to display a profile by its name.
string(64)		Enter the name of the profile to be displayed.
interface serial		Enter to display a profile based on a serial interface.
<interface-id>		Enter to display a profile by specific slot number / port number. The format is <0>/<9-16> without spaces between Slot Number/Port Number. For example, 0/9.

Mode

Privileged EXEC Mode

Examples

iS5comm# show serial profile all

```
    Profile                 : p1
    Status                  : Inactive
     Packet size             : 1400
     Buffering               : Disabled Packetizing             : Disabled
     Max connection          : 64
     TCP keep alive seconds  : 240

     Profile                 : m1
     Status                  : Inactive
     Role                    : Server
     Local client port       : 502
     Keep-alive seconds      : 240
     Max connections         : 64
```

```
Max TCP pending messages: 16
Send exception          : Enabled
```

iS5comm# show serial profile active

```
Profile                 : p1
Status                  : Active
Serial interface        : 10
Protocol                : RAW Socket
Mode                    : Server
Direction               : In
Transport               : TCP
Local Server IP         : 192.168.20.2
Local Server Port       : 15010
Number of clients       : 0
Serial RX byte counter  : 0
Serial TX byte counter  : 0
KeepAlive interval (sec): 240
Dynamic master enabled  : disabled
Max connections         : 64
Packetizing             : OFF
TCP buffering           : disabled
Turnaround delay(msec)  : 0
Hold time(msec)         : 0
Rx-to-Tx delay(msec)    : 0

Profile                 : p2
Status                  : Active
Serial interface        : 11
Protocol                : RAW Socket
Mode                    : Client
Direction               : Out
Transport               : TCP
Remote Server IP        : 192.168.20.66
Remote Server Port      : 15020
Serial RX byte counter  : 0
Serial TX byte counter  : 0
TCP RX byte counter     : 0
TCP TX byte counter     : 0
Connection to server    : YES
Local Client Port       : 15021
```

```
KeepAlive interval (sec): 240
Reconnect timer(sec)    : 120
Packetizing             : OFF
TCP buffering           : disabled
Turnaround delay(msec)  : 0
Hold time(msec)         : 0
Rx-to-Tx delay(msec)    : 0
```

iS5comm# show serial profile interface serial 0/9

```
Profile                 : p3
Status                  : Active
Serial interface        : 9
Protocol                : RAW Socket
Transport               : UDP
Max connections         : 64
Remote connections      : 2
Remote Ip    1          : 192.168.20.66
Remote Port  1          : 15031
Remote Udp   1 RX cnt   : 0
Remote Udp   1 TX cnt   : 4
Remote Ip    2          : 192.168.20.66
Remote Port  2          : 49777
Remote Udp   2 RX cnt   : 6
Remote Udp   2 TX cnt   : 4
Local IP                : 192.168.20.2
Local Port              : 15030
Serial RX byte counter  : 4
Serial TX byte counter  : 6
Pack size               : 1400
Pack timer(msec)        : 10
Pack char               : disabled
Turnaround delay(msec)  : 0
Hold time(msec)         : 0
Rx-to-Tx delay(msec)    : 0
```

13.47. shutdown

To disable a serial interface, use the command **shutdown** in Serial Interface Configuration Mode. The no form of the command enables the interface.

shutdown

no shutdown

Mode

Serial Interface Configuration Mode

Examples

iS5comm(config-serial-if)# shutdown

13.48. stop-bits

To signal the end of a serial frame or packet, use the **stop-bits** command in Interface Configuration Mode. The stop bit is used to signal the completion of the message transmission.

stop-bits

```
stop-bits
 <integer (1-2)>
```

no stop-bits

```
no stop-bits
```

Parameters

Parameter	Type	Description
integer (1-2)	Integer	Enter a value from the range. The default is 1. Choose 1 stop bit if parity is used or 2 stop bits with no parity.

Mode

Serial Interface Configuration Mode

Examples

iS5comm(config)# configure terminal

iS5comm(config)# interface serial 0/1

iS5comm(config-serial-if)# stop-bits 1

iS5comm(config-serial-if)# no stop-bits

NOTE: “no stop-bits” will revert the stop bits settings to default value which is 1.

13.49. tcp buffering

To buffer data, use the **tcp buffering** command in Direction Mode (Raw) and Profile Mode (Preemptive-Raw). TCP buffering is similar to TCP_NODELAY. If this feature is set, it follows Nagle algorithm, and data is buffered until there is a sufficient amount to be send out, thereby avoiding frequent sending of small packets, which results in poor utilization of the network. If this feature is not set, the segments are always sent as soon as possible, even if there is only a small amount of data.

tcp buffering

```
tcp buffering
 {enable | disable}
```

Parameters

Parameter	Type	Description
`enable`		Enter this option to enable TCP buffering.
`disable`		Enter this option to disable TCP buffering. This is the default option.

Mode

Direction Mode (Raw)

Serial Profile Mode (Preemptive Raw)

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol tcp

iS5comm(raw-p1-TCP)# direction in

iS5comm(raw-p1-TCP-in)# tcp buffering enable

iS5comm(raw-p1-TCP-in)# tcp buffering disable

iS5comm# configure terminal

iS5comm(config)# serial connection-type preemptive-raw profile p2

iS5comm(preempt-p2)# tcp buffering disable

iS5comm(preempt-p2)# tcp buffering enable

13.50. transmit-exception

To enable / disable sending TCP exception back to the master if a response has not been received from RTU within the expected time, use the **transmit-exception** command in Role Mode.

transmit-exception

```
MODBUS server
 transmit-exception
 {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enter this option to enable sending TCP exception back to the master. Default is “Enable” which is numerically denoted as 1.
disable		Enter this option to disable sending TCP exception back to the master. The numerical notation for disable is 0.

Mode

Role Mode (Modbus Server)

Examples

iS5comm# configure terminal

iS5comm(config)# serial connection-type modbus profile m1

iS5comm(modbus-m1)# role server

iS5comm(modbus-m1-server)# transmit-exception enable

13.51. transport protocol

To configure the transport protocol to be used for Raw Socket communication, use the **transport protocol** command in Serial Profile Mode (Raw Socket). The transport protocol can be either TCP or UDP.

transport protocol

```
transport protocol
```

```
{tcp | udp}
```

Parameters

Parameter	Type	Description
tcp		Enter for Transmission Control Protocol.
udp		Enter for User Datagram Protocol.

Mode

Serial Profile Mode (Raw Socket)

Examples

iS5comm(config)# serial connection-type raw profile p1

iS5comm(raw-p1)# transport protocol

SERIAL_TRANSPORT commands :

transport protocol { tcp | udp }

iS5comm(raw-p1)# transport protocol tcp

iS5comm(serial-p1-TCP)# !

iS5comm(raw-p1)# transport protocol udp

iS5comm(raw-p1-UDP)#

13.52. turnaround delay

To define the delay between individual messages, use the **turnaround delay** command in Serial Interface Configuration Mode. This is the amount of delay inserted between the transmission of individual messages on a serial port. It represents the delay between sending a message and the next poll out of the serial port. Some devices does not respond to specific message like broadcast; in that case, enough time must be ensured for processing.

turnaround delay

```
turnaround delay
 <integer (0-1000)>
```

Parameters

Parameter	Type	Description
`integer (0-1000)`	Integer	Enter a value for the delay between individual messages. The default is 0 ms.

Mode

Serial Interface Configuration Mode

Examples

iS5comm(config)# configure terminal

iS5comm(config)# interface serial 0/1

iS5comm(config-serial-if)# turnaround delay 100

iS5comm(config-serial-if)# turnaround delay 0

TCP

14. TCP

Transmission Control Protocol (TCP) is a portable implementation of the industry standard TCP based on RFC 793. The software consists of the core TCP protocol, a library that provides a Socket Layer Interface (SLI) to support both a Telnet Server and FTP server. TCP interacts with the Network Layer protocols (IPv4/IPv6) and uses their services for end-to-end communication.

14.1. tcp max retries

To configure the maximum number of retries for re-transmission in TCP module, use the command **tcp max retries** in Global Configuration Mode.

tcp

```
tcp max retries <number retries (1-12>
```

Parameters

Parameter	Type	Description
`max`		Enter to configure the maximum number of retries for re-transmission in TCP module.
`retries`		Enter to configure the maximum number of retries for re-transmission in TCP module.
`<number retries (1-12>`	Integer	Enter a number for maximum retries. The value ranges from 1 to 12.

Mode

Global Configuration Mode

Examples

iS5comm(config)# tcp max retries 1

14.2. show tcp

To display the TCP connections, the information about all listeners, the TCP statistics information, and TCP retransmission details, use the command **show tcp** in Privileged EXEC Mode.

show tcp

```
show tcp {connections | listeners | retransmission details | statistics}
```

Parameters

Parameter	Type	Description
connections		Enter to display the TCP connections for the switch such as Local IP Address type, Local IP, Local Port and Remote Port. It also displays if a connection is TCP MD5 protected and the number of incoming segments that failed MD5 authentication.
listeners		Enter to display the information such as Local IP Address Type, Local IP and Local Port for each listener in the network.
retransmission		Enter to set the Retransmission related configuration.
details		Enter to display the TCP retransmission details.
statistics		Enter to display the TCP statistics information such as “Max Connections”, “Active Opens”, “Passive Opens”, “Attempts Fail”, etc.

Mode

Privileged EXEC Mode

Examples

iS5comm# show tcp connections

```
     Context Name : default


    TCP Connections
    ===============
    Local IP Address Type  : IPv4
    Local IP               : 0.0.0.0
    Local Port             : 22
    Remote IP Address Type : IPv4
    Remote IP              : 0.0.0.0
```

```
Remote Port            : 0
TCP State              : Listen
MD5 Authenticated      : No
TCP-AO Authenticated   : No

TCP Connections
 ===============

Local IP Address Type  : IPv4
Local IP               : 0.0.0.0
Local Port             : 80
Remote IP Address Type : IPv4
Remote IP              : 0.0.0.0
Remote Port            : 0
TCP State              : Listen
MD5 Authenticated      : No
TCP-AO Authenticated   : No

TCP Connections
 ===============
Local IP Address Type  : IPv4
Local IP               : 0.0.0.0
Local Port             : 443
Remote IP Address Type : IPv4
Remote IP              : 0.0.0.0
Remote Port            : 0
TCP State              : Listen
MD5 Authenticated      : No
TCP-AO Authenticated   : No

TCP Connections
===============

Local IP Address Type  : IPv4
Local IP               : 192.168.10.1
Local Port             : 22
Remote IP Address Type : IPv4
Remote IP              : 192.168.10.10
Remote Port            : 63370
```

```
    TCP State              : Established
    MD5 Authenticated      : No
    TCP-AO Authenticated   : No
```

iS5comm# show tcp listeners

```
    TCP Listeners
    ===============
    Context Name : default
     --------------
    Local IP Address Type  : IPv4
    Local IP               : 0.0.0.0
    Local Port             : 22

    Local IP Address Type  : IPv4
    Local IP               : 0.0.0.0
    Local Port             : 80

    Local IP Address Type  : IPv4
    Local IP               : 0.0.0.0
    Local Port             : 443

    Address Type [0 - IPv4 and IPv6] [1 - IPv4] [2 - IPv6]
```

iS5comm(config)# show tcp retransmission details

```
     Context Name : default

    RTO Algorithm Used : VAN JACOBSON
    Min Retransmission Timeout : 50 msec
    Max Retransmission Timeout : 2000 msec
```

iS5comm# show tcp statistics

```
     Context Name : default

    Max Connections : 500
    Active Opens : 0
    Passive Opens : 387
    Attempts Fail : 0
    Estab Resets : 3
    Current Estab : 1
    Input Segments : 44096
    Output Segments : 69643
```

```
Retransmitted Segments : 29
Input Errors : 2
TCP Segments with RST flag Set: 0
HC Input Segments : 44096
HC Output Segments : 69643
```

UDP

15. UDP

UDP (User Datagram Protocol) is a portable implementation of the industry standard UDP. It is used in packet-switched computer communication networks and in interconnected systems of such networks.

The software consists of the core UDP protocol and a library that provides a Socket Layer Interface (similarly to BSD sockets) for applications like SNMP. It supports a number of standard features in addition to the core protocol.

15.1. show udp

To display the UDP configuration or statistics, use the command **show udp** in Privileged EXEC Mode.

show udp

```
show udp {connections | statistics}
```

Parameters

Parameter	Type	Description
`connections`		Enter to display the UDP configuration such as Local IP Address Type, Local IP, Local Port, Remote IP Address Type, Remote IP and Remote Port for various connections.
`statistics`		Enter to display the UDP statistics such as InDatagrams, outDatagrams, HC InDatagrams, HC OutDatagrams, UDP No Ports and UDP IN Errors.

Mode

Privileged EXEC Mode

Examples

iS5comm# show udp connections

```
    Global UDP Connections
    ======================
```

```
Local IP Address Type  : IPv4
Local IP               : 0.0.0.0
Local Port             : 68
Remote IP Address Type : IPv4
Remote IP              : 0.0.0.0
Remote Port            : 0
Local IP Address Type  : IPv4
Local IP               : 0.0.0.0
Local Port             : 61813
Remote IP Address Type : IPv4
Remote IP              : 0.0.0.0
Remote Port            : 0
```

iS5comm# show udp statistics

```
Global UDP Statistics
=========================

InDatagrams             : 40
OutDatagrams            : 40
HC InDatagrams          : 40
HC OutDatagrams         : 40
UDP No Ports            : 16679
UDP In Errors           : 16679
UDP with no Checksum    : 0
No. ICMP error packets  : 0
UDP with wrong Checksum : 0
UDP In Broadcast Mode   : 16679
```

STP

16. STP

STP (Spanning-Tree Protocol) is a link management protocol that provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations. To establish path redundancy, STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby or blocked state.

For an Ethernet network to function properly, only one active path should exist between two stations. Multiple active paths between stations in a bridged network can cause loops in which Ethernet frames can endlessly circulate. STP logically breaks such loops and prevents looping traffic from clogging the network. The dynamic control of the topology provides continued network operation in the presence of redundant or unintended looping paths.

The STP functionality is realized in the network using one of the three following STPs:

- RSTP
- MSTP
- PVRST+

RSTPis a portable implementation of the IEEE 802.1D standard. It provides rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN. It reduces the time to reconfigure the active topology of the network when physical topology or topology configuration parameters changes. It provides increased availability of MAC service when there is a reconfiguration or failure of components in a bridged LAN. It can interoperate with legacy STP bridges without any change in the configuration.

MSTP is a portable implementation of the IEEE 802.1s standard. It is used to configure spanning tree on per VLAN basis or multiple VLANs per spanning tree. It allows you to build several MST over VLAN trunks, and group or associate VLANs to spanning tree instances, so the topology of one instance is independent of the other instance. It provides multiple forwarding paths for data traffic and enables load balancing. It improves the overall network fault tolerance, as failure in one instance does not affect the other instances.

PVRST+ is an enhancement of RSTP, which works in conjunction with VLAN to provide better control over traffic in the network. It maintains a separate spanning tree for each active VLAN in the network, thus providing load balancing through multiple instances of spanning tree, fault tolerance and rapid reconfiguration support through RSTP. ***NOTE:*** *For each VLAN, a spanning-tree instance is created. Number of spanning-tree instances supported in PVRST depends on the number of instances supported by the hardware. PVRST operates only on supported instances*

16.1. clear spanning-tree detected protocols

To restart the protocol migration process on all interfaces in the switch and force renegotiation with the neighboring switches, use the command **clear spanning-tree detected protocols** in Global Configuration Mode.

clear spanning-tree detected protocols

```
clear spanning-tree detected protocols [interface interface-type <inter-face-id>] [switch default]
```

Parameters

Parameter	Type	Description
`interface`		Enter to restart the protocol migration process on the specified interface.
`interface-type`		Enter to restart the protocol migration process on the specified interface. The interface can be: • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
`<interface-id>`		Enter to clear a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
`switch`		Enter to specify a Switch Name/Context Name.
`default`		Enter default for a Switch Name/Context Name.

Mode

Global Configuration Mode

Examples

iS5comm# clear spanning-tree detected protocols interface gigabitethernet 0/1

16.2. clear spanning-tree

To delete all bridge and port level spanning tree statistics information, use the command **clear spanning-tree** in Global Configuration Mode.

For RSTP, the information contains number of:

- Transitions to forwarding state
- RSTP BPDU count received / transmitted
- Config BPDU count received / transmitted
- TCN BPDU count received / transmitted
- Invalid BPDU count transmitted
- Port protocol migration count

For MSTP, the information contains number of:

- Port forward transitions
- Port received BPDUs
- Port transmitted BPDUs
- Port invalid BPDUs received
- Port protocol migration count
- BPDUs sent / received for each MSTI

For PVRST, the information contains number of:

- Transitions to forwarding state
- PVRST BPDU count received / transmitted
- Config BPDU count received / transmitted
- TCN BPDU count received / transmitted
- Port protocol migration count

clear spanning-tree

```
clear spanning-tree mst <instance-id (1-64)> counters [interface inter-
face-type <interface-id>
```

Parameters

Parameter	Type	Description
`mst`		Enter to clear the statistical counters specific to the MSTP instance already created in the switch.
`<instance-id (1-64)>`		Enter a value for the MSTP instance already created in the switch. This value ranges from 1 to 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs. This option is applicable, only if the spanning tree mode is set as MST.
`counters`	Integer	Enter a number for maximum retries. The value ranges from 1 to 12.
`interface`		Enter to clear all port-level spanning-tree statistics information for the given port.
`interface-type`		Enter to clear all port-level spanning-tree statistics information for the specified type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
`<interface-id>`		Enter to clear a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.

Mode

Global Configuration Mode

Prerequisites

The statistics information can be deleted, only if the spanning tree functionality has not been shut down in the switch. The type of spanning tree mode should be set, if the functionality is already shutdown.

Examples

iS5comm(config)# clear spanning-tree counters interface gigabitethernet 0/1

16.3. debug customer spanning-tree

To enable tracing and generates debug statements for customer spanning tree debugging support, use the command **debug customer spanning-tree** in Privileged EXEC Mode. The no form of this command disables tracing for customer spanning tree debugging support.

debug customer spanning-tree

```
debug customer spanning-tree cep interface {Extreme-Ethernet <interface-id>
| gigabitethernet <interface-id>} {[all] [bpdu] [bridge-detec-
tion-state-machine] [errors] [events] [global] [init-shut] [management]
[memory] [port-info-state-machine] [port-receive-state-machine]
[port-role-selection-state-machine] [protocol-migration-state-machine]
[pseudoInfo-state-machine] [redundancy] [role-transition-state-machine]
[sem-variables] [state-transition-state-machine] [timer]
[topology-change-state-machine]} [{short (0-7) | alerts | critical | debug-
ging | errors | informational | notification | warnings}]
```

no debug spanning-tree

```
no debug spanning-tree {[all] [bpdu] [bridge-detection-state-machine]
[errors] [events] [global] [init-shut] [management] [memory]
[port-info-state-machine] [port-receive-state-machine] [port-role-selec-
tion-state-machine] [protocol-migration-state-machine] [pseudo-
Info-state-machine] [redundancy] [role-transition-state-machine] [sem-vari-
ables] [state-transition-state-machine] [timer]
[topology-change-state-machine]}
```

Parameters

Parameter	Type	Description
`cep interface`		Enter to display the customer spanning tree information for the specified customer edge port (CEP).
`interface`		Enter to display the interface-specific information of active ports. **NOTE:** This command does not support virtual interfaces, tunnels, or interface VLANs type of interfaces.
`Gigabitethernet`		Enter to display gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
`<interface-id>`		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
`Extreme-Ethernet`		Enter to display the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
`<interface-id>`		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
`all`		Enter to generate debug statements for all RSTP / MSTP
`bpdu`		Enter to generate debug statements for BPDU-related traces.
`bridge-detection-state-machine`		Enter to generate debug statements for bridge detection SEM.
`errors`		Enter to generate debug statements for all failure traces.
`events`		Enter to generate debug statements for event handling traces. This trace is generated to denote events that are posted to STP configuration queue whenever you configure any of the STP features.
`global`		Enter to generate debug statements for
`init-shut`		Enter to generate debug statements for init and shutdown traces. This trace is generated on failed and successful initialization and shutting down of STP related module and memory.
`management`		Enter to generate debug statements for management traces. This trace is generated whenever you configure any of the STP features.

Parameter	Type	Description
memory		Enter to generate debug statements for memory related traces. This trace is generated on failed and successful allocation of memory for STP process.
port-info-state-machine		Enter to generate debug statements for port information SEM.
port-receive-state-machine		Enter to generate debug statements for port receive SEM.
port-role-selection-state-machine		Enter to generate debug statements for role selection SEM.
port-transmit-state-machine		Enter to generate debug statements for port transmit SEM
protocol-migration-state-machine		Enter to generate debug statements for protocol migration SEM.
pseudoInfo-state-machine		Enter to generate debug statements for port receive pseudo information SEM.
redundancy		Enter to generate debug statements for redundancy code flow traces. This trace is generated in standby node STP while taking backup of configuration information from active node.
role-transition-state-machine		Enter to generate debug statements for role transition SEM
sem-variables		Enter to generate debug statements for state machine variable changes traces. This trace is generated on failed and successful creation and deletion of semaphore.
state-transition-state-machine		Enter to generate debug statements for state transition SEM.
timer		Enter to generate debug statements for timer module traces. Tis generated on failed and successful start, stop and restart of STP timers.
topology-change-state-machine		Enter to generate debug statements for topology change SEM.

Parameter	Type	Description
<level (0-7)>	Integer	Enter to generate debug statements for or the specified severity level value.This value ranges from 0 to 7.
alerts		Enter to generate debug statements for immediate action.
critical		Enter to generate debug statements for critical conditions.
debugging		Enter to generate debug statements for debugging messages.
emergencies		Enter to generate debug statements when system cannot be used.
errors		Enter to generate debug statements for for error conditions.
informational		Enter to generate debug statements for information messages.
notification		Enter to generate debug statements for significant messages.
warnings		Enter to generate debug statements for warning conditions.

Mode

Privileged EXEC Mode

Prerequisites

Debug customer spanning-tree can be executed only on customer edge ports. To set port type as customer edge ports, bridge mode is set as provider-edge bridge mode.

Default

Tracing of the STP module is disabled.

Examples

iS5comm# debug spanning-tree errors 1

16.4. debug spanning-tree

To enables the tracing of the STP module as per the configured debug levels, use the command **debug spanning-tree** in Privileged EXEC Mode. The trace statements are generated for the configured trace levels. This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single

execution of the command. The no form of this command disables the tracing of the STP module as per the configured debug levels. The trace statements are not generated for the configured trace levels.

debug spanning-tree

```
debug spanning-tree {[all] [bpdu] [bridge-detection-state-machine] [errors]
[events] [global] [init-shut] [management] [memory]
[port-info-state-machine] [port-receive-state-machine] [port-role-selec-
tion-state-machine] [protocol-migration-state-machine] [pseudo-
Info-state-machine] [redundancy] [role-transition-state-machine] [sem-vari-
ables] [state-transition-state-machine] [timer]
[topology-change-state-machine]} [switch <default>] [{<level(0-7)> | alerts
| critical | debugging | errors | informational | notification | warnings}]
```

no debug spanning-tree

```
no debug spanning-tree {[all] [bpdu] [bridge-detection-state-machine]
[errors] [events] [global] [init-shut] [management] [memory]
[port-info-state-machine] [port-receive-state-machine] [port-role-selec-
tion-state-machine] [protocol-migration-state-machine] [pseudo-
Info-state-machine] [redundancy] [role-transition-state-machine] [sem-vari-
ables] [state-transition-state-machine] [timer]
[topology-change-state-machine]} [switch <default>] | informational | noti-
fication | warnings}] | alerts
```

Parameters

Parameter	Type	Description
`all`		Enter to generate debug statements for all RSTP / MSTP
`bpdu`		Enter to generate debug statements for BPDU-related traces.
`bridge-detection-state-machine`		Enter to generate debug statements for bridge detection SEM.
`errors`		Enter to generate debug statements for all failure traces.
`events`		Enter to generate debug statements for event handling traces. This trace is generated to denote events that are posted to STP configuration queue whenever you configure any of the STP features.
`global`		Enter to generate global debug messages.
`init-shut`		Enter to generate debug statements for init and shutdown traces. This trace is generated on failed and successful initialization and shutting down of STP related module and memory.
`management`		Enter to generate debug statements for management traces. This trace is generated whenever you configure any of the STP features.
`memory`		Enter to generate debug statements for memory related traces. This trace is generated on failed and successful allocation of memory for STP process.
`port-info-state-machine`		Enter to generate debug statements for port information SEM.
`port-receive-state-machine`		Enter to generate debug statements for port receive SEM.
`port-role-selection-state-machine`		Enter to generate debug statements for role selection SEM.
`port-transmit-state-machine`		Enter to generate debug statements for port transmit SEM
`protocol-migration-state-machine`		Enter to generate debug statements for protocol migration SEM.
`pseudoInfo-state-machine`		Enter to generate debug statements for port receive pseudo information SEM.

Parameter	Type	Description
redundancy		Enter to generate debug statements for redundancy code flow traces. This trace is generated in standby node STP while taking backup of configuration information from active node.
role-transition-state-machine		Enter to generate debug statements for role transition SEM
sem-variables		Enter to generate debug statements for state machine variable changes traces. This trace is generated on failed and successful creation and deletion of semaphore.
state-transition-state-machine		Enter to generate debug statements for state transition SEM.
timer		Enter to generate debug statements for timer module traces. Tis generated on failed and successful start, stop and restart of STP timers.
topology-change-state-machine		Enter to generate debug statements for topology change SEM.
switch		Enter to generate debug statements for switch / context.
default		Enter to generate debug statements for the default for switch / context.
<level (0-7)>		Enter to generate debug statements for or the specified severity level value.This value ranges from 0 to 7.
alerts		Enter to generate debug statements for immediate action.
critical		Enter to generate debug statements for critical conditions.
debugging		Enter to generate debug statements for debugging messages.
emergencies		Enter to generate debug statements when system cannot be used.
errors		Enter to generate debug statements for for error conditions.
informational		Enter to generate debug statements for information messages.
notification		Enter to generate debug statements for significant messages.
warnings		Enter to generate debug statements for warning conditions.

Mode

Privileged EXEC Mode

Default

Tracing of the STP module is disabled.

Examples

iS5comm# debug spanning-tree errors 1

16.5. errordisable

To set the error disable recovery timer in an interface, use the command **errordisable** in Interface Configuration Mode. This command executes only if the spanning tree functionality has not been shut down in the switch.

errordisable

```
errordisable recovery-interval <seconds(30-65535)>
```

Parameters

Parameter	Type	Description
`recovery-interval`		Enter to set the error disable recovery timer in an interface. The “errordisable recovery” time is the amount of time to bring the interface out of the error-disabled state.
`<seconds(30-65535)>`	Integer	Enter a value for the error disable recovery timer in an interface. The range is from 30 to 65535 seconds. The default is 30000.

Mode

Interface Configuration Mode

Examples

iS5comm(config-if)# errordisable recovery-interval 666

16.6. instance

To create an MST instance and map it to VLANs, use the command **instance** in MSTP Configuration Mode. The no form of this command deletes the instance and unmaps specific VLANs from the MST instance.

instance

```
instance <instance ID (1-64/4094)> vlan <vlan-range>
```

no instance

```
no instance <instance ID (1-64/4094)> vlan <vlan-range>
```

Parameters

Parameter	Type	Description
instance ID		Enter to configure the ID of MSTP to be created / deleted and mapped with / unmapped from VLAN.
<instance ID (1-64/4094)>	Integer	Enter an instance ID. This value ranges from 1 to 64.his value ranges from 1 to 64. The special value 4094 can be used in the switch that supports PBB-TE. Except vlan instance mapping, other commands for STP configuration will not be applicable in this Mode.This special value represents PTETID that identifies VID used by ESP. **NOTE:** Instance 0 is created and mapped with all VLANs (1-4094).
vlan		Enter to configure a VLAN ID or list of VLAN IDs that should be mapped with / unmapped from the specified MST instance.
<vlan-range>	Integer	Enter a VLAN ID or list of VLAN IDs. This value is a string whose maximum size is 9. For example, the value is provided as 4000-4010 to represent the list of VLANs IDs from 4000 to 4010.

Mode

MSTP Configuration Mode

Examples

iS5comm(config)# spanning-tree mode mst

```
Spanning Tree enabled protocol is RSTP, now RSTP is being shutdown and
MSTP is being enabled
```

S5comm(config)# spanning-tree mst configuration

NOTE: This how MSTP Configuration Mode is entered.

iS5comm(config-mst)# instance 1 vlan 2

16.7. name

To configure the name for the MST region, use the command **name** in MSTP Configuration Mode. The no form of this command resets the name to its default value.

name

```
name <string (32)>
```

no name

Parameters

Parameter	Type	Description
<string (32)>		Enter a name for the MST region. The name is unique and used to identify the specific MST region. Each MST region contains multiple spanning tree instances and runs special instance of spanning tree known as IST to disseminate STP topology information for other STP instances.

Mode

MSTP Configuration Mode

Examples

iS5comm(config)# spanning-tree mode mst

```
Spanning Tree enabled protocol is RSTP, now RSTP is being shutdown and
MSTP is being enabled
```

S5comm(config)# spanning-tree mst configuration

NOTE: This how MSTP Configuration Mode is entered.

iS5comm(config-mst)# name regionone

16.8. revision

To configure the revision number for the MST region, use the command **revision** in MSTP Configuration Mode. The no form of this command resets the revision number to its default value.

revision

```
revision <value(0-65535)>
```

no revision

Parameters

Parameter	Type	Description
<value(0-65535)>		Enter a revision number for the MST region.

Mode

MSTP Configuration Mode

Examples

iS5comm(config)# spanning-tree mode mst

```
Spanning Tree enabled protocol is RSTP, now RSTP is being shutdown and
MSTP is being enabled
```

S5comm(config)# spanning-tree mst configuration

NOTE: This how MSTP Configuration Mode is entered.

iS5comm(config-mst)# revision 100

16.9. set performance-data

To performs performance-data related configuration, use the command **set performance-data** in Global Configuration Mode.

set performance-data

```
set performance-data {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enter to enable performance-data-status. This is the default.
disable		Enter to disable performance-data-status.

Mode

Global Configuration Mode

Examples

iS5comm(config)# set performance-data enable

16.10. set performance-data-status

To enables or disables the collection of performance data for the for RSTP and MSTP protocol, use the command **set performance-data-status** in Global Configuration Mode. This command executes only if the spanning tree functionality has not been shut down in the switch.

set performance-data-status

```
set performance-data-status {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enter to enable the collection of RSTP and MSTP performance data on all ports in the device.
disable		Enter to disable the collection of RSTP and MSTP performance data on all ports in the device. By default, the collection of performance data is disabled.

Mode

Global Configuration Mode

Examples

iS5comm(config)# set performance-data-status enable

16.11. show spanning-tree

To display spanning tree information, use the command **show spanning-tree** in Privileged EXEC Mode. This command executes only if the spanning tree functionality has not been shut down in the switch.

show spanning-tree

```
show spanning-tree [active [detail] [switch <default>]]
 [blockedports [switch <default>]]
 [bridge [{address | detail | forward-time | hello-time | id | max-age |
priority | protocol | switch}]
```

```
 [detail [switch <default>]]

 [interface {Extreme-Ethernet <interface-id> | gigabitethernet <inter-
face-id>} [bpduguard] [cost] [encapsulationtype] [inconsistency]
[layer2-gateway-port] [priority] [restricted-role] [restricted-tcn] [root-
cost] [state] [stats]]

 [layer2-gateway-port [switch <default>]]

 [mst [<instance-id (0-4094)>] [configuration [switch <default>]] [detail
[switch <default>]] [interface {Extreme-Ethernet <interface-id> | giga-
bitethernet <interface-id>} [detail] [hello-time] [stats]] [switch
<default>]]

 [pathcost method [switch <default>]]

 [performance-data] [interface {Extreme-Ethernet <interface-id> | giga-
bitethernet <interface-id>} [instance] [<instance-id>]

 [root [{address | cost | detail | forward-time | id | max-age | port |
priority [system-id [switch <default>]] | switch}]

 [summary [switch <default>]]

 [switch <default>]]

 [vlan <vlan-id/vfi_id> [active [detail] [switch <default>] [blockedports
[switch <default>]] [detail [switch <default>] [active [switch <default>]]]
[interface {Extreme-Ethernet <interface-id> | gigabitethernet <inter-
face-id>} [active] [cost] [detail] [priority] [rootcost] [state] [stats]]
[pathcost method [switch <default>]] [root [{address | cost | detail |
forward-time | id | max-age | port | priority | switch}] [summary [switch
<default>]] [switch <default>]]
```

Parameters

Parameter	Type	Description
active		Enter to display the spanning tree information of active ports.
detail		Enter to display the detailed spanning tree related information of the switch and all ports enabled in the switch. The information contains status of spanning tree operation, current selected spanning mode, current spanning tree compatibility version, bridge and root priority, bridge and root addresses, port path cost, port priority, port timers, bridge and port level spanning tree statistics information, transmit hold-count value, link-type, and status of L2GP, loop guard, BPDU receive, BPDU transmit, restricted TCN, restricted role and portfast features.
switch		Enter to display the switch name/context name.
default		Enter default to display the default switch.
blockedports		Enter to display the summary of port states.
switch		Enter to display the switch name/context name.
default		Enter default to display the default switch.
bridge		Enter to display the he spanning tree bridge information. The information contain bridge ID, hello time, maximum age time, forward delay time and protocol enabled, for the RSTP. The information also contains the instance ID for MST.
address		Enter to display the MAC address of the bridge.
detail		Enter to display the priority, address, maximum age time and forward delay time for the bridge.
forward-time		Enter to display the forward time of the bridge.
hello-time		Enter to display the hello time of the bridge.
id		Enter to display the ID of the bridge.
max-age		Enter to display the maximum age time of the bridge.
priority		Enter to display the priority of the bridge.
protocol		Enter to display the protocol currently enabled in the bridge.
switch		Enter to display the switch related information.
interface		Enter to display the interface-specific information of active ports.

Parameter	Type	Description
Gigabitethernet		Enter to display gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to display the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links.
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
bpduguard		Enter to display the spanning tree BPDU guard for RSTP and MSTP.
cost		Enter to display the summary of port states.
detail		Enter to display the detailed information about the port and bridge port cost.
encapsulationtype		Enter to display the spanning tree encapsulation type.
inconsistency		Enter to display the Spanning-tree inconsistent state for RSTP, MSTP and PVRST.
layer2-gateway-port		Enter to display the spanning tree layer two gateway port specific configuration.
portfast		Enter to display the spanning tree portfast state.
priority		Enter to display the spanning tree port priority.
restricted-role		Enter to display the spanning-tree restricted role.
restricted-tcn		Enter to display the spanning-tree restricted topology change.
rootcost		Enter to display the spanning tree rootcost (pathcost to reachthe root) value.
state		Enter to display the spanning tree state.
stats		Enter to display the input and output packets by switching path for the interface.
layer2-gateway-port		Enter to display the spanning tree layer two gateway port specific configuration.

Parameter	Type	Description
switch		Enter to display the switch name/context name.
default		Enter default to display the default switch.
mst		Enter to display the MST instance related information.
<instance-id (0-4094)>		Enter a value for the multiple spanning tree port specific information for the specified MSTI. This value ranges from 1 to 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs. display the MST instance related information.
configuration		Enter to display the multiple spanning tree instance related information. This information contains the MST region name, MST region revision, and a list containing MSTI IDs and VLAN IDs mapped to the corresponding MSTI.
switch		Enter to display the switch name/context name.
default		Enter default to display the default switch.
detail		Enter to display the spanning tree information of active ports.
switch		Enter to display the switch name/context name.
default		Enter default to display the default switch.
interface		Enter to display the spanning tree information of active ports.
Gigabitethernet		Enter to display gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to display the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.

Parameter	Type	Description
detail		Enter to display the detailed multiple spanning tree port specific information for the specified interface. The information contain port priority, port cost, root address, priority and cost, IST address, priority and cost, bridge address, priority and cost, forward delay, maximum age, maximum hop count, and BPDUs sent and received.
hello-time		Enter to display the hello time of the MSTIs assigned to the specified interface.
stats		Enter to display the number of BPDUs sent and received for the MSTIs assigned to the specified interface.
switch		Enter to display the switch name/context name.
default		Enter default to display the default switch.
pathcost		Enter to display the port pathcost method configured for the switch.
method		Enter to display the port pathcost method configured for the switch.
performance-data		Enter to display the spanning tree information of active ports.
interface		Enter to display the spanning-tree performance related information for the specified type of interface.
Gigabitethernet		Enter to display gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to display the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
instance		Enter to display spanning-tree performance data for the specified MST Instance ID.
root		Enter to display the spanning-tree root information. **NOTE:** This configuration is not supported in PVRST Mode.

Parameter	Type	Description
address		Enter to display the MAC address of the bridge.
cost		Enter to display the cost of the root bridge.
detail		Enter to display detailed information for the port and bridge.
forward-time		Enter to display the forward time of the root bridge.
hello-time		Enter to display the hello time of the root bridge.
id		Enter to display the ID of the root bridge.
max-age		Enter to display the maximum age time of the root bridge.
port		Enter to display the root port.
priority		Enter to display the priority of the root bridge.
switch		Enter to display the switch related information.
summary		Enter to display the spanning tree information of active ports.
switch		Enter to display the switch related information.
vlan		Enter to display the interface specific PVRST information for the specified VLAN.
<vlan-id/vfi_id>		Enter a number for VLAN / VFI ID. • <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094 • VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535 **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries. **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
active		Enter to display the PVRST related information for the specified active VLAN ID.

Parameter	Type	Description
detail		Enter to display the detailed PVRST related information for the specified active VLAN ID. The information contains current selected spanning Mode, current spanning tree compatibility version, bridge and root priority, bridge and root addresses, port path cost, port priority, timer values, bridge and port level spanning tree statistics information, and transmit hold-count value.
switch		Enter to display the PVRST related information for the switch name/context name.
default		Enter default to display the PVRST related information for the default switch.
blockedports		Enter to display the list of ports in blocked state and the total number of blocked ports for the specified VLAN.
switch		Enter to display the PVRST related information for the switch name/context name.
default		Enter default to display the PVRST related information for the default VLAN.
active		Enter to display the PVRST related information for the specified active VLAN ID.
switch		Enter to display the PVRST related information for the switch name/context name.
default		Enter default to display the PVRST related information for the default switch.
interface		Enter to display interface specific PVRST related information for the specified type of interface
Gigabitethernet		Enter to display gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to display the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links.

Parameter	Type	Description
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
active		Enter to display the detailed PVRST related information for the specified active VLAN ID.
cost		Enter to display the cost of the specified port.
detail		Enter to display the detailed interface specific PVRST related information for the port.
priority		Enter to display the priority of the specified port.
rootcost		Enter to display the root cost of the port. The root cost defines the pathcost to reach the root bridge.
state		Enter to display the state of the port.
stats		Enter to display the port level spanning tree statistics information.
pathcost		Enter to display the port pathcost method configured for the specified VLAN.
method		Enter to display the port pathcost method configured for the specified VLAN.
switch		Enter to display the PVRST related information for the switch name/context name
default		Enter default to display the PVRST related information for the default switch.
root		Enter to display the spanning-tree root information. **NOTE:** This configuration is not supported in PVRST Mode.
address		Enter to display the MAC address of the root.
cost		Enter to display the cost of the root.
detail		Enter to display detailed PVRST related information for the root. This information contain root priority, root address, root cost, root port, hello time, maximum age and forward delay.
forward-time		Enter to display the forward time of the root.
hello-time		Enter to display the hello time of the root.
id		Enter to display the ID of the root.

Parameter	Type	Description
max-age		Enter to display the maximum age time of the root.
port		Enter to display the root.
priority		Enter to display the priority of the root bridge.
system-id		Enter to display the Bridge system ID.
switch		Enter to display the switch related information.
default		Enter default to display the PVRST related information for the default VLAN.
summary		Enter to display the summary of port states
switch		Enter to display the switch related information.
default		Enter default to display the PVRST related information for the default VLAN.

Mode

Privileged EXEC Mode

Examples

iS5comm # show spanning-tree

```
    ------------------------------------------------------------------
    Spanning-tree for VLAN 1

    We are the root of the Spanning Tree
    Root Id         Priority   32769
    Address    e8:e8:75:90:0b:01
    Cost       0
    Port       0
    Hello Time 2 sec 0 cs, Max Age 20 sec 0 cs, Forward Delay 15 sec 0 cs

    Spanning Tree Enabled Protocol PVRST
    Bridge Id       Priority 32769
    Address e8:e8:75:90:0b:01
    Hello Time 2 sec 0 cs, Max Age 20 sec 0 cs, Forward Delay 15 sec 0 cs
    Dynamic Path Cost is Disabled
    Dynamic Path Cost Lag-Speed Change is Disabled
```

```
Name      Role          State         Cost      Prio    Type
----      ----          -----         ----      ----    ------
Gi0/11    Designated    Forwarding    20000     128     P2P
Ex0/2     Designated    Forwarding    2000      128     P2P
```

iS5comm# show spanning-tree active detail switch default

```
Spanning-tree for VLAN 1


Bridge is executing the rstp compatible PVRST Protocol
Bridge Identifier has priority 32769, Address e8:e8:75:90:0b:01
Configured Hello time 2 sec 0 cs, Max Age 20 sec 0 cs, Forward Delay 15
sec 0 cs


Dynamic Path Cost is Disabled
We are the root of the spanning tree
Number of Topology Changes 0
Time since topology Change 0 seconds ago
Transmit Hold-Count 6
Root Times: Max Age 20 sec 0 cs, Forward Delay 15 sec 0 cs, Hello Time 2
sec 0 cs


Port 11 [Gi0/11] of VLAN 1 is Designated, Forwarding
Port PathCost 20000    , Port Priority 128      , Port Identifier
128.11
Designated Root has priority 32769, address e8:e8:75:90:0b:01
Designated Bridge has priority 32769, address e8:e8:75:90:0b:01
Designated Port Id is 128.11, Designated PathCost 0
Timers: Hello Time - 2 sec 0 cs, MaxAge - 20 sec 0 cs,
Forward Delay - 15 sec 0 cs, Hold - 1 sec 0 cs
No of Transitions to forwarding State :3
BPDUs : sent 2755 , received 0
Bpdu Guard  is None
Root Guard  is Disabled
BPDU filter is Disabled


Port 26 [Ex0/2] of VLAN 1 is Designated, Forwarding
Port PathCost 2000     , Port Priority 128      , Port Identifier
128.26
Designated Root has priority 32769, address e8:e8:75:90:0b:01
Designated Bridge has priority 32769, address e8:e8:75:90:0b:01
Designated Port Id is 128.26, Designated PathCost 0
```

```
    Timers: Hello Time - 2 sec 0 cs, MaxAge - 20 sec 0 cs,
    Forward Delay - 15 sec 0 cs, Hold - 1 sec 0 cs
    No of Transitions to forwarding State :1
    BPDUs : sent 2758 , received 0
    Bpdu Guard  is None
    Root Guard  is Disabled
    BPDU filter is Disabled
```

iS5comm# show spanning-tree blockedports switch default

```
    % Blocked Ports can be retrieved per VLAN basis in PVRST
```

iS5comm# show spanning-tree bridge address

```
    Bridge Address is e8:e8:75:90:2e:01
```

iS5comm# show spanning-tree bridge forward-time

```
    Bridge Forward delay is  15 sec
```

iS5comm# show spanning-tree bridge

```
    Bridge ID                 HelloTime  MaxAge       FwdDly
    Protocol
    ---------                 ---------  ------       ------ --------
    80:00:e8:e8:75:90:2e:01   02s 00cs   20s 00cs     15 s 0  cs     rstp
```

iS5comm# show spanning-tree bridge hello-time

```
    Bridge Hello Time is 2 sec 0 cs
```

iS5comm# show spanning-tree bridge id

```
    Bridge ID is 80:00:e8:e8:75:90:2e:01
```

iS5comm# show spanning-tree bridge max-age

```
    Bridge Max Age is 20 sec 0 cs
```

iS5comm# show spanning-tree bridge protocol

```
    Bridge Protocol Running is RSTP
```

iS5comm# show spanning-tree bridge priority

```
    Bridge Priority is 32768
```

iS5comm# show spanning-tree bridge detail

```
    Bridge Id       Priority 32768,
    Address e8:e8:75:90:2e:01
    Hello Time 2sec 0cs,
    Max Age 20sec 0cs,
    Forward Delay 15 sec 0 cs
```

iS5comm# show spanning-tree detail

```
    spanning-tree portfast bpduguard disable
    Forward delay optimization alternate-role Enabled
    Spanning tree Protocol Enabled.
```

```
Bridge is executing the STP compatible Rapid Spanning Tree Protocol
Bridge Identifier has priority 32768, Address e8:e8:75:90:0b:01
Configured Hello time 2 sec 0 cs, Max Age 20 sec 0 cs,
Forward Delay 30 sec 0 cs
Dynamic Path Cost Enabled
Flush Interval 0 centi-sec, Flush Invocations 35
Flush Indication threshold 0
We are the root of the spanning tree
Number of Topology Changes 1
Time since topology Change 4250 seconds ago
Transmit Hold-Count 6
Root Times: Max Age 20 sec 0 cs  Forward Delay 30 sec 0 cs
Hello Time 2 sec 0 cs
Port 10 [Gi0/10] is Designated, Forwarding
Port PathCost 20000, Port Priority 128, Port Identifier  128.10
Designated Root has priority 32768, address e8:e8:75:90:0b:01
Designated Bridge has priority 32768, address e8:e8:75:90:0b:01
Designated Port Id is 128.10, Designated PathCost 0
No of Transitions to forwarding State :32
Auto-Edge is enabled
PortFast is disabled, Oper-Edge is disabled
LinkType is point to Point
BPDUs : sent 67637 , received 0
Timers: Hello - 1, Forward Delay - 0, Topology Change - 0,
Error Disable Recovery Interval 300 sec 0 cs
Restricted Role is disabled.
Restricted TCN is disabled.
bpdu-transmit enabled
bpdu-receive enabled
Root Guard is disabled.
Loop Guard is disabled.
Dot1W mode disabled.
```

show spanning-tree interface gigabitethernet 0/1 bpduguard

```
Bpdu Guard  is None
```

iS5comm# show spanning-tree interface gigabitethernet 0/1 layer2-gateway-port switch default

```
Switch default
Port Gi0/1 PseudoRootId
Instance      Priority         MacAddress         State
----------    ----------   -------------------  ----------
MST00          4096        00:00:11:22:33:44   Forwarding
```

```
MST01          8192        00:00:12:34:45:55   Forwarding
MST02          4096        00:00:12:34:45:5a   Forwarding
```

iS5comm# show spanning-tree mst 1

```
## MST01
Vlans mapped:    2
Bridge     Address e8:e8:75:90:0b:01    Priority 32768
Root       Address e8:e8:75:90:0b:01    Priority 32768
Root       this switch for MST01
Interface Role         Sts          Cost     Prio.Nbr Type
--------- ----         ---          ----     -------- ----
```

iS5comm# show spanning-tree mst configuration

```
Name            [regionone]
Revision        100
Max-Instance    1
Instance        Vlans mapped
--------      ----------------------------------------
0              1,3-1024,1025-2048,2049-3072,
 3073-4094
1              2
-------------------------------------------------------
```

iS5comm# show spanning-tree mst 1 interface gigabitethernet 0/1

```
Switch default
Gi0/1 of MST00 is Disabled  , Discarding
Edge port: no
Link type: Shared
Port Hello Timer: 2 sec 0 cs
Bpdus sent 0 , Received 0
Instance  Role         Sts          Cost     Prio.Nbr
--------  ----         ---          ----     --------
0         Disabled     Discarding   200000   128.1
```

iS5comm# show spanning-tree mst 1 interface gigabitethernet 0/1 stats

```
MST01     Bpdus sent 2, Received 0
```

iS5comm# show spanning-tree mst 1 interface gigabitethernet 0/1 hello-time

```
MST01     2 secs 0 cs
```

iS5comm# show spanning-tree mst 1 interface gigabitethernet 0/1 detail

```
Gi0/1 of MST01 is Master    , Forwarding
Port info     port id 128.1       priority 128   cost 200000
Designated root  address 00:01:02:03:04:11     priority 32768 cost 0
```

```
    Designated bridge address 00:01:02:03:04:11     priority 32768 port id
    128.1
```

iS5comm# show spanning-tree performance-data

```
     STP Performance data
    ====================
    Received Event Time Stamp(In millisecs)        : 0
    Port State Change Time Stamp(In millisecs)     : 527555293
```

iS5comm# show spanning-tree performance-data int gi 0/1

```
    STP Performance data at Port 1
    ==============================
    Rcvd Event Time Stamp(In millisecs)                : 0
    Rcvd Event                                         : PORT_DOWN
    Rcvd State Change Time Stamp(In millisecs)         : 527552273
```

iS5comm# show spanning-tree root

```
    Root ID                 RootCost MaxAge         FwdDly         RootPort
    -------                 -------- ------         ------         --------
    80:00:e8:e8:75:90:0b:01  0        20sec 00cs     30sec 00cs     0
```

iS5comm# show spanning-tree root address

```
    Root Bridge Address is e8:e8:75:90:0b:01
```

iS5comm# show spanning-tree root cost

```
    Root Cost is 0
```

iS5comm# show spanning-tree root forward-time

```
    Root Bridge Id is 80:00:e8:e8:75:90:0b:01
```

iS5comm# show spanning-tree root max-age

```
    Root MaxAge is 20 secs 0 cs
```

iS5comm# show spanning-tree root port

```
    Root Port is 0
```

iS5comm# show spanning-tree root priority

```
    Root Priority is 32768
```

iS5comm# show spanning-tree root detail

```
    We are the root of the Spanning Tree
    Root Id         Priority   32768
    Address    e8:e8:75:90:0b:01
    Cost       0
    Port       0
    Max Age 20 sec 0 cs, Forward Delay 30 sec 0 cs
    Hello Time 2 sec 0 cs
```

iS5comm# show spanning-tree root switch default

```
Root ID                  RootCost MaxAge         FwdDly         RootPort
-------                  -------- ------         ------         --------
80:00:e8:e8:75:90:0b:01  0        20sec 00cs     30sec 00cs     0
```

iS5comm# show spanning-tree blockedports

```
Blocked Interfaces List:
Gi0/1,Gi0/2,Gi0/3,Gi0/4,Gi0/5,Gi0/6,Gi0/7,Gi0/8,Gi0/9,Gi0/11,Gi0/12,Gi0/
13,Gi0/14,Gi0/15,Gi0/16,Gi0/17,Gi0/18,Gi0/19,Gi0/20,Gi0/21,Gi0/22,Gi0/23
,Gi0/24,Ex0/1,Ex0/2,Ex0/3,Ex0/4,po1,po2,
The Number of Blocked Ports in the system is :29
```

iS5comm# show spanning-tree pathcost method

```
Spanning Tree port pathcost method is Long
```

iS5comm# show spanning-tree summary

```
Spanning tree enabled protocol is RSTPSpanning Tree port pathcost method
is Long
RSTP Port Roles and States
Port-Index        Port-Role    Port-State   Port-Status
----------        ---------    ----------   -----------
Gi0/1             Disabled     Discarding   Enabled
Gi0/2             Disabled     Discarding   Enabled
Gi0/3             Disabled     Discarding   Enabled
Gi0/4             Disabled     Discarding   Enabled
Gi0/5             Disabled     Discarding   Enabled
Gi0/6             Disabled     Discarding   Enabled
Gi0/7             Disabled     Discarding   Enabled
Gi0/8             Disabled     Discarding   Enabled
Gi0/9             Disabled     Discarding   Enabled
Gi0/10            Designated   Forwarding   Enabled
Gi0/11            Disabled     Discarding   Enabled
Gi0/12            Disabled     Discarding   Enabled
Gi0/13            Disabled     Discarding   Enabled
Gi0/14            Disabled     Discarding   Enabled
Gi0/15            Disabled     Discarding   Enabled
Gi0/16            Disabled     Discarding   Enabled
Gi0/17            Disabled     Discarding   Enabled
Gi0/18            Disabled     Discarding   Enabled
Gi0/19            Disabled     Discarding   Enabled
Gi0/20            Disabled     Discarding   Enabled
Gi0/21            Disabled     Discarding   Enabled
Gi0/22            Disabled     Discarding   Enabled
Gi0/23            Disabled     Discarding   Enabled
```

```
Gi0/24            Disabled     Discarding   Enabled
Ex0/1             Disabled     Discarding   Enabled
Ex0/2             Disabled     Discarding   Enabled
Ex0/3             Disabled     Discarding   Enabled
Ex0/4             Disabled     Discarding   Enabled
```

iS5comm# show spanning-tree vlan 1 blockedports switch default

```
Switch default
Blocked Interfaces List:
The Number of Blocked Ports in the system is :0
```

iS5comm# show spanning-tree vlan 1 pathcost-method switch default

```
Switch default
Spanning Tree port pathcost method is Long
iS5comm# show spanning-tree vlan 1 summary switch default
Switch default
Spanning tree enabled protocol is PVRST
Spanning-tree pathcost method is long
PVRST Port Roles and States
Port-Index  Port-Role    Port-State   Port-Status
----------  ---------    ----------   -----------
1           Designated   Discarding   Enabled
2           Designated   Forwarding   Enabled
```

iS5comm# show spanning-tree vlan 1

```
Spanning-tree for VLAN 1
We are the root of the Spanning Tree
Root Id         Priority   32769
Address    e8:e8:75:90:0b:01
Cost       0
Port       0
Hello Time 2 sec 0 cs, Max Age 20 sec 0 cs, Forward Delay 15 secn0 cs
Spanning Tree Enabled Protocol PVRST
Bridge Id       Priority 32769
Address e8:e8:75:90:0b:01
Hello Time 2 sec 0 cs, Max Age 20 sec 0 cs, Forward Delay 15 sec 0 cs
Dynamic Path Cost is Disabled
Dynamic Path Cost Lag-Speed Change is Disabled
Name     Role         State        Cost     Prio   Type
----     ----         -----        ----     ----   ------
Gi0/11   Designated   Forwarding   20000    128    P2P
Ex0/2    Designated   Forwarding   2000     128    P2P
```

iS5comm# show spanning-tree vlan 1 bridge

```
Bridge ID                HelloTime MaxAge FwdDly Protocol
---------                --------- ------ ------ --------
80:00:00:01:02:03:04:01  2 sec 0 cs 20 sec 0 cs 15 sec 0  cs Pvrst
```

16.12. shutdown spanning-tree

To shut down spanning tree functionality in the switch, use the command **shutdown spanning-tree** in Global Configuration Mode. The switch does not execute any kind of STP to form a loop free topology in the Ethernet network and operates with the existing topology structure.

shutdown spanning-tree

Mode

Global Configuration Mode

Default

Spanning tree MSTP is started and enabled in the switch..

Examples

iS5comm(config)# tcp max retries 1

16.13. spanning-tree

To enable and define spanning tree operation, use the **spanning-tree** command in Global Configuration Mode. Spanning tree operation provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations. It logically breaks such loops and prevents looping traffic from clogging the network. The no form of this command disables the spanning tree operation in the switch and resets the spanning tree related information to its default values. The spanning tree operation is automatically enabled in the switch, once the spanning tree Mode is changed.The default spanning tree algorithm is rapid spanning tree. Note that the spanning tree operation can be enabled in the switch only if the spanning tree functionality has not been shut down in the switch.

spanning-tree

```
spanning-tree [compatibility {stp | rst | mst}]
 [flush-indication-threshold <value (0-65535)>]
```

[flush-interval <centi-seconds (0-500)>] [forward-time <seconds(4-30)>]

[forwarddelay optimization alternate-role {disabled | enabled}]

[hello-time <seconds(0-20)>] [max-age <seconds (6-40)>]

[mode {mst | pvrst| pvst| rapid-pvst| rst}]

[mst {<instance ID <instance ID (1-64> {primary | secondary} {priority <value (0-61440)> | flush-indication-threshold <value (0-65535)>} | configuration | forward-time <seconds(4-30> | hello-time <seconds(0-2)> | instance-id <(1-64)>| max-age <seconds (6-40)> | max-hops <(6-40)> | max-instance | <(1-64>}]

[pathcost dynamic [lag-speed]] [portfast bpduguard default] [priority <value (0-61440)>] [transmit hold-count <value (0-61440)>]

[vlan <vlan-id/vfi_id> {brg-priority <integer(0-61440)> | forward-time <seconds(4-30)> | hello-time <seconds(0-2)> | hold-count <value (1-10)> | max-age <seconds (6-40)> | brg-priority <integer(0-61440)> | root {primary | secondary}]

no spanning-tree

spanning-tree {compatibility | flush-indication-threshold| flush-interval | forward-time | forwarddelay | hello-time | max-age | mode | mst | pathcost | portfast | priority | transmit | vlan}

Parameters

Parameter	Type	Description
`compatibility`		Enter to set the STP compatibility version in the switch for all ports.
`stp`		Enter to configure Spanning Tree Protocol configuration.
`rst`		Enter to configure Rapid Spanning Tree configuration.
`mst`		Enter to configure Multiple Spanning Tree configuration.
`flush-indication-threshold`		Enter to configure the flush indication threshold value for a specific instance. When flush indication threshold is default value and flush interval is non-default value, instance based flushing occurs during the first flush indication trigger. When the flush indication threshold value is non-default (x) and flush-interval value is non-default, port & instance based flushing is triggered until the threshold (x) is reached. Once the threshold is reached, instance based flushing is triggered & timer starts.
`<value (0-65535>`	Integer	Enter a value to indicate the number of flush indications to go before the flush-interval timer method triggers and ranges from 0 (default) to 65535.
`flush-interval`		Enter to configure the flush interval timer value (in centi-seconds).
`<centi-seconds (0-500)>`	Integer	Enter a value to indicate the number of flush indications invoked from spanning-tree module per instance basis. This value ranges from 0 to 500 hundredths of a second. If the flush interval timer is set to zero, port and instance based flushing occurs (default functionality). If it is set to non-zero, instance based flushing occurs (dependent on the flush-indication-threshold value).
`forward-time`		Enter to configure the number of seconds for which a port waits before changing from the blocking state to the forwarding state. The values configured for the spanning tree timers should satisfy the following conditions: 2 * (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1) The STP timers can be configured in the switch, only if the spanning tree functionality has not been shut down in the switch. The type of spanning tree mode should be set, if the functionality is already shutdown. This spanning tree timer's configuration is not supported in PVRST mode.

Parameter	Type	Description
<seconds (4-30)>	Integer	Enter a value to indicate the forward time. This value ranges from 4 to 30 seconds. In MSTP, this time configuration is applied for IST root (that is, MSTI 0). The default is 15 seconds.
hello-time		Enter to configure the time interval (in seconds) between two successive configuration BPDUs generated by the root switch. This value is configured on per-port basis for MSTP and is configured globally for RST.
<seconds (0-2)>	Integer	Enter a value for hello- time. This value should be either 1 or 2 seconds. The default is 2 seconds.
max-age		Enter to configure the maximum expected arrival time (in seconds) of hello BPDUs. STP information learned from network on any port is discarded, once the configured arrival time expires. The spanning tree topology is re-computed after this time interval.
<seconds (6-40)>	Integer	Enter a value representing maximum age. This value ranges from 6 to 40 seconds. In MSTP, this time configuration is applied for IST root (that is, MSTI 0). The default is 20 seconds.
forwarddelay		Enter to configure the forward delay timer
optimization		Enter for optimization for spanning-tree related protocol during transition from alternate to designated port role.
alternate-role		Enter to configure the alternate port role transition by optimized configuration.
disabled		Enter to disable optimization for spanning-tree related protocol in alternate port role transition. All ports while transitioning from ALTERNATE-DESIGNATED will have fdWhile set to fwdDelay.
mode		Enter to set the type of spanning tree to be executed, enable spanning tree operation and start spanning tree functionality in the switch.
mst		Enter to configure the switch to execute MSTP for preventing undesirable loops. MSTP configures spanning tree on per VLAN basis or multiple VLANs per spanning tree. The mode cannot be set as mst, if the base bridge Mode is configured as transparent bridging.

Parameter	Type	Description
pvrst		Enter to configure the switch to execute PVRST+ for preventing undesirable loops. PVRST+ is an enhancement of RSTP which works in combination with VLAN to provide better control over traffic in the network. The Mode cannot be set as pvrst, if the base bridge Mode is configured as transparent bridging. The pvrst can be set as the spanning tree Mode, only if the GVRP feature is disabled.
pvst		Enter to configure the switch to execute PVST for preventing undesirable loops. PVST maintains separate spanning tree instance for each VLAN in the network and forwards VLAN trunk for only some VLANs. The Mode cannot be set as pvst, if the base bridge Mode is configured as transparent bridging. This feature is currently not supported.
rapid-pvst		Enter to configure the switch to execute rapid PVST for preventing undesirable loops. Rapid PVST combines the functionalities of RSTP and PVST, and creates a tree for each VLAN. The Mode cannot be set as rapid-pvst, if the base bridge Mode is configured as transparent bridging. This feature is currently not supported.
rst		Enter to configure the switch to execute RSTP for preventing undesirable loops. RSTP provides rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN.
mst		Enter to start MST configuration
instance ID		Enter to configure the ID of MSTP instance already created in the switch. This option is applicable, only if the spanning tree mode is set as MST.
<instance ID (0-64)>	Integer	Enter an instance ID. This value ranges from 1 to 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs.
root		Enter to configure the switch as root. **NOTE:** This command executes only if • instance is created • spanning tree mode is set as MST.
primary		Enter to configure the switch as primary root. It sets high enough priority (low value) for the switch so that the switch can be made as the bridge root of the spanning-tree instance. The priority value is set as 24576.

Parameter	Type	Description
secondary		Enter to configure the switch as secondary root. Sets the switch as a secondary root, if the primary root fails. The priority value is set as 28672.
priority		Enter to switch priority configuration for spanning tree instance
<priority (0-61440)>	Integer	Enter a priority value. This value ranges from 0 to 61440. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288, etc. The default is 32768.
flush-indication-threshold		Enter to configure flush indication threshold.
<value (0-65535)>	Integer	Enter a flush indication threshold value.
configuration		Enter to start MST configuration mode. In MSTP configuration mode, instance specific and MST region configuration can be done.
max-hops		Enter maximum number of hops allowed.
<(6-40)>	Integer	Enter a value representing maximum number of hops allowed. This value ranges from 6 to 40.
max-instance		Enter maximum MSTP instance value.
pathcost dynamic		Enter to enable dynamic pathcost calculation. Note that the dynamic path cost calculation feature can be configured in the switch, only if the spanning tree functionality has not been shut down in the switch. The type of spanning tree mode should be set, if the functionality is already shutdown
lag-speed		Enter for pathcost calculated when LA port speed changes due to addition or deletion of ports in port channel. Note that the manually assigned path cost is used even if the lag speed feature is enabled in the switch when the path cost is assigned manually.
portfast		Enter to specify the portfast feature in the port. This feature specifies that the port is connected to only one hosts and hence can rapidly transit to forwarding. This feature can cause temporary bridging loops, if hubs, concentrators, switches, bridges and so on are connected to this port. This feature takes effect only after the interface is shutdown and turned on again.
bpduguard		Enter to put an interface in the error-disabled state when it receives a bridge protocol data unit (bpdu).
default		Enter to enable bpduguard by default on all edgeports.

Parameter	Type	Description
priority		Enter to configure a priority value that is assigned to the switch.
<value (0-61440)>	Integer	Enter a priority value for the switch and for the MSTI, in RSTP and MSTP respectively. This value ranges from 0 to 61440. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.
transmit		Enter to set the transmit hold-count value for the switch, where the value is a counter that is used to limit the maximum transmission rate of the switch and to avoid flooding. This value specifies the maximum number of packets that can be sent in a given hello time interval. Note that the transmit hold count value configuration is not supported in PVRST Mode.
hold-count		Enter to configure a hold-count counter.
<value (0-61440)>	Integer	Enter a hold-count value which ranges from 0 to 61440.
vlan		Enter for configures spanning tree related information for VLAN.
<vlan-id/vfi_id>	Integer	VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
forward-time		Enter to configure the number of seconds, a port waits before changing from the listening and learning states to the forwarding state.
<seconds(4-30)>	Integer	Enter a value which ranges from 4 to 30 seconds. Default is 15.
hello-time		Enter to configure the time interval (in seconds) between two successive configuration BPDUs generated by the root switch.

Parameter	Type	Description
<seconds(1-10)>	Integer	Enter a value which ranges from 1 to 10 seconds. Default is 2.
max-age		Enter to configure the maximum expected arrival time (in seconds) of hello BPDUs. STP information learned from network on any port is discarded, once the configured arrival time expires. The spanning tree topology is re-computed after this time interval.
<seconds(6-40)>	Integer	Enter a value which ranges from 6 to 40 seconds. Default is 20.
hold-count		Enter to configure the maximum number of packets that can be sent in a given hello time interval. This value is used to limit the maximum transmission rate of the switch and to avoid flooding.
<integer(1-10)>	Integer	Enter a value which ranges from 4 to 10. Default is 3.
brg-priority		Enter to configure the bridge priority to be assigned for the specified VLAN. Default is 32768 + VLAN ID.
<integer(0-61440)>	Integer	Enter a value which ranges from 0 to 61440. The value should be set in increments of 4096, that is, the value can be set as 0, 4096, 8192, 12288 and so on.
root		Enter to configure Configures the root type for the given VLAN interface.
primary		Enter to configure the switch to become root for a given VLAN. The priority of the switch is lowered until it becomes root
secondary		Enter to configure the switch to become backup root for a given VLAN. The priority of the switch is lowered until it becomes one priority higher than the root, so it can become root if the current root fails

Mode

Global Configuration Mode

Examples

iS5comm (config)# spanning-tree

iS5comm(config)#spanning-tree compatibility stp

iS5comm(config)# spanning-tree flush-indication-threshold 2

iS5comm(config)# spanning-tree flush-interval 20

iS5comm(config)# spanning-tree forward-time 6

iS5comm(config)# spanning-tree max-age 6

iS5comm(config)# spanning-tree hello-time 6

iS5comm(config)#spanning-tree mode rst

iS5comm(config)# spanning-tree mst max-instance 1

iS5comm(config)# spanning-tree mode mst

```
Spanning Tree enabled protocol is RSTP, now RSTP is being shutdown and
MSTP is being enabled
```

S5comm(config)# spanning-tree mst configuration

NOTE: This how MSTP Configuration Mode is entered.

iS5comm(config)# spanning-tree pathcost dynamic

iS5comm(config)# spanning-tree portfast bpduguard default

iS5comm(config)# spanning-tree priority 4096

iS5comm(config)# spanning-tree transmit hold-count 5

iS5comm(config)# spanning-tree mode pvrst

```
Spanning Tree enabled protocol is MSTP, now MSTP is being shutdown.
PVRST is started.
```

iS5comm(config)# spanning-tree vlan 1 forward-time 18

```
Forward Time for the given instance is set.
```

iS5comm(config-if)# spanning-tree vlan 1 cost 250

16.14. spanning-tree

To enable and define spanning tree operation for an interface, use the **spanning-tree** command in Interface Configuration Mode. The no form of this command disables the spanning tree operation on an interface and resets the spanning tree to its default values. Note that the spanning tree operation can be enabled in the switch only if the spanning tree functionality has not been shut down in the switch.

spanning-tree

```
spanning-tree [auto-edge] [bpdu-receive {enabled disabled}]
 [bpdu-transmit {enabled | disabled}]
 [bpdufilter {disable | enable}]
 [bpduguard {disable | enable [admin-down] [disable-discarding] | enable |
none}]
 [cost <pathcost value(0-200000000)]
```

```
 [disable] [encap {ISL | dot1q}]

 [guard {loop | none | root}]

 [layer2-gateway-port] [link-type {point-to-point | shared}]

 [mode dot1w {disable | enable}]

 [mst {<instance-id (1-64)> {cost <cost value(0-200000000) | disable |
port-priority <port priority value(0-240)> | pseudoRootId priority <priority
value(0-61440)> mac-address <ucast_mac>} | hello-time <port based
value(1-2)>}

 [port-priority <port priority value(0-240)>]

 [portfast]

 | pseudoRootId priority <priority value(0-61440)> mac-address <ucast_mac>}

 [restricted-role]

 [restricted-tcn]

 [vlan <vlan-id/vfi_id> {cost <pathcost value(0-200000000)

 | port-priority <port priority (0-240)> | status {disable | enable}]
```

no spanning-tree

```
spanning-tree {auto-edge | bpdufilter | bpduguard | cost | disable | encap |
guard | layer2-gateway-port | link-type | mst | port-priority | portfast |
pseudoRootId | restricted-role | restricted-tcn | vlan}
```

Parameters

Parameter	Type	Description
auto-edge		Enter to enable automatic detection of bridge attached on an interface. Once automatic detection is enabled, the edge port parameter is automatically detected and set. The port is set as edge port, if no BPDU is received on the port. The port is set as non-edge port if any BPDU is received
bpdu-receive		Enter to configure the processing status of the BPDUs received in a port. BPDUs are used to carry bridge related information that is used during spanning tree operation.
enabled		Enter to allow normal processing of BPDUs received on the port.
disabled		Enter to discard the BPDUs received on the port.
bpdu-transmit		Enter to configure the BPDU transmission status of a port. BPDUs are used to carry bridge related information that is used during spanning tree operation. The transmission status is reset to its default value, once the spanning tree mode is changed.
enabled		Enter to allow the transmission of BPDUs from the port.
disabled		Enter to block the transmission of BPDUs from the port.
bpdufilter	Integer	Enter to configure the status of BPDU filter feature in an interface.
disable		Enter to disable the BPDU filter in the interface; the port state is maintained till it is manually made up.
enable		Enter to enable BPDU filter in the interface to prevent temporary loops; it moves the port to disabled discarding state when BPDU is received on this port.
bpduguard		Enter to configure the status of BPDU guard feature in an interface.
disable		Enter to disable the BPDU guard feature in the interface; the port state is maintained till it is manually made up.
enable		Enter to enable BPDU guard feature i in the interface to prevent temporary loops; it moves the port to disabled discarding state when BPDU is received on this port.
admin-down		Enter to disable the port and puts the port in error-disabled state on receiving BPDU.
disable-discarding		Enter to disable spanning-tree on the port.

Parameter	Type	Description
none		Enter to remove BPDU guard on the specified interface. Global BPDU guard configuration takes effect if this port is an edge port.
cost		Enter to configure the port's path cost value that contributes to the path cost of paths containing this particular port. The paths' path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. The configured path cost is used, even if the dynamic pathcost calculation feature or LAGG speed feature is enabled. This configuration is not supported for the spanning tree mode PVRST.
<path cost value(0-200000000)>	Integer	Enter a value for path cost. This value ranges from 1 to 200000000.
disable		Enter to disable the spanning tree operation on the port. The port does not take part in the execution of spanning tree operation for preventing undesirable loops in the network.
encap	Integer	Enter to configure the encapsulation type used in the interface.
ISL		Enter to configure the Encapsulation type as ISL
dot1q	Integer	Enter to set the Encapsulation type as dot1q
guard		Enter to configure the various guard features such as root guard in a port.
loop	Integer	Enter to enable loop guard feature in the port. This feature changes the port to an inconsistent state if no BPDUs are received. Thus isolating the failure and letting spanning tree converge to a stable topology until the port starts receiving BPDUs again. **NOTE:** This parameter can be configured only for Point-to-point links. Loop guard feature is not supported for shared links **NOTE:** PVRST Loop Guard feature can be enabled on all port types – access, trunk & hybrid, but the behavior of a guard loop enabled hybrid port in an interoperation scenario is not defined in the implementation.
none		Enter to disable both root and loop guard features in the port. This is the default.

Parameter	Type	Description
root		Enter to enable root guard feature in the port. This feature prevents the port from becoming root port or blocked port. The port changes to the root-inconsistent state, if the port receives superior BPDUs. The port automatically reverts back to forwarding state, once the superior BPDUs are not received. **NOTE:** Root Guard implementation in PVRST is applicable only for trunk ports.
layer2-gateway-port		Enter to configure a port to operate as a L2GP (L2 gateway port). L2GP operates similar to that of the normal port operation but pretends to continuously receive BPDUs when admin state of the port is up.
link-type		Enter to configure the link status of the LAN segment attached to the port. The options available are:
point-to-point		Enter to use this option when the port is to be treated as if it is connected to a point-to-point link.
shared		Enter to use this option when the port is to be treated as if it is using a shared media connection.
mode		Enter to enable or disable the bridge to send agreement PDU in accordance with 802.1w.
dot1w		Enter to enable or disable the bridge to send agreement PDU in accordance with 802.1w.
disable		Enter to disable the bridge to send agreement PDU in accordance with 802.1w.
enable		Enter to enable the bridge to send agreement PDU in accordance with 802.1w.
mst		Enter to specify the spanning tree instance.
<instance-id (1-64)>	Integer	Enter a value for instance ID. This value ranges from 1 to 64.
cost		Enter to configure the cost value associated with the port.
<cost value(0-200000000)>	Integer	Enter a value for path cost. This value ranges from 1 to 200000000.
disable		Enter to disable the spanning tree on the port
port-priority		Enter to configure the port priority.

Parameter	Type	Description
<port priority value(0-240)>	Integer	Enter a value for port priority. This value ranges from 0 to 61440. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.
pseudoRootId		Enter to configure the pseudo root related information for a port set as L2GP. The information contains pseudo root priority and pseudo root MAC address for the port. This configuration is not utilized in PVRST Mode.
priority		Enter for pseudo root priority.
<port priority value(0-61440)>	Integer	Enter value for port priority. This value ranges from 0 to 61440. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.
mac-address		Enter to configure the unicast MAC address of the pseudo root. Port configured as L2GP uses this value as its address.
<ucast_mac>		Enter the unicast MAC address of the pseudo root. For example, 00:00:12:34:45:55.
hello-time		Enter to set the port-based hello timer value.
<port based value(1-2)>	Integer	Enter a port-based hello timer value.
port-priority		Enter to configure the port priority value
<port priority value(0-240)>	Integer	Enter a port-priority value. This value ranges from 0 t
portfast		Enter to configure the portfast feature in the port. This feature specifies that the port is connected to only one host and hence can rapidly transit to forwarding. This feature can cause temporary bridging loops if hubs, concentrators, switches, bridges and so on are connected to this port. This feature takes effect only after the interface is shut down and turned on again.
pseudoRootId		Enter to the pseudo root related information for a port set as L2GP. The information contains pseudo root priority and pseudo root MAC address for the port. This configuration is not utilized in PVRST Mode
priority		Enter to configure port priority value.
<port priority value(0-61440)>	Integer	Enter for pseudo root priority.

Parameter	Type	Description
mac-address	Integer	Enter to configure the unicast MAC address of the pseudo root. A port configured as L2GP uses this value as its address.
<ucast_mac>		Enter the unicast MAC address of the pseudo root. For example, 00:00:12:34:45:55.
restricted-role		Enter to enable the root-guard/ Restricted role feature on the port.
restricted-tcn		Enter to enable the Topology change guard/ Restricted tcn feature on the port.
vlan		Enter for configures spanning tree related information on a per VLAN basis.
<vlan-id/vfi_id>	Integer	VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
cost		Enter to configure the port's path cost value that contributes to the path cost of paths containing this particular port. The paths' path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. The configured path cost is used, even if the dynamic pathcost calculation feature or LAGG speed feature is enabled. This configuration is not supported for the spanning tree mode PVRST.
<cost value(0-200000000)>	Integer	Enter a value for path cost. This value ranges from 1 to 200000000.
port-priority		Enter to configure the priority value assigned to the port.

Parameter	Type	Description
<port priority value(0-240)>	Integer	Enter a priority value to be assigned to the port. This value is used during port role selection process. This value ranges from 0 to 240. This value should be set in steps of 16, that is, you can set the value as 0, 16, 32, 48 and so on. The default port-priority is 128.
status		Enter to configure the status of PVRST on a port for the specified VLAN. PVRST works in conjunction with VLAN to provide better control over traffic in the network. It maintains a separate spanning tree for each active VLAN in the network, thus providing load balancing through multiple instances of spanning tree, fault tolerance and rapid reconfiguration support through RSTP.
disable		Enter to disable the PVRST Status for the specified VLAN ID.
enable		Enter to enable the PVRST Status for the specified VLAN ID.

Mode

Interface Configuration Mode

Examples

iS5comm (config)# interface gi 0/1

iS5comm (config-if)# spanning-tree auto-edge

iS5comm (config-if)# spanning-tree bpdu-receive disabled

iS5comm (config-if)# spanning-tree bpdu-transmit enabled

iS5comm (config-if)# spanning-tree bpduguard enable admin-down

iS5comm(config-if)# spanning-tree cost 2200iS5comm (config-if)# spanning-tree link-type point-to-pointiS5comm(config-if)# spanning-tree portfast

iS5comm(config)# spanning-tree portfast bpduguard default

iS5comm(config-if)# spanning-tree port-priority 32

iS5comm (config-if)# spanning-tree restricted-role

iS5comm(config-if)# spanning-tree restricted-tcn

iS5comm(config-if)# spanning-tree layer2-gateway-port

iS5comm(config-if)# spanning-tree mst 1 pseudoRootId priority 8192 mac-address 00:00:12:34:45:55

iS5comm(config-if)# spanning-tree bpdufilter enable

iS5comm(config-if)# spanning-tree mode dot1w enable

iS5comm(config-if)# spanning-tree vlan 1 status disable

MRP

17. MRP CLI Commands

This section describes the CLI commands used to configure the *MRP* feature.

Media Redundancy Protocol (*MRP*) is a networking protocol designed to implement redundancy and recovery in a ring topology. *MRP* is designed to react deterministically on a single failure on a switch in the *MRP* ring. An *MRP* instance is configured between two ports known as ring ports and can act as manager or client in the ring. The *MRP* node which is configured as manager has the responsibility of avoiding the loop in the ring by making one ring port as blocking and other as forwarding. The convergence time of *MRP* is very fast as compared to spanning tree protocols. On a port either *MRP* can be enabled or spanning tree may be selected.

To configure *MRP*, first it needs to be enabled at the global level, the instance needs to be created with required mode and then instance needs to be mapped to the ring ports, this chapter describes the commands used.

Note: To enable an *MRP* ring instance on a port; first spanning tree needs to be disabled. Both protocols cannot run together on the same port.

17.1. Redundancy

Redundancy within the network considers the presence of more network elements (switches, link) than necessary operation, in order to prevent the loss of communication caused by a failure. To effect this, there is more than one physical path between any two nodes. IEC 61918 specified ring topology, every switch has a redundant connection (link) into the network. the redundant links are not required for a failure-free/normal operation of the network. In case of a failure, these redundant links are used to prevent the breakdown of the network. The disadvantage of ring topology is that, it can introduce a “packet loop” that creates broadcast storms in the network.

panning Tree protocols, such as *RSTP*, specify a method for providing media redundancy while preventing the undesirable packet loop in a network (i.e.) RSTP were developed to detect and eliminates the physical loop in the network. Also, in case of a failure in the network, a topology change notification is sent out to create a different safe path.

Although STP is effective enough for many networks, it takes longer time for re-convergence in case of failure. This is not good enough for mission-critical industrial Ethernet applications. To overcome the limitations of *RSTP*, *MRP* protocol was developed. *MRP* uses mechanisms similar to *RSTP* (e.g., delete forwarding database after reconfiguration, set ports into blocking or forwarding mode), but it takes lesser time for re-convergence in case of failure. Below is the comparison of *MRP* with *RSTP*.

Table 1: Comparison between MRP and RSTP

	MRP	RSTP
Topology	Ring	Any
Number of Switches	Up to 50 switches to meet the 200ms reconfiguration requirement.	Maximum of 40 Switches
Recovery Time	Recovery time in case of a failure can run into Less than 200ms	Recovery time in case of a failure can run into seconds depending on the topology and size of the network.
Configuration	Simple	Medium

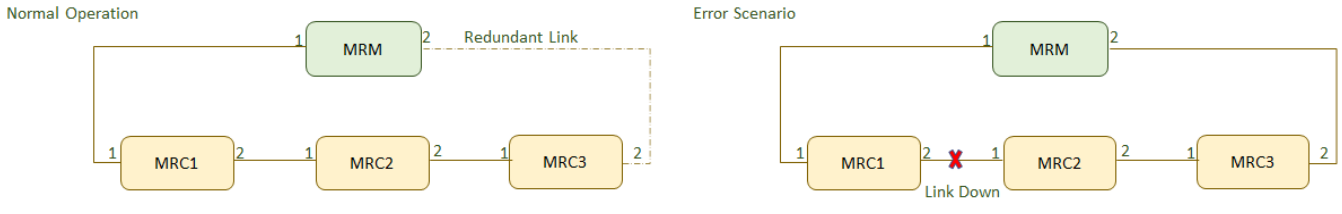
17.2. Media Redundancy Protocol

An *MRP* compliant network shall have a ring topology with multiple nodes. According to IEC 62439-2, One of nodes in the network takes on the role of the redundancy manager (*MRM*), the other nodes are the redundancy clients (*MRC*). The ports at a node which are connected with the subsequent or preceding node are named ring ports.

17.3. MRP Function

It is the Redundancy Manager's responsibility to monitor the ring topology. During normal ring operation (i.e., no link or node failure in the ring topology) the Redundancy Manager disconnects one of its ring ports, so that the ring topology becomes 'loop free' from a communication point of view. As soon as the ring is open due to the failure of a node, and the data communication is broken, the Redundancy Manager reconfigures the data paths within 200ms. It enables the disconnected ring port and creates a new loop free topology.

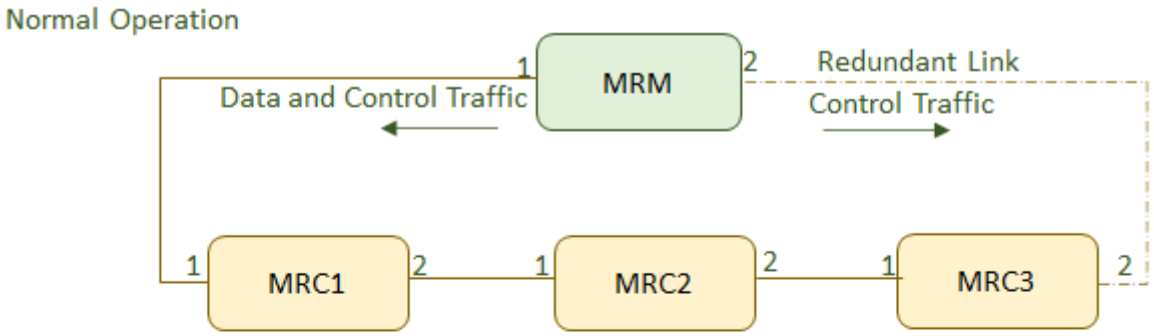
Figure 1: MRP Normal Operation Vs Error Scenario



17.4. Normal Operation: (Ring Closed)

In order to detect errors in the network, the redundancy manager sends MRP_Test frames on both of its ring ports. These frames run through the ring in both directions until they arrive at the other ring port of the manager. These MRP_Test frames are marked with a special MAC address and forwarded by the MRCs only to the opposite ring ports. They are sent periodically every MRP_Test default interval (20 ms by default). If the MRP_Test frames arrive on both ends back to the *MRM*, the ring is detected as defect free(ring closed) and the *MRM* blocks the loop. This is done by changing the state to BLOCKED at one of the ring ports in the MRM and the other as FORWARDING as shown in Figure 2 below. On this BLOCKED port only test frames to supervise the ring (MRP_Test frames) are sent. Data frames are sent by the *MRM* only on the port in the FORWARDING state.

Figure 2: MRP Normal Operation



	Ring Port1	Ring Port 2
MRM	Forwarding	Blocked
MRC1	Forwarding	Forwarding
MRC2	Forwarding	Forwarding
MRC3	Forwarding	Forwarding

Blocked port can tx and rx only the control traffic. Hence MRM transmit the data traffic via ring port 1 only.

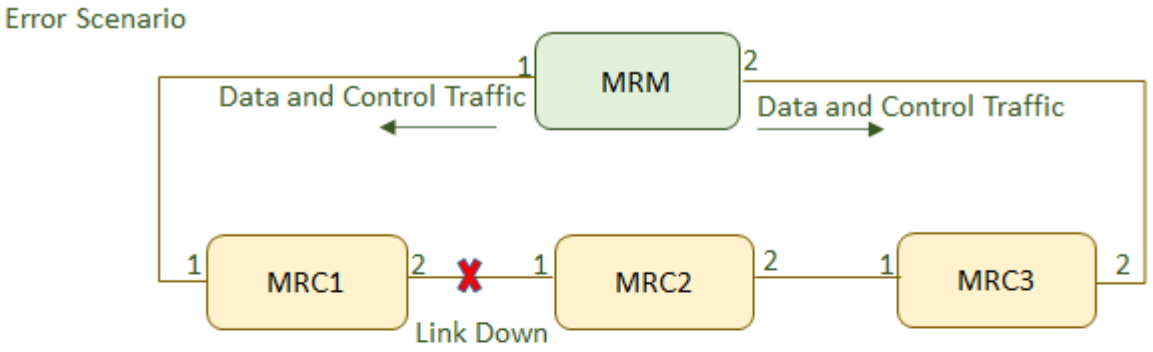
17.5. Failure Detection: (Ring Open)

If MRP_Test frames, typically 3 frames in sequence of are not received by the *MRM*, the ring topology is considered as interrupted. So it takes 60 ms to detect a failure in the ring. To change the topology in the

whole ring, all *MRC*s and the *MRM* have to clear their FDBs at the same time as the redundant port is changing state from BLOCKED to FORWARDING to keep the network consistent. The *MRM* sends 3 MRP_TopologyChange messages in 10ms delay into the ring with the indication that the topology has changed. The blocked port on the *MRM* changes the state from BLOCKING to FORWARDING. Every *MRC* receiving MRP_TopologyChange indications is supposed to clear its Filtering Data Base (FDB) at the MRP_TOPchgT time. Afterwards it has to build up again the FDB based on the new topology.

The time between detecting a ring interruption and restoring a new data structure is referred to as the recovery time. The recovery time has a maximum value of 200ms. As soon as the fault is recovered in the network, the redundancy manager disconnects its ring port again and informs the clients of the change.

Figure 3: MRP Error Scenario



	Ring Port1	Ring Port 2
MRM	Forwarding	Forwarding
MRC1	Forwarding	Link Down
MRC2	Link Down	Forwarding
MRC3	Forwarding	Forwarding

Ring is open, due to link fault between MRC1 & MRC2. MRM ports (1 &2) are in forwarding state to tx and rx both data and control traffic.

17.6. Alarms supported in MRP

Alarms are raised for various events that occur in the device. Alarms for the events in *MRP* are grouped under protocols. As defined in the PRD document, the following alarms are supported for events associated with *MRP*.

- *MRP* Status changes
- *MRM* condition detected/cleared.

Figure 4: Alarms supported in MRP

```
iS5comm# sh alarm supported all
```

```
ALARM-ID    ALARM-SUPPORTED
---------  ------------------

2000        Power supply limit exceeded
2001        Mainboard temperature overheat
2002        CPU usage exceeded threshold
2003        Flash usage exceeded threshold
2004        RAM usage exceeded threshold
2005        Power supply not operational
2006        Line card state

3000        Interface link state
3001        Cyber-security link
3002        Line module temperature threshold reached

4000        Invalid login

5000        Firmware upgrade failed

6000        RSTP root bridge node
6001        VRRP master - VRID
6002        MRP Ring status changed
6003        MRP Multiple MRM condition
```

17.7. MRP status changed:

The alarm is raised with set whenever there is a change in the ring status. This event can occur whenever there is a change in ring status. i.e., ring is closed or opened due to changes in topology or configuration. When the ring state machine is disabled, the alarm is cleared.

Figure 5: Alarms raised for Ring status change

```
iS5comm# sh alarm history protocol
```

```
ID    TYPE      TIMESTAMP      STATE          DESCRIPTION                SEVERITY
-----------------------------------------------------------------------------------
6000  PROTOCOL Oct/5/14:15:41   SET   RSTP root bridge node              Info
6002  PROTOCOL Oct/5/14:15:42   CLR   MRP Ring status changed            Critical
6002  PROTOCOL Oct/5/14:15:44   SET   MRP Ring status changed            Critical
```

17.8. MRM condition/detected

The alarm is raised when the ring node detects more then one manager nodes in the network. The alarm will be cleared when this condition is cleared.

17.9. mrp

To enable and disable the *MRP* protocol, use the command **mrp enable / disable** in Global Configuration Mode.

mrp

```
mrp { enable | disable }
```

Parameters

Parameter	Type	Description
enable		Enables the MRP feature globally on device.
disable		Disables the MRP feature globally on device.

Mode

Global Configuration Mode

Examples

iS5comm(config)# mrp enable

iS5comm(config)# mrp disable

17.10. mrp ringid

To create an *MRP* instance, use the command **mrp ringid** in Global Configuration Mode. The no form of this command deletes an *MRP* instance.

mrp

```
mrp { ringid < short(1-2) > }
```

no mrp ringid

```
no mrp { ringid < short(1-2) > }
```

Parameters

Parameter	Type	Description
ringid		Enter to create Ring id of the MRP instance.
id	integer	Enter a value in the range from 1 to 2.

Mode

Global Configuration Mode

Examples

- Users can delete the *MRP* instance. The details are shown below.

```
(config)# mrp ringid 1


(config-mrp)# exit


(config)# no mrp ringid 1
```

17.11. mrp vid

To create an *MRP* domain *VLAN* identifier, use the command **vid** in MRP Ring Configuration Mode. The no form of this command deletes an *MRP* domain *VLAN* identifier.

vid

```
vid  < VLAN id (1-4094) >
```

no vid

```
no vid
```

Parameters

Parameter	Type	Description
VLAN id (1-4094)	integer	Enter a value in the range of 1 to 4094

Mode

MRP Ring Configuration Mode

Examples

- Users are able to configure *MRP* over *VLAN* using the below shown CLI command under *MRP* Ring Mode. *MRP* signaling frames (test and control) are sent with IEEE 802.1Q *VLAN* tags with the configured *VLAN* and priority as 7.

```
(config)# mrp ringid 1


(config-mrp)# vid 2


(config-mrp)# end
```

- User are able to unconfigure *MRP* over *VLAN* under *MRP* Ring Mode as shown below.

```
(config)# mrp ringid 1


(config-mrp)# no vid


(config-mrp)# end
```

17.12. mode

To set the *MRP* mode of the device, use the command **mode** in *MRP* Ring Configuration Mode.

mode

```
mode [ { disable | { client | manager | manager-autocomp } port1 < interface-type
> < interface-id > port2 < interface-type > < interface-id > } ]
```

Parameters

Parameter	Type	Description
client		Enter to configure *MRP* instance as a client (*MRC*) in the *MRP* ring, which forwards the test frames between the ring ports.
manager		Enter to configure *MRP* instance as manager (*MRC*) in the *MRP* ring, which generates the test frames on both ring ports and handles/avoids the loop.
manager -autocomp		Enter to configure *MRP* instance as manager auto (*MRA*) in the *MRP* ring. It competes with the other *MRA* nodes in the ring to become *MRM* based on priority, if priority is highest it turns to act as *MRM* else turn *MRC*.
disable		Enter to disables the *MRP* instance on ring ports if any.
port1		Enter to set *MRP* mode on ring on port 1.
port2		Enter to set *MRP* mode on ring on port 2.

Mode

MRP Configuration Mode

Examples

iS5comm# configure terminal

iS5comm(config)# mrp ringid 1

iS5comm(config-mrp)# vid 2

iS5comm(config-mrp)# mode manager-autocomp port1 gigabitethernet 0/1 port2 gigabitethernet 0/2

17.13. priority

To set the *MRP* priority of the device to become the manager (*MRM*) of the ring, use the command **priority** in *MRP* Ring Configuration Mode.

priority

```
priority < (0-65535) >
```

Parameters

Parameter	Type	Description
priority	0-65535	Enter to configure *MRP* priority to be manager (*MRM*) in the ring, in case auto manager is enabled.

Mode

MRP Configuration Mode

Examples

iS5comm# configure terminal

iS5comm(config)# mrp ringid 1

iS5comm(config-mrp)# priority 8000

17.14. uuid

To configure the UUID value of the ring, use the command **uuid** in *MRP* Ring Configuration Mode.

uuid

```
uuid < string(32) >
```

Parameters

Parameter	Type	Description
uuid	string(32)	Enter to configure *MRP UUID* as 32 octet string (hex). The UUID is a 128-bit domain UUID unique to a domain/ring. All MRP instances belonging to the same ring must have the same domain ID.

Mode

MRP Configuration Mode

Examples

iS5comm# configure terminal

iS5comm(config)# mrp ringid 1

iS5comm(config-mrp)# uuid 10C20ACC507B55760487569C4CD9E3BB

17.15. show mrp

This command shows information of the *MRP* configuration.

show mrp

```
show mrp { ringid < short(1-2) > } [ detail ] [ counters ]
```

Parameters

Parameter	Type	Description
ringid		Specifies the ring ID that the user wishes to view.
id (1-2)	integer	Enter a value in the range of 1 - 2.
detail		Enter to display the detail information of the *MRP* configuration (e.g. ring name, UUID, priority, etc.)
counters		Enter to display the *MRP* counters

Mode

Privileged Exec Mode

Definitions of Errors

Multiple *MRM* failures and errors: This error indicated by an *MRM* when more than one *MRM* are active in the *MRP* ring. Possible values are as follows:

- false—no Multi-*MRM* error
- true—more than one *MRM* present in the ring

Single Side Error—displays Single Side Error state: This error also indicated by an *MRM* when the test frames of an *MRM* have been seen, but only on one ring port. Possible values are as follows:

- false—no One Side Rx error
- true—test frame received only on one ring port

Examples

```
iS5comm# show mrp ringid 1 detail
MRP Ring Info
-------------------------------------
```

```
 Id           : 1
 Admin Mode   : Manager
 Port 1       : Gi0/2
 Port 1 state : Forwarding
 Port 2       : Gi0/1
 Port 2 state : Forwarding
 State       : Open
 Multiple MRM : True
 Single side Err : False
 UUID         : 10C20ACC507B55760487569C4CD9E3BB
 Manager pri  : 1F40-------------------------------------
iS5comm# show mrp counters
 MRP Ring Counters
--------------------------------------
Id                                  : 1
Ring Port 1
Test frames received            : 0
TC frames received              : 0
Link up frames sent             : 0
Link down frames sent           : 0
Ring Port 2
Test frames received            : 0
TC frames received              : 0
Link up frames sent             : 0
Link down frames sent           : 0
```

LA

18. LA

LA (Link Aggregation) is a method of combining physical network links into a single logical link for increased bandwidth. LA increases the capacity and availability of the communications channel between devices (both switches and end stations) using existing Fast Ethernet and Gigabit Ethernet technology. LA also provides load balancing where the processing and communication activity is distributed across several links in a trunk, so that no single link is overwhelmed. By taking multiple LAN connections and treating them as a unified, aggregated link, practical benefits in many applications can be achieved.

LA provides the following important benefits:

- Higher link availability
- Increased link capacity

Improvements are obtained using existing hardware (no upgrading to higher-capacity link technology is necessary)

The Link Aggregation Control Protocol (LACP), described by IEEE 802.3ad, defines a method for two switches to automatically establish and maintain link aggregation groups (LAG)s, or also called port channels or channel-groups. Port channels combine the bandwidth of multiple Ethernet ports into a single logical link, and management functions treat a LAG as if it were a single physical port.

When LACP is not enabled, a port channel might attempt to transmit packets to a remote single interface, which causes the communication to fail.

When LACP is enabled, a local LAG cannot transmit packets unless a LAG with LACP is also configured on the remote end of the link.

A channel group is a collection of Ethernet interfaces on a single switch. A port channel interface is a virtual interface that serves a corresponding channel group and connects to a compatible interface on another switch to form a port channel. Port channel interfaces can be configured and used in a manner similar to Ethernet interfaces. Port channel interfaces are configurable as Layer 2 interfaces, Layer 3 (routable) interfaces, and VLAN members.

The switch supports up to 8 link aggregation groups, with a maximum of up to 8 ports per group.

18.1. channel-group

To add a port as a member of the specified port channel that is already created in the switch, use the command **channel-group** in Interface Configuration Mode. The no form of the command deletes the aggregation of the port from all port channels.

channel-group

```
channel-group <channel-group-number(1-65535)> mode {active | on | passive}
```

no channel-group

Parameters

Parameter	Type	Description
<channel-group-number(1-65535)>	Integer	Enter to add a port as a member of the specified port channel that is already created in the switch. This is a unique value that represents the specific port-channel created. This value ranges from 1 to 65535.
mode		Enter to configure the LACP activity for the port.
active		Enter to configure starting of LACP negotiation unconditionally.
on		Enter to force the interface to channel without LACP. This is equivalent to manual aggregation.
passive		Enter to configure starting of LACP negotiation only when LACP packet is received from peer.

Mode

Interface Configuration Mode

Prerequisites

This command executes successfully, only if

- the LA functionality is started and enabled in the switch.

Examples

iS5comm(config)# interface gi 0/9

iS5comm (config-if)# channel-group 2 mode active

18.2. channel-protocol

To enable link aggregation (LA) in the switch, use the command **channel-protocol** in Global Configuration Mode. This command is a standardized implementation of the existing command set port-channel and it operates similarly to this command. The no form of the command disables LA in the switch.

channel-protocol

```
channel-protocol lacp
```

no channel-protocol

Parameters

Parameter	Type	Description
lacp		Enter to configure LACP (Link Aggregation Control Protocol) to provide manage channeling.

Mode

Global Configuration Mode

Default

LA is disabled

Examples

iS5comm(config)# channel-protocol lacp

18.3. channel-protocol

To enable link aggregation (LA) in the switch, use the command **channel-protocol** in Global Configuration Mode. This command is a standardized implementation of the existing command set port-channel and it operates similarly to this command. The no form of the command disables LA in the switch.

channel-protocol

```
channel-protocol lacp
```

no channel-protocol

Parameters

Parameter	Type	Description
`lacp`		Enter to configure LACP (Link Aggregation Control Protocol) to provide manage channeling.

Mode

Global Configuration Mode

Default

LA is disabled

Examples

iS5comm(config)# channel-protocol lacp

18.4. debug etherchannel

To enable the trace messages for link aggregation, use the command **debug etherchannel** in Privileged EXEC Mode. The trace statements are generated for the configured trace levels.This command is a standardized implementation of the existing command **debug lacp** and operates similar to this command.The no form of the command disables the tracing of the link aggregation as per the configured debug levels. The trace statements are not generated for the configured trace levels.

debug etherchannel

```
debug etherchannel [all] [detail] [error] [event]
```

no debug etherchannel

```
no debug etherchannel [all] [detail] [error] [event]
```

Parameters

Parameter	Type	Description
`all`		Enter to generate debug statements for all kinds of traces.
`detail`		Enter to generate detailed debug statements for traces
`error`		Enter to generate debug statements for all failure traces.
`event`		Enter to generate debug statements for event traces. This trace is generated when any of packets are sent successfully or when an ACK is received. Event generates error messages for the following scenarios: • Packet reception/transmission • Timer expiry • Port creation/deletion indication • Port status change indication

Mode

Privileged EXEC Mode

Examples

iS5comm# debug etherchannel detail

18.5. debug lacp

To enable the tracing of the LACP as per the configured debug levels, use the command **debug lacp** in Privileged EXEC Mode. This command allows combination of debug levels to be configured (i.e. more than one level of trace can be enabled or disabled. The debug levels are configured one after the other and not in single execution of the command. The no form of the command disables the tracing of LACP as per the configured debug levels. Trace statements are not generated for the configured trace level.

debug lacp

```
debug lacp [all] [buffer] [data] [events] [failall] [init-shutdown] [mgmt]
[os] [packet]
```

no debug lacp

```
no debug lacp [all] [buffer] [data] [events] [failall] [init-shutdown]
[mgmt] [os] [packet]
```

Parameters

Parameter	Type	Description
all		Enter to generate debug statements for all kinds of traces.
buffer		Enter to generate debug statements for buffer-related traces.
data		Enter to generate debug statements for data path traces. This trace is generated during failure in packet processing.
events		Enter to generate debug statements for event traces. This trace is generated when any of packets are sent successfully or when an ACK is received.
failall		Enter to generate debug statements for all kind of failure traces.
init-shutdown		Enter to generate debug statements for init and shutdown traces. These traces are generated during module initialization and shutdown.
mgmt		Enter to generate debug statements for management traces. This trace is generated whenever you configure any of the LA features.
os		Enter to generate debug statements for OS resource related traces. This trace is generated during failure in message queues.
packet		Enter to generate debug statements for packet dump traces. This trace is generated for all events generated during processing of packets.

Mode

Privileged EXEC Mode

Default

init-shutdown

Examples

iS5comm# debug lacp data

18.6. default port

To configure the port that should be set as default port for a port channel, use the command **default port** in Interface Configuration Mode. The configured port attaches with the port channel and participates

only in dynamic aggregation selection.The no form of the command deletes the default port assigned for the port channel.

default port

```
default port {Extreme-Ethernet <interface-id> | gigabitethernet <inter-face-id>]
```

no default port

Parameters

Parameter	Type	Description
Gigabitethernet		Enter to configure the type of interface to be set as default port for the port channel as gigabitetethernet type interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to configure a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to configure the type of interface to be set as default port for the port channel as Extreme-Ethernet type interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to configure a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.

Mode

Interface Configuration Mode

Prerequisites

- This command can be executed successfully, only if the LA functionality is started and enabled in the switch.
- Only one port can be set as a default port.
- The port that is to be set as default port should have not been added as a member port for any of the port channel.

Examples

iS5comm# interface gigabitethernet 0/2

iS5comm(config-if)# default port gigabitethernet 0/2

18.7. defaulted-state-threshold

To configure the default threshold on all ports in system and track the maximum number of times error recovery can be triggered from default state, use the command **defaulted-state-threshold** in Interface Configuration Mode. The no form of the command resets the defaulted state threshold value to default.

defaulted-state-threshold

```
defaulted-state-threshold <integer (0-20)>
```

no defaulted-state-threshold

Parameters

Parameter	Type	Description
<integer (0-20)>	Integer	Enter a value for the default threshold on all ports in system and track the maximum number of times error recovery can be triggered from default state. This value ranges from 0 to 20. The default is 5.

Mode

Interface Configuration Mode

Examples

iS5comm# interface gi 0/2

iS5comm(config-if)# defaulted-state-threshold 10

18.8. hw-failure recovery-threshold

To configure the hardware failure recovery threshold on all ports in system and track the maximum number of times when error recovery is triggered after a hardware failure, use the command **hw-failure recovery-threshold** in Interface Configuration Mode. The configured port attaches with the port channel and participates only in dynamic aggregation selection. The no form of the command resets the value of hardware failure recovery threshold on port.

hw-failure recovery-threshold

```
hw-failure recovery-threshold <integer (0-20)>
```

no hw-failure recovery-threshold

Parameters

Parameter	Type	Description
<integer (0-20)>	Integer	Enter a value for the hardware failure recovery threshold on all ports in system and track the maximum number of times error recovery triggered after a hardware failure. This value ranges from 0 to 20. The default is 5.

Mode

Interface Configuration Mode

Examples

iS5comm# interface gi 0/2

iS5comm(config-if)# hw-failure recovery-threshold 10

18.9. lacp admin-key

To configure the LACP actor admin key and LACP Mode for a port, use the command **lacp admin-key** in Interface Configuration Mode.

lacp admin-key

```
lacp admin-key <admin-key(1-65535)> [mode {active | passive}]
```

Parameters

Parameter	Type	Description
<admin-key(1-65535)>	Integer	Enter a value to configure the LACP actor admin key that is used while port participates in dynamic aggregation selection. The port is made as part of best aggregation selected based on system ID and admin key.This value ranges from 1 to 65535.
mode		Enter to configure the LACP Mode for the port.
active		Enter to configure starting of LACP negotiation unconditionally. This is the default mode.
passive		Enter to configure starting of LACP negotiation only when LACP packet is received from a peer.

Mode

Interface Configuration Mode

Prerequisites

This command executes successfully, only if

- the LA functionality is started and enabled in the switch.
- The admin key can be configured only for ports that select aggregator dynamically (the port is configured as default interface for a port channel)

Examples

iS5comm(config)# interface gi 0/9

iS5comm (config-if)# lacp admin-key 1 mode active

18.10. lacp port-identifier

To configure the LACP actor admin port ID to be filled in the LACP, use the command **lacp port-identifier** in Interface Configuration Mode. The no form of the command resets the global LACP System ID to its default value.

lacp port-identifier

```
lacp port-identifier <port-id (1-65535)>
```

Parameters

Parameter	Type	Description
<port-id (1-65535)>	Integer	Enter a value to configure the LACP actor admin port ID to be filled in the LACP PDUs. This value represents the concerned aggregation port. This value ranges from 1 to 65535. The maximum limit depends on the number of ports. For example, if there are 24 ports, then the maximum value will be 24 only and the value will range from 1 to 24.

Mode

Interface Configuration Mode

Prerequisites

This command executes successfully, only if

- the LA functionality is started and enabled in the switch.
- This configuration takes effect only on the interface that is configured for LACP.

Examples

iS5comm(config)# interface gi 0/9

iS5comm (config-if)# lacp port-identifier 2

18.11. lacp port-priority

To configure the LACP port priority, use the command **lacp port-priority** in Interface Configuration Mode. The no form of the command resets the LACP port priority to its default value.

lacp port-priority

```
lacp port-priority <priority (0-65535)>
```

no lacp port-priority

Parameters

Parameter	Type	Description
<priority (0-65535)>	Integer	Enter a value to configure the LACP port priority. This value ranges from 0 to 65535. This port priority is used in combination with LACP port identifier during the identification of best ports in a port channel. The priority determines if the link is an active link or a standby link, when the number of ports in the aggregation exceeds the maximum number supported by the hardware. The links with lower priority become active links. The default is 128.

Mode

Interface Configuration Mode

Prerequisites

This command executes successfully, only if

- the LA functionality is started and enabled in the switch.
- This configuration takes effect only on the interface that is configured for LACP
- The LACP port priority will not be reset to its default value if the port is removed from one port channel and added to another port channel.

Examples

iS5comm(config)# int gi 0/9

iS5comm(config- if)# lacp port-priority 1

18.12. lacp rate

To configure the LACP rate, use the command **lacp rate** in Interface Configuration Mode. This command is a standardized implementation of the existing command **lacp timeout**. It operates similar to the existing command. The no form of the command resets the LACP rate to its default value.

lacp rate

```
lacp rate {normal | fast}
```

no lacp rate

Parameters

Parameter	Type	Description
`normal`		Enter to configure to ingress the LACP control packets at normal rate. That is, LACP PDU should be received every 30 seconds and the timeout value (no packet is received from peer) is set as 90 seconds. This is the default.
`fast`		Enter to configure to ingress the LACP control packets at fast rate. That is, LACP PDU should be received every 1 second and the timeout value is set as 3 seconds.

Mode

Interface Configuration Mode

Prerequisites

This command executes successfully, only if

- the LA functionality is started and enabled in the switch.
- This configuration takes effect only on the interface that is configured for LACP.

Examples

iS5comm(config)# interface gi 0/9

iS5comm (config-if)# lacp rate fast

18.13. lacp system-identifier

To configure the global LACP system ID, use the command **lacp system-identifier** in Global Configuration Mode. The no form of the command resets the global LACP System ID to its default value.

lacp system-identifier

```
lacp system-identifier <system-id (aa:aa:aa:aa:aa:aa)>
```

no lacp system-identifier

Parameters

Parameter	Type	Description
<system-id (aa:aa:aa:aa:aa:aa)>		Enter a string to configure the global LACP system ID. The system ID denotes a 6-octet unicast MAC address value that is used as a unique identifier for the switch containing the aggregator.

Mode

Global Configuration Mode

Prerequisites

This command executes successfully, only if

- the LA functionality is started and enabled in the switch.

Examples

iS5comm(config)# lacp system-identifier 00:01:02:03:04:05

18.14. lacp system-priority

To configure the LACP priority, use the command **lacp system-priority** in Global Configuration Mode. The no form of the command resets the LACP priority to its default value.

lacp system-priority

```
lacp system-priority <priority (0-65535)>
```

no lacp system-priority

Parameters

Parameter	Type	Description
<priority (0-65535)>	Integer	Enter to configure the LACP priority associated with actor's system ID. This priority value ranges between 0 and 65535. The switch with the lowest LACP decides the standby and active links in the LA. The default is 32768.

Mode

Global Configuration Mode

Prerequisites

This command executes successfully, only if

- the LA functionality is started and enabled in the switch.
- when D-LAG status is disabled

Examples

iS5comm(config)# set port-channel enable

18.15. lacp timeout

To configure the LACP timeout period within which LACP PDUs should be received on a port and avoid timing out of the aggregated link, use the command **lacp timeout** in Interface Configuration Mode. The no form of the command resets the LACP timeout period to its default value.

lacp timeout

```
lacp timeout {long | short}
```

no lacp timeout

Parameters

Parameter	Type	Description
`long`		Enter to configure the LLACP timeout period as 90 seconds. The LACP PDU should be received every 30 seconds. This is the default.
`short`		Enter to configure the LLACP timeout period as 3 seconds. The LACP PDU should be received every second.

Mode

Interface Configuration Mode

Prerequisites

This command executes successfully, only if

- the LA functionality is started and enabled in the switch.
- This configuration takes effect only on the interface that is configured for LACP.

Examples

iS5comm(config)# interface gi 0/9

iS5comm (config-if)# lacp timeout short

18.16. lacp wait-time

To configure the LACP wait-time for an interface, use the command **lacp wait-time** in Interface Configuration Mode. The no form of the command resets the LACP wait-time to its default value.

lacp wait-time

```
lacp wait-time <time <(0-10)>
```

no lacp wait-time

Parameters

Parameter	Type	Description
<time (0-10)>	Integer	Enter a value to configure the LACP wait time for an interface. This value ranges from 0 to 10 seconds. The wait time represent the time (in seconds) till which the port waits before entering into aggregation after receiving partner information (that is, this represents the time taken to attach to the port channel). The default is 2.

Mode

Interface Configuration Mode

Prerequisites

This command executes successfully, only if

- the LA functionality is started and enabled in the switch.
- This configuration takes effect only on the interface that is configured for LACP.
- The LACP wait-time will not be reset to its default value if the port is removed from one port channel and added to another port channel

Examples

iS5comm(config)# interface gi 0/9

iS5comm (config-if)# lacp wait-time 1

18.17. port-channel max-ports

To configure the maximum number of ports that can be attached to a port channel, use the command **port-channel max-ports** in Interface Configuration Mode. The best ports are maintained in active state and other ports are maintained in standby state, if the total number of ports attached to the port channel exceeds the configured value.

port-channel max-ports

```
port-channel max-ports <integer (2-8)>
```

Parameters

Parameter	Type	Description
<integer (2-8)>	Integer	Enter a value to configure the maximum number of ports that can be attached to a port channel. This value ranges from 2 to 8. The default is 8.

Mode

Interface Configuration Mode

Prerequisites

This command executes successfully, only if

- the LA functionality is started and enabled in the switch.

Examples

iS5comm(config)# interface gi 0/9

iS5comm (config-if)# port-channel max-ports 5

18.18. port-channel

To configure the load balancing policy for all port channels created in the switch, the defaulted state threshold value for tracking the maximum number of times a port in defaulted state undergoes error recovery, the value of error-recovery threshold, the hardware failure recovery threshold value, the action to be performed on reaching the recovery threshold, and same state recovery threshold value for tracking the maximum number of times the port stays in the same state before triggering error recovery, use the command **port-channel** in Global Configuration Mode. The no form of the command resets the load balancing policy and all threshold values to their default values. It also resets the action to be performed on reaching the recovery threshold.

port-channel

```
port-channel {load-balance {dest-ip | dest-ip6 | dest-l4-port | dest-mac |
l3-protocol | mac-dest-vid | mac-src-dest-vid | mac-src-vid |
service-instance | src-dest-ip | src-dest-mac | src-ip | src-ip6 |
src-l4-port | src-mac | vlan-id} [<port-channel-index(1-65535)>]
 | defaulted-state-threshold <integer (0-20)>
 | error-recovery-threshold <integer (0-20)>
 | hw-failure recovery-threshold <integer (0-20)>
 | rec-threshold-exceed-action <integer (0-20)>
```

```
 | same-state {none | shutdown}
```

no port-channel

```
port-channel {load-balance [<port-channel-index(1-65535)>]
|defaulted-state-threshold | error-recovery-threshold | hw-failure
recovery-threshold | rec-threshold-exceed-action | same-state}
```

Parameters

Parameter	Type	Description
load-balance		Enter to configure the load balancing policy for all port channels created in the switch. The policy sets the rule for distributing the Ethernet traffic among the aggregated links to establish load balancing.
dest-ip		Enter to specify that the load distribution is based on the destination IP address. The bits of the destination IP address in the packet are used to select the port in which the traffic should flow.
dest-ip6		Enter to specify that the load distribution is based on the destination IPv6 address. The bits of the destination IP address in the packet are used to select the port in which the traffic should flow.
dest-l4-port		Enter to specify that the load distribution is based on the destination Layer 4 port. The bits of the destination Layer 4 port in the packet are used to select the port in which the traffic should flow.
dest-mac		Enter to specify that the load distribution is based on the destination host MAC address. The bits of the destination MAC address in the packet are used to select the port in which the traffic should flow. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
l3-protocol		Enter to specify that the load distribution is based on the Layer 3 protocol. The bits of the Layer 3 protocol in the packet are used to select the port in which the traffic should flow.
mac-dest-vid		Enter to specify that the load distribution is based on the destination MAC address and VLAN ID. The VLAN ID and destination MAC address in the packet are used to select the port in which the traffic should flow.
mac-src-dest-vid		Enter to specify that the load distribution is based on the VLAN ID, and destination and source MAC address. The VLAN ID, source MAC address and destination MAC address in the packet are used to select the port in which the traffic should flow.
mac-src-vid		Enter to specify that the load distribution is based on the source MAC address and VLAN ID. The VLAN ID and source MAC address in the packet are used to select the port in which the traffic should flow.

Parameter	Type	Description
service-instanc		Enter to specify that the load distribution is based on the service-instance. The ISID in the packet is used to select the port in which the traffic should flow. Packets with the same service-instance use the same port. Packets with different service-instance use different ports such that the load is balanced among ports. The port can have packets with different service-instances as well. **NOTE:** Service Instance Selection Policy is only applicable for Provider Backbone Bridges.
src-dest-ip		Enter to specify that the load distribution is based on the source and destination IP address. The bits of the source and destination IP address in the packet are used to select the port in which the traffic should flow.
src-dest-mac		Enter to specify that the load distribution is based on the source and destination MAC address. The bits of the source and destination MAC address in the packet are used to select the port in which the traffic should flow.
mac-src-vid		Enter to specify that the load distribution is based on the source MAC address and VLAN ID. The VLAN ID and source MAC address in the packet are used to select the port in which the traffic should flow.
src-ip		Enter to specify that the load distribution is based on the source IP address. The bits of the source IP address in the packet are used to select the port in which the traffic should flow.
src-ip6		Enter to specify that the load distribution is based on the source IPv6 address. The bits of the source IP address in the packet are used to select the port in which the traffic should flow.
src-l4-port		Enter to specify that the load distribution is based on the source Layer 4 port. The bits of the source Layer 4 port in the packet are used to select the port in which the traffic should flow.
src-mac		Enter to specify that the load distribution is based on the source MAC address. The bits of the source MAC address in the packet are used to select the port in which the traffic should flow. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.
vlan-id		Enter to specify that the load distribution is based on the VLAN ID. The VLAN ID in the packet is used to select the port in which the traffic should flow.

Parameter	Type	Description
<port-channel-index(1-65535)>	Integer	Enter to configure the load balancing policy for the specified port-channel. This is a unique value that represents the specific port-channel created. This value ranges from 1 to 65535.
defaulted-state-threshold		Enter to configure the defaulted state threshold value for tracking the maximum number of times a port in defaulted state undergoes error recovery. This value overrides the threshold value configured on the ports.
<integer (0-20)>	Integer	Enter a value for defaulted state threshold value for tracking the maximum number of times a port in defaulted state undergoes error recovery. This value ranges from 0 to 20. The default is 5.
error-recovery-threshold		Enter to configure the error-recovery-threshold.
<integer (0-20)>	Integer	Enter a value for error-recovery-threshold. It ranges from 0 to 20. The default is 5.
hw-failure		Enter to configure the hardware failure.
recovery-threshold		Enter to configure the hardware failure recovery threshold value for tracking the maximum number of times a port can undergo recovery after a hardware failure. This value overrides the threshold value configured on the ports.
<integer (0-20)>	Integer	Enter a value for hardware failure recovery threshold. This value ranges from 0 to 20. The default is 5.
rec-threshold-exceed-action		Enter to configure the action to be performed on reaching the recovery threshold.
none		Enter to set the recovery threshold exceed action as none in the port channel, in which no action will be is performed on reaching the recovery threshold of the port and the port remains in the same state (admin up). This is the default option.
shutdown		Enter to shut down the recovery threshold exceed action in the port channel, in which the administrative status of the port is made as down when the recovery is triggered after reaching the threshold value.
same-state		Enter to configure the same state recovery threshold value for tracking the maximum number of times the port stays in the same state before triggering error recovery.
recovery-threshold		Enter to configure the same state recovery threshold value for tracking the maximum number of times the port stays in the same state before triggering error recovery.

Parameter	Type	Description
<integer (0-20)>	Integer	Enter a value for the same state recovery threshold. This value ranges from 0 to 20. The default is 5.

Mode

Global Configuration Mode

Default

load balance—src-dest-mac

rec-threshold-exceed-action—none

All threshold values—5

Prerequisites

This command executes successfully, only if

- Port-Channel is created in the system and mapped to a context.
- the LA functionality is started and enabled in the switch.

Examples

iS5comm(config)# port-channel load-balance mac-src-dest-vid 1

iS5comm(config)# port-channel defaulted-state-threshold 10

iS5comm(config)# port-channel error-recovery-threshold 16

iS5comm(config)# port-channel hw-failure recovery-threshold 10

iS5comm(config)# port-channel rec-threshold-exceed-action none

S5comm(config)# port-channel same-state recovery-threshold 10

18.19. same-state recovery-threshold

To configure the same state recovery threshold on all ports in system and to track the maximum number of times the port stays in the same state before triggering error recovery, use the command **same-state recovery-threshold** in Interface Configuration Mode. The no form of the command resets the value of same state recovery threshold on port.

same-state recovery-threshold

```
same-state recovery-threshold <integer (0-20)>
```

no same-state recovery-threshold

Parameters

Parameter	Type	Description
`<integer (0-20)>`	Integer	Enter a value for the same state recovery threshold on all ports in system. This value ranges from 0 to 20. The default is 5.

Mode

Interface Configuration Mode

Examples

iS5comm (config)# interface gi 0/2

iS5comm(config-if)# same-state recovery-threshold 10

18.20. set port-channel

To configure the admin status of LA in the switch, use the command **set port-channel** in Global Configuration Mode.

set port-channel

```
set port-channel {enable | disable}
```

Parameters

Parameter	Type	Description
`enable`		Enter to enable LA feature in the switch. The LA feature allows aggregating individual point-to-point links into a port channel group, so that the capacity and availability of the communications channel between devices are increased using the existing interface technology. Also, it starts the LA in the switch if the LA has been shut down. **NOTE:** a port-channel can be also called a link aggregation group or LAG.
`disable`		Enter to disable LA feature in the switch. This is the default.

Mode

Global Configuration Mode

Examples

iS5comm(config)# set port-channel enable

18.21. show etherchannel

To display the EtherChannel information port-channels created in the switch, use the command **show etherchannel** in Privileged EXEC Mode. This information contains “admin” and “oper” status of port-channel module and status of protocol operate Mode for each group.

show etherchannel

```
show etherchannel [<channel-group-number(1-65535)>] [detail] [load-balance]
[port] [port-channel] [protocol] [summary]
```

Parameters

Parameter	Type	Description
`<channel-group-number(1-65535)>`	Integer	Enter a value identifying a port-channel group to display EtherChannel information for the specified port-channel group. This is a unique value that represents the specific port-channel created. This value ranges from 1 to 65535.
`detail`		Enter to display detailed EtherChannel information. The information contain admin and oper status of port channel module, LACP system priority, status of protocol operate Mode for each group, port details for each group and port channel details. The port details contain port state, group to which the port belongs, port mode, aggregation state, port-channel ID, pseudo port-channel ID, admin key, oper key, port number, port state, and LACP port-priority, wait-time, port identifier, activity and timeout. The port channel details contain port channel ID, number of member ports, ID of hot standby port, port state, status of protocol operate Mode, aggregator MAC and default port ID.
`load-balance`		Enter to display the load balancing policy applied for each port-channel groups.
`port`		Enter to display the status of protocol operate mode and port details for each group. The port details contain port state, group to which the port belongs, port Mode, aggregation state, port-channel ID, pseudo port-channel ID, admin key, oper key, port number, port state, and LACP port-priority, wait-time, port identifier, activity and timeout.
`port-channel`		Enter to display the admin and oper status of port channel module, and port channel details. The port channel details contain port channel ID, number of member ports, ID of hot standby port, port state, status of protocol operate Mode, aggregator MAC and default port ID.
`protocol`		Enter to display the status of protocol operate mode for each port-channel group.
`summary`		Enter to display the admin and oper status of port channel module, number of channel groups used, number of aggregators, group IDs, and port channel ID, status of protocol operate Mode and member ports for each group

Mode

Privileged EXEC Mode

Prerequisites

This command executes successfully only if,

- LA functionality is started in the switch.
- Port channel is created in the system

Examples

iS5comm# show etherchannel

```
Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel recovery action on exceeding Threshold is None
Port-channel Independent mode is disabled
Port-channel System Identifier is  00:01:02:03:04:05
LACP System Priority: 5
LACP Error Recovery Time: 0
LACP Error Recovery Threshold: 5
LACP Recovery Triggered count: 0
LACP Error Recovery Threshold for Defaulted State : 5
LACP Error Recovery Threshold for Hardware Failure : 5
LACP Same state threshold : 5

Channel Group Listing
---------------------
Group : 1
----------
Group Status : L2
Protocol : Disabled
Group : 2
----------
Group Status : L2
Protocol : Disabled
```

iS5comm# show etherchannel detail

```
Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel Independent mode is disabled
Port-channel System Identifier is  00:01:02:03:04:05
LACP System Priority: 5
```

```
                  Channel Group Listing
    ---------------------
    Group: 1
    ----------
    Protocol :LACP
    Ports in the Group

    ------------------
    Port : Gi0/2
    -------------
    Port State = Up in Bundle
    Channel Group : 1
    Mode : Active
    Port-channel = Po1
    Pseudo port-channel = Po1
    LACP port-priority  = 128
    LACP Wait-time  = 2 secs
    LACP Port Identifier = 2
    LACP Activity : ActiveLACP Timeout : LongAggregation
    State : Aggregation, Sync, Collecting, Distributing, Defaulted
    LACP Port   Admin  Oper   Port   Port     State   Priority    Key
    Number  State
    ------------------------------------------------------------------------
    Gi0/2    Bundle  128         1      1      0x2     0xbe
    Port-channel : Po1
    -------------------
    Number of Ports = 1
    HotStandBy port = null
    Port state = Port-channel Ag-Inuse
    Protocol = LACP
    Aggregator-MAC  00:03:02:03:04:41
    Maximum number of Ports  = 5
    Port-Channel Mtu         = 1500
    Port-Channel Speed       = 100 Mbps
    Port-Channel High Speed  = 0 Mbps
    Port-Channel Member Ports
    Speed = 100 MbpsPort-Channel
    Member Ports High Speed  = 100 Mbps
```

iS5comm# show etherchannel load-balance

```
     Channel Group Listing
```

```
 ---------------------
Group : 1
----------
Source and Destination Mac VID
```

iS5comm# show etherchannel port

```
 Channel Group Listing
---------------------
Group: 1----------
Protocol :LACP
                Ports in the Group                  ------------------
Port : Gi0/2
-------------
Port State = Up in Bundle
Channel Group : 1
Mode : Active
Port-channel = Po1
Pseudo port-channel = Po1
LACP port-priority  = 128
LACP Wait-time  = 2 secs
LACP Port Identifier = 2
LACP Activity : Active
LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting, Distributing,
Defaulted

LACP Port   Admin  Oper   Port
PortPort     State   Priority    Key    Key    Number  State
-----------------------------------------------------------------------
Gi0/2    Bundle  128         1      1      0x2     0xbe
```

iS5comm # show etherchannel port-channel

```
Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel Independent mode is enabled
Port-channel System Identifier is  00:01:02:03:04:05
LACP System Priority: 5
                Channel Group Listing
---------------------Group : 1
----------e : L2
```

```
                Port-channels in the group:
---------------------------
Port-channel : Po1
------------------
Number of Ports = 1
HotStandBy port = null
Port state = Port-channel Ag-Not-Inuse
Protocol = LACP
Aggregator-MAC  00:04:02:03:04:41
Maximum number of Ports  = 5
Port-Channel Mtu         = 1500
Port-Channel Speed       = 0 Mbps
Port-Channel High Speed  = 0 Mbps
Port-Channel Member Ports Speed = 100 Mbps
Port-Channel Member Ports High Speed = 100 Mbps
```

iS5comm # show etherchannel protocol

```
 Channel Group Listing
                ---------------------
Group : 1
----------
Group Status : L2
Protocol : LACP
```

iS5comm# show etherchannel summary

```
Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel recovery action on exceeding Threshold is None
Port-channel Independent mode is disabled
Port-channel System Identifier is  e8:e8:75:90:0b:01
LACP System Priority: 32768
LACP Error Recovery Time: 0
LACP Error Recovery Threshold: 5
LACP Recovery Triggered count: 0
LACP Error Recovery Threshold for Defaulted State : 5
LACP Error Recovery Threshold for Hardware Failure : 5
LACP Same state threshold : 5
```

18.22. show interfaces etherchannel

To display the EtherChannel details for all aggregated ports and port channels, use the command **show interfaces etherchannel** in Privileged EXEC Mode. The port details contain port state, group to which the

port belongs, port Mode, aggregation state, port-channel ID, pseudo port-channel ID, admin key, oper key, port number, port state, and LACP port-priority, wait-time, port identifier, activity and timeout. The port channel details contain port channel ID, number of member ports, ID of hot standby port, port state, status of protocol operate Mode, aggregator MAC, and default port ID.

show interfaces etherchannel

```
show interfaces {Extreme-Ethernet <interface-id> | Gigabitethernet <inter-
face-id>} etherchannel
```

Parameters

Parameter	Type	Description
`Gigabitethernet`		Enter to display gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
`<interface-id>`		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
`Extreme-Ethernet`		Enter to display the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
`<interface-id>`		Enter to display a specific slot number / port number. The format is <0>/<1-4> without spaces between Slot Number/Port Number. For example, 0/1.
`etherchannel`		Enter to display the EtherChannel details for a specific interface.

Mode

Privileged EXEC Mode

Prerequisites

This command executes successfully only if,

- LA functionality is started in the switch.

Examples

iS5comm# show interfaces gigabitethernet 0/1 etherchannel

```
    Port : Gi0/1
    -------------
```

```
Port State = Up, Independent
Channel Group :  1
Mode : Active
Port-channel = Null
Pseudo port-channel = Po1
LACP port-priority  = 1
LACP Wait-time  = 1 secs
LACP Admin Port = 2
LACP Activity : Active
LACP Timeout : Short

Aggregation State : Aggregation, Sync, Defaulted Expired

                  LACP Port   Admin  Oper   Port
  Port     State   Priority    Key       Number  State
-------------------------------------------------------
Gi0/1    Indep   1           1      1      0x1     0xf3
```

iS5comm# show interfaces etherchannel

```
Port : Gi0/2
-------------

Port State = Up, Independent
Channel Group : 1
Mode : Active
Port-channel = Null
Pseudo port-channel = Po1
LACP port-priority  = 128
LACP Wait-time  = 2 secs
LACP Port Identifier = 2
LACP Activity : Active
LACP Timeout : Long

Aggregation State : Aggregation, Sync, Defaulted Expired

 LACP Port   Admin  Oper   Port
  Port     State   Priority    Key       Number  State
-------------------------------------------------------
Gi0/2    Indep   128         1      1      0x2     0xb3

Port-channel : Po1
```

```
-------------------

Number of Ports = 1
HotStandBy port = null
Port state = Port-channel Ag-Not-Inuse
Protocol = LACP
Aggregator-MAC  00:04:02:03:04:41
Maximum number of Ports  = 5

Port-Channel Mtu         = 1500
Port-Channel Speed       = 0 Mbps
Port-Channel High Speed  = 0 Mbps
Port-Channel Member Ports Speed = 100 Mbps
Port-Channel Member Ports High Speed  = 100 Mbps
```

18.23. show lacp

To display LACP counter / neighbor information for all port-channels, use the command **show lacp** in Privileged EXEC Mode.

show lacp

```
show lacp {<port-channel(1-65535)> {counters | neighbor [detail]} | counters
| neighbor [detail]}
```

Parameters

Parameter	Type	Description
<port-channel (1-65535)>	Integer	Enter a value for port-channel to display LACP counter / neighbor information for the specified port-channel. This is a unique value that represents the specific port-channel created. This value ranges from 1 to 65535.
counters		Enter to display the LACP counter information. The information contains port ID, LACP PDUs sent and received, number of markers sent and received, number of marker response sent and received, number of LACP PDUs packets and number of LACP PDUs errors.
neighbor		Enter to display LACP neighbor information. This information contains partner system ID, flags details, LACP partner port priority, operational key, and port state
detail		Enter to display the detailed LACP neighbor information. This information contain partner system ID, flags, aggregation state, and LACP partner port priority, partner oper key, partner port state, activity and timeout.

Mode

Privileged EXEC Mode

Prerequisites

This command executes successfully only if,

- LA functionality is started and enabled in the switch.

Examples

iS5comm# show lacp 1 counters

```
    LACPDUs            Marker     Response    LACPDUs         Error States
    Port   Sent  Recv      Sent  Recv      Sent   Recv      Pkts Err
    Detd Trgd
    ------------------------------------------------------------------------
    -----------
    Channel group: 1
    ------------------
    No interfaces aggregated in the channel group
```

18.24. shutdown port-channel

To shut down LA feature in the switch and release all resources allocated to the LA feature, use the command **shutdown port-channel** in Global Configuration Mode. LA feature allows aggregating individual point-to-point links into a port channel group, so that the capacity and availability of the communications channel between devices are increased using the existing interface technology. The no form of the command starts and enables LA feature in the switch, and allocates required memory to the LA module. The LA feature is made available in the switch only if the LA is enabled in the switch.

shutdown port-channel

no shutdown port-channel

Mode

Global Configuration Mode

Default

LA is started in the switch, but not enabled. That is LA operational status is disabled

Prerequisites

LA cannot be started in the switch, if the base bridge Mode is configured as transparent bridging

Examples

iS5comm(config)# shutdown port-channel

LLDP

19. LLDP

LLDP (Link Layer Discovery Protocol) supports a set of attributes that it uses to discover the neighbor devices. These attributes contain type, length, and value descriptions and are referred to as Time to Live (TLV)s. LLDP supported devices can use TLVs to receive and send information to their neighbors.

TLV (Time to Live) is value that defines for the receiving agent how long the information contained in the TLV Value field is valid.

TTL = message transmission interval * hold time multiplier.

For example, if the value of LLDP transmission interval is 30, and the value of the LLDP hold multiplier is 4, then the value 120 is encoded in the TTL field in the LLDP header.

Fast transmission periods are initiated when a new neighbor is detected, and cause LLDP packets to be transmitted at a shorter time interval than during normal operation of the protocol. The fast transmission period ensures that more than one LLDP packet is transmitted when a new neighbor is detected. The first transmission is immediate, and the subsequent transmissions occur at the specified fast transmission (TX) interval.

The switch supports the following mandatory basic management TLVs.

- Port description TLV
- System name TLV
- System description
- System capabilities TLV
- Management address TLV
- Port VLAN ID TLV (IEEE 802.1 organizationally specific TLVs)
- MAC/PHY configuration/status TLV (IEEE 802.3 organizationally specific TLVs)

LLDP conforms to IEEE 802.1AB-2005 standard. The LLDP allows systems on an Ethernet LAN to advertise their key capabilities and also to learn about the key capabilities of other systems on the same Ethernet LAN. This, in turn, promotes a unified network management view of the LAN topology and connectivity to aid network administration and trouble-shooting.

LLDP provides the following features:

- Provides full conformance to the 802.1AB specification.
- Supports all mandatory TLVs (Chassis ID, Port ID and Time To Live).
- Supports optional TLVs - Port description, System name, System description, System capabilities and Management address.

- Supports organizationally specific optional TLVs - Port VLAN ID, Port and protocol VLAN ID, VLAN name, MAC or PHY configuration or status, Link Aggregation and Maximum frame size.
- Provides a generic set of APIs for easy integration into different platforms.
- Supports the basic MIB, as well as, the extension MIBs in Appendix F and Appendix G as defined in the 802.1AB specification and a proprietary MIB for management.
- Provides support for notifications through Traps

19.1. clear lldp

To clear LLDP-related information, use the command **clear lldp** in Global Configuration Mode.

clear lldp

```
clear lldp {counters | table}
```

Parameters

Parameter	Type	Description
counters		Enter to clear the inbuilt counter which has the total count of LLDP frames that are transmitted/ received. **NOTE:** This command does not clear the global statistics.
table		Enter to clear all LLDP information about the neighbors

Mode

Global Configuration Mode

Prerequisites

This command executes only if LLDP is started.

Examples

iS5comm(config)# clear lldp counters

iS5comm(config)# clear lldp table

19.2. debug lldp

To specify debug level for LLDP module, use the command **debug lldp** in Privileged EXEC Mode. The no form of the command disables debug option for LLDP module.

debug lldp

```
debug lldp {all | all-fail | buf | critical | ctrl | data-path | init-shut |
mgmt] | pkt-dump | redundancy | resource

 | tlv {all | chassis-id | inventory-management | lagg | mac-phy | max-frame
| med-capability | mgmt-addr | mgmt-digest | network-policy | port-descr |
port-id | port-vlan | ppvlan | proto-id | pwr-mdi | sys-capab | sys-descr |
sys-name | ttl | vid-digest | vlan-name}
```

no debug lldp

```
no debug lldp {all | all-fail | buf | critical | ctrl | data-path |
init-shut | mgmt] | pkt-dump | redundancy | resource | tlv}
```

Parameters

Parameter	Type	Description
all		Enter to generate debug statements for all kinds of traces.
all-fail		Enter to generate debug statements for all kinds of failure traces.
buf		Enter to generate buffer allocation / release traces.
critical		Enter to generate debug statements for critical SEM.
ctrl		Enter to generate debug statements for control plane traces.
data-path		Enter to generate debug statements for data path traces. This trace is generated during failure in packet processing.
init-shut		Enter to generate debug statements for initiation and shutdown traces. his trace is generated on failed initialization and shutting down of LLDP related entries.
mgmt		Enter to generate debug statements for management traces. This trace is generated during failure in configuration of any of the LLDP features.
pkt-dump		Enter to generate debug statements for packet dump traces.
redundancy		Enter to generate debug statements for the LLDP redundancy module.
resource		Enter to generate debug statements for OS resource related traces. This trace is generated during failure in message queues.
tlv		Enter to generate debug statements for TLV related traces for the following traces:
all		Enter to generate debug statements for all TLV trace messages.
Chassis-ID		Enter to generate debug statements for Chassis-ID TLV traces.
inventory-management		Enter to generate debug statements for inventory-management TLV traces.
lagg		Enter to generate debug statements for Link Aggregation TLV traces.
mac-phy		Enter to generate debug statements for MAC or PHY TLV traces.
max-frame		Enter to generate debug statements for maximum frame TLV traces.
med-capability		Enter to generate debug statements for MED Capability TLV traces.
mgmt-addr		Enter to generate debug statements for Management VID TLV traces.
mgmt-digest		Enter to generate debug statements for Management VID traces.

Parameter	Type	Description
network-policy		Enter to generate debug statements for Network-policy TLV traces.
port-descr		Enter to generate debug statements for Port description TLV traces.
port-id		Enter to generate debug statements for Port-ID TLV traces.
port-vlan		Enter to generate debug statements for Port-VLAN TLV traces.
ppvlan		Enter to generate debug statements for Port-protocol-VLAN TLV traces.
proto-id		Enter to generate debug statements for Protocol-ID TLV traces.
pwr-mdi		Enter to generate debug statements for power-through-MDI TLV traces
sys-capab		Enter to generate debug statements for system capabilities TLV traces.
sys-descr		Enter to generate debug statements for system description TLV traces.
sys-name		Enter to generate debug statements for system name TLV traces.
ttl		Enter to generate debug statements for TTL TLV traces.
vid-digest		Enter to generate debug statements for VID digest TLV traces.
vlan-name		Enter to generate debug statements for VLAN-name TLV traces.

Mode

Privileged EXEC Mode

Prerequisites

This command executes only if LLDP is started

Examples

iS5comm# debug lldp init-shut

iS5comm# debug lldp tlv sys-descr

19.3. lldp

To configure global LLDP properties on the switch such as, interval at which LLDPDU are transmitted, chassis identifier, hold time-multiplier value, reinitialization delay time, transmit delay, or maximum number of consecutive LLDPDUs that can be transmitted at any time or during fast transmission period, use the command **lldp** in Global Configuration Mode. This command executes only if LLDP is started. The no form of the command resets the multiplier, the notification interval, reinitialization delay time, the transmission interval, and the transmit delay to their default values.

lldp

```
lldp {MessageFastTx <range (1-3600)>
 | chassis-id-subtype {chassis-comp <string(255)> | if-alias | if-name |
local <string(255)> | mac-addr | nw-addr | port-comp <string(255)>}
 | holdtime-multiplier <value(2-10)>
 | notification-interval <seconds(5-3600)>
 | reinitialization-delay <seconds(1-10)>
 | transmit-interval <value(5-32768)>
 | tx-delay <value(1-8192)>
 | txFastInit <value(1-8)>}
```

no lldp

```
no lldp {holdtime-multiplier | notification-interval | reinitializa-
tion-delay | transmit-interval | tx-delay}
```

Parameters

Parameter	Type	Description
MessageFastTx		Enter to configure the interval at which LLDP frames are transmitted on behalf of this LLDP agent during fast transmission period. Fast transmission periods are initiated when a new neighbor is detected, and cause LLDP packets to be transmitted at a shorter time interval than during normal operation of the protocol. The fast transmission period ensures that more than one LLDP packet is transmitted when a new neighbor is detected. The first transmission is immediate, and the subsequent transmissions occur at the specified fast transmission (TX) interval.
<range (1-3600)>	Integer	Enter a message fast transmit interval value with a default 1.
chassis-id-subtype		Enter to configure an ID for LLDP chassis subtype which is a unique address of any module. **NOTE:** Chassis ID value can be set only for the chassis-component and local system subtypes. For all other subtypes, it takes the value from the system automatically.
chassis-comp		Enter to configure the chassis identifier based on the value of entPhysicalAlias object for a chassis component
<string(255)>	Integer	Enter an ID value based on the value of entPhysicalAlias object.
if-alias		Enter to configure the chassis identifier based on the value of ifAlias for an interface on the chassis.
if-name		Enter to configure the chassis identifier based on the value of ifName object for an interface on the chassis
local		Enter to configure the chassis identifier based on a locally defined value.
<string(255)>	Integer	Enter an ID value for the local system subtype.
mac-addr		Enter to configure the chassis identifier based on the value of a unicast source address of a port on the chassis.
nw-addr		Enter to configure the chassis identifier based on the network address associated with a particular chassis. The encoded address is actually composed of two fields. The first field is a single octet, representing the IANA AddressFamilyNumbers value for the specific address type, and the second field is the network address value

Parameter	Type	Description
port-comp		Enter to configure the chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis.
<string(255)>	Integer	Enter an ID value based on the value of entPhysicalAlias object.
holdtime-multiplier		Enter to configure the holdtime-multiplier range, which is how long the receiving device holds an LLDP packet before discarding it.
<value(2-10)>	Integer	Enter a holdtime-multiplier value. It ranges from 2 to 10 with default of 4.
notification-interval		Enter to configure the time interval in which the local system generates a notification-event. In the specific interval, generating more than one notification-event is not possible.
<seconds(5-3600)>	Integer	Enter a value for the time interval in which the local system generates a notification-event. It ranges from 5 to 3600 with default of 5 seconds.
reinitialization-delay		Enter to configure the reinitialization delay time which is the minimum time an LLDP port will wait before reinitializing LLDP transmission.
<seconds(1-10)>	Integer	Enter a value for this reinitialization delay time. This value ranges from 1 to 10 seconds with a default of 2 seconds.
transmit-interval		Enter to configure the transmission interval in which the server sends the LLDP frames to the LLDP module.
<value(5-32768)>	Integer	Enter a value for the transmission interval. It ranges from 5 to 32768 with default of 30.
tx-delay		Enter to configure the transmit delay which is the minimum amount of delay between successive LLDP frame transmissions. **NOTE:** tx-delay should be less than or equal to 0.25 * Message Tx Interval
<value(1-8192)>	Integer	Enter a value for the transmit delay. It ranges from 1 to 8192 seconds with default of 2 seconds.
txCreditMax		Enter to configure the maximum number of consecutive LLDPDUs that can be transmitted at any time.
<value(1-10)>	Integer	Enter a value for maximum number of consecutive LLDPDUs. This value ranges from 1 to 10 with a default of 5.

Parameter	Type	Description
txFastInit		Enter to configure the value used to initialize the txFast variable which determines the number of transmissions that are made in fast transmission mode
<value(1-8)>	Integer	Enter a value for the number of LLDPDUs that are transmitted during a fast transmission period. This value ranges from 1 to 10 seconds with a default of 4 seconds.

Mode

Global Configuration Mode

Examples

iS5comm(config)# lldp MessageFastTx 3500

iS5comm(config)# lldp chassis-id-subtype chassis-comp IS5Comswitch

iS5comm(config)# lldp chassis-id-subtype if-alias

iS5comm (config)# lldp holdtime-multiplier 5

iS5comm(config)# lldp notification-interval 150

iS5comm(config)# lldp reinitialization-delay 4

iS5comm(config)# lldp transmit-interval 50

iS5comm(config)# lldp txCreditMax 3

iS5comm(config)# lldp txFastInit 3

19.4. lldp

To configure LLDP properties such as, on an interface, use the command **lldp** in Interface Configuration Mode. This command executes only if LLDP is started. The no form of the command resets all LLDP properties to their default values. This command can be executed only if LLDP is started.

lldp

```
lldp {Dest-mac <mac_addr>
 | med-location med-tlv-select elin-location location-id <string(10-25)>
 | med-tlv-select {ex-power-via-mdi | inventory-management | location-id |
med-capability | network-policy} [mac-addr <mac-addr>]
 | notification {remote-table-chg | mis-configuration {mac-addr <mac-addr>}}
```

```
 | port-id-subtype if-alias | if-name | local <string(255)> | mac-addr |
port-comp <string(255)>}

 | receive [mac-addr <mac-addr>]

 | tlv-select {basic-tlv {mgmt-addr {all | ipv4 <ucast_addr> | ipv6
<ipv6_addr>} | port-descr | sys-capab | sys-descr | sys-name} | dot1tlv
{link-aggregation | mgmt-vid | port-vlan-id | protocol-vlan-id {<vlan_id
(1-4094)> | all} | vid-usage-digest | vlan-name {<vlan_id (1-4094)> | all}}
[mac-addr <mac-addr>] | dot3tlv {link-aggregation | macphy-config |
max-framesize}

 | transmit [mac-addr <mac-addr>]
```

no lldp

```
no lldp {Dest-mac | med-location | med-tlv-select | notification | receive |
tlv-select | transmit}
```

Parameters

Parameter	Type	Description
Dest-mac		Enter to configure destination mac-address to be used by the LLDP agent for transmission on this port. **NOTE:** This command can be executed only for LLDP ver 2.
<mac_addr>		Enter a message fast transmit interval value (txFast).
med-location		Enter to configure the Location Identification TLV related configuration.
elin-location		Enter to configure the Emergency Location Information Number (ELIN) location subtype information advertised by the endpoint.
location-id		Enter for location information related configuration.
<string(10-25)>		Enter a location identification value.
med-tlv-select		Enter to configure the LLDP-MED TLV transmission on a given switch port. **NOTE:** MAC-address can be configured only if • LLDP version v2 is enabled • lldp dest-mac is configured
ex-power-via-mdi		Enter to configure the extended power via MDI TLV related transmission for the LLDP module.
inventory-management		Enter to configure the Inventory-management TLV related transmission for the LLDP module.
location-id		Enter to configure the Location identification TLV related transmission for the LLDP module
med-capability		Enter to configure the Med Capability TLV transmission for the LLDP module.
network-policy		Enter to configure the Network-policy TLV related transmission for the LLDP module.
mac-addr		Enter to configure the basic TLV transmission to use the MAC address as destination MAC address by the LLDP agent on the specified switch port.
<mac-addr>		Enter a destination MAC address.
notification		Enter to configure the control of the transmission of LLDP notifications.

Parameter	Type	Description
remote-table-chg		Enter to configure sending trap notification to NMS when remote table change occurs.
mis-configuration		Enter to configure sending trap notification to NMS when misconfiguration is identified.
mac-addr		Enter to configure the MAC address to be used as destination MAC address by the LLDP agent on the specified port
port-id-subtype		Enter to configure an ID for LLDP port subtype.
if-alias		Enter to configure the chassis identifier based on the value of ifAlias for an interface on the chassis.
if-name		Enter to configure the chassis identifier based on the value of ifName object for an interface on the chassis
local		Enter to configure the chassis identifier based on a locally defined value.
<string(255)>	Integer	Enter an ID value for the a chassis identifier
mac-addr		Enter to configure the LLDP port ID subtype and port ID value.
port-comp		Enter to configure the chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis.
<string(255)>	Integer	Enter an ID value based on the value of entPhysicalAlias object.
receive		Enter to configure to set LLDP admin status on an interface to Receive.
mac-addr		Enter to configure specifies the MAC destination address of the LLDP agent.
<mac-addr>		Enter a destination MAC address.
tlv-select		Enter to configure the TLV type configuration.
basic-tlv		Enter to set the basic TLV transmission configuration.
mgmt-addr		Enter to enable the basic TLV transmission to maintain the management addresses through which a management module can manage the system and allow the transmission on the current interface.
all		Enter to enable the transmission of a particular ipv4 address on the current interface.

Parameter	Type	Description
ipv4		Enter to enable the transmission of only configured IPv4 addresses.
<ucast_addr>		Enter an Unicast IP address. The format is A.B.C.D
ipv6		Enter to enable the transmission of only configured IPv6 addresses.
<ipv6_addr>		Enter an IPv6 address. The format is AAAA::BBBB.
port-descr		Enter to enable the basic TLV transmission for the administratively assigned description for the port.
sys-capab		Enter to enable the basic TLV transmission for the administratively assigned system name.
sys-descr		Enter to enable the basic TLV transmission for the administratively assigned system description. The system description includes system's hardware name and type, and system's operating software and its version.
sys-name		Enter to enable the system capabilities of the basic TLV transmission
dot1tlv		Enter to enable the basic TLV transmission for the administratively assigned description for the port.
link-aggregation		Enter to perform dot1 TLV configuration while transmitting the LLDP frames to the link-aggregation TLV. **NOTE:** This parameter can be set only when LLDP version is set as v2.
mgmt-vid		Enter to perform dot1 TLV configuration while transmitting the LLDP frames to the management TLV. **NOTE:** This parameter can be set only when LLDP version is set as v2.
port-vlan-id		Enter to specify the VLAN ID of the port that uniquely identifies a specific VLAN. This VLAN ID is associated with a specific group of protocols for the specific port
protocol-vlan-id		Enter to specify the protocol ID that represents a specific group of protocols that are associated together when assigning a VID to a frame. This group ID is associated with the specific port.
<vlan_id (1-4094)>		Enter to set the protocol id as the mentioned vlan id. This value ranges from 1 to 4094.
all		Enter to set the protocol ID to all.

Parameter	Type	Description
vid-usage-digest		Enter to perform dot1 TLV configuration while transmitting the LLDP frames to the VID usage digest TLV. **NOTE:** This parameter can be set only when LLDP version is set as v2.
vlan-name		Enter to specify the administratively assigned string, which is used to identify the VLAN.
<vlan_id (1-4094)>		Enter to set the protocol id as the mentioned vlan id. This value ranges from 1 to 4094.
all		Enter to set the protocol ID to all.
mac-addr		Enter to configure specifies the MAC destination address of the LLDP agent. **NOTE:** This parameter can be set only when LLDP version is set as v2.
<mac-addr>		Enter a destination MAC address.
dot3tlv		Enter to perform dot3 TLV configuration while transmitting the LLDP frames to the particular port apart from the basic settings.
link-aggregation		Enter to configure the link aggregation protocol statistics for each port on the device.
macphy-config		Enter to configure the physical MAC address of the TLV.
max-framesize		Enter to configure the maximum frame size of the TLV.
transmit		Enter to configure to set LLDP admin status on an interface to Transmit.
mac-addr		Enter to configure specifies the MAC destination address of the LLDP agent.
<mac-addr>		Enter a destination MAC address.

Mode

Interface Configuration Mode

Examples

iiS5comm(config-if)# lldp dest-mac 00:11:22:33:44:55

```
    % Dest-Mac address cannot be configured for lldp version1
```

iS5comm(config-if)# exit

iS5comm(config)# set lldp version v2

iS5comm (config-if)# lldp med-location elin-location location-id 12345678912345

iS5comm(config-if)# lldp med-tlv-select inventory-management

iS5comm(config-if)# lldp med-tlv-select location-id mac-address 00:01:03:04:06:07

iS5comm(config-if)# lldp med-tlv-select inventory-managementiS5comm(config-if)# lldp med-tlv-select location-id mac-address 00:01:03:04:06:07

iS5comm(config-if)# lldp notification remote-table-chg

iS5comm(config-if)# lldp port-id-subtype mac-addr

iS5comm(config-if)# lldp port-id-subtype local slot0/1

iS5comm(config-if)# lldp tlv-select basic-tlv port-descr

iS5comm(config-if)# lldp tlv-select dot1tlv port-vlan-id mac-address 00:11:22:33:44:55

iS5comm(config-if)# lldp tlv-select dot3tlv macphy-config

iS5comm(config-if)# lldp receive

iS5comm(config-if)# lldp transmit

iS5comm(config-if)# lldp med-tlv-select inventory-management

iS5comm(config-if)# lldp med-tlv-select location-id mac-address 00:01:03:04:06:07

19.5. set lldp

To enable or disable globally the LLDP feature on the switch, to enable tagging, and select a LLDP version, use the command **set lldp** in Global Configuration Mode.

set lldp

```
set lldp {disable | enable | tag status {enable | disable} | version {v1 |
v2}}
```

Parameters

Parameter	Type	Description
disable		Enter to disable LLDP feature in the switch. There will be no transmitting / receiving the LLDP packets between LLDP module and the server.This is the default.
enable		Enter to enable LLDP feature in the switch or to transmits /receive the LLDP packets between LLDP module and the server.
tag		Enter to set the transmitted LLDPDU (LLDP Data Units) to be tagged or untagged.
status		Enter to configure the status of the transmitted LLDPDU as tagged or not.
disable		Enter to disable tagging of the LLDPDU. Untagged LLDPDU do not carry a VLAN identifier as part of the Ethernet header.
enable		Enter to enable tagging of the LLDPDU. When the LLDP tag is enabled, the Tagged LLDP packets are transmitted on edge virtual bridge (EVB) uplink access ports (UAP), and untagged LLDP packets will be transmitted on the other ports. The configured management IP address is carried in the management address TLV of the LLDP packet.
version		Enter to determine the LLDP version to be used.
v1		Enter to enable LLDP 2005 version 1.
v2		Enter to enable LLDP 2009 version 2

Mode

Global Configuration Mode

Examples

iS5comm(config)# set lldp enable

iS5comm(config)# set lldp version v2

iS5comm (config)# set lldp tag status enable

19.6. set lldp-med

To enables or disables the LLDP-MED on the port, use the command **set lldp-med** in Interface Configuration Mode.

set lldp-med

```
set lldp-med {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enter to enable LLDP-MED on the port.
disable		Enter to disable LLDP-MED on the port.

Mode

Interface Configuration Mode

Examples

iS5comm (config-if)# set lldp-med enable

19.7. show lldp

To display the LLDP global configuration details to be initialized on an interface, use the command **show lldp** in Privileged EXEC Mode.

show lldp

```
show lldp [errors]
 [interface {Extreme-Ethernet <interface-id> | Gigabitethernet <inter-
face-id>}]
 [local {{Extreme-Ethernet <interface-id> | Gigabitethernet <interface-id>}
[mac-addr <mac-addr>]} [mgmt-addr]]
 [neighbors [Extreme-Ethernet <interface-id> | Gigabitethernet <inter-
face-id>}] [chassis-id <string(255)>] [detail]]
 [peers {Extreme-Ethernet <interface-id> | Gigabitethernet <interface-id>}
|chassis-id <string(255)>} [<mac-addr> [mgmt-addr]] [detail]
 [statistics]
 [traffic [{Extreme-Ethernet <interface-id> | Gigabitethernet <inter-
face-id>} [mac-addr <mac-addr>]}
```

Parameters

Parameter	Type	Description
errors		Enter to display the information about the errors such as memory allocation failures, queue overflows and table overflow
interface		Enter to display the information about interfaces where LLDP is enabled
Gigabitethernet		Enter to display gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to display the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-4> without spaces between Slot Number/Port Number. For example, 0/1.
local		Enter to display the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces
Gigabitethernet		Enter to display gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to display the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-4> without spaces between Slot Number/Port Number. For example, 0/1.
mac-addr		Enter to display information about neighbors for the specified destination MAC address of the LLDP agent.
<mac-addr>		Enter a destination MAC address.

Parameter	Type	Description
mgmt-addr		Enter to display information about the management addresses configured in the system and Tx enabled ports.
neighbors		Enter to display information about neighbors on an interface or all interfaces.
Gigabitethernet		Enter to display gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to display the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-4> without spaces between Slot Number/Port Number. For example, 0/1.
chassis-id		Enter to display LLDP Neighbor information for the specified chassis identifier value.
<string(255)>		Enter a value for the specified chassis identifier value. This value is a string value with a maximum size of 255.
detail		Enter to display the information obtained from all received TLVs.
peers		Enter to display peer related information.
Gigabitethernet		Enter to display gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to display the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-4> without spaces between Slot Number/Port Number. For example, 0/1.

Parameter	Type	Description
chassis-id		Enter to display LLDP Neighbor information for the specified chassis identifier value.
<string(255)>		Enter a value for the specified chassis identifier value. This value is a string value with a maximum size of 255.
mac-addr		Enter to display information about neighbors for the specified destination MAC address of the LLDP agent.
<mac-addr>		Enter a destination MAC address.
detail		Enter to display the information obtained from all received TLVs.
statistics		Enter to display the LLDP remote table statistics information
traffic		Enter to display LLDP counters on all interfaces or on a specific interface. This includes the following: • Total Frames Out • Total Entries Aged • Total Frames In • Total Frames Received In Error • Total Frames Discarded • Total TLVS Unrecognized • Total TLVs Discarded
Gigabitethernet		Enter to display gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to display the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to display a specific slot number / port number. The format is <0>/<1-4> without spaces between Slot Number/Port Number. For example, 0/1.
mac-addr		Enter to display information about neighbors for the specified destination MAC address of the LLDP agent.
<mac-addr>		Enter a destination MAC address.

Mode

Privileged EXEC Mode

Examples

iS5comm# show lldp

```
LLDP is enabled
LLDP Version                        : v1
Transmit Interval                   : 50
Holdtime Multiplier                 : 4
Reinitialization Delay              : 2
Tx Delay                            : 2
Notification Interval               : 5
Chassis Id SubType                  : Mac Address
Chassis Id                          : e8:e8:75:90:0b:01
LLDP Tag Status                     : disabled
Configured Management Ipv4 Address  : 0.0.0.0Configured Management Ipv6
Address  : ::
```

iS5comm# show lldp interface gigabitethernet 0/1

```
0/1:
Tx State            : Enabled
Rx State            : Enabled
Tx SEM State        : INITIALIZE
Rx SEM State        : WAIT PORT OPERATIONAL
Notification Status : Disabled
Notification Type   : Mis-configuration
DestinationMacAddr  : 01:80:c2:00:00:0e
```

iS5comm# show lldp local (only gi 0/1 shown below)

```
Capability Codes   :(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS
Cable Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Chassis Id SubType            : Mac Address
Chassis Id                    : e8:e8:75:90:0b:01
System Name                   : iS5com
System Description            : iS5com
iBiome Software version :1.2.17, Raptor L3 Switch
System Capabilities Supported : B,R
System Capabilities Enabled   : B,R
-LLDP-MED Info
```

```
Device Class                  : Network Connectivity
LLDP-MED Inventory Info
Hardware Revision             : 1531-0001-B02
Firmware Revision             : 6.7.2
Software Revision             : 6.2.0
Serial Number                 :
Manufacturer Name             : iS5Com
Model Name                    :
Asset Id                      : DummyId

LLDP-MED PoE Info
Power Device Type             : PSE Device
Power Source                  : Primary

Gi0/1 :
Port Id SubType               : Interface Alias
Port Id                       : Gi0/1
Port Description              : Ethernet Interface Port 01
Enabled Tx Tlvs         : Port Description, System Name,
System Description, System Capability,
Management AddressExtended 802.3 TLV Info
-MAC PHY Configuration & Status
Auto-Neg Support & Status     : Not Supported, Enabled
Advertised Capability Bits    : 0000
Operational MAU Type          : 0
-Link Aggregation
Capability & Status           : Not Capable, Not In
AggregationAggregated Port Id           : 0
-Maximum Frame Size           : 1500

Extended 802.1 TLV Info-Port VLAN Id                : 1
-Port & Protocol VLAN Id
Protocol VLAN Id     Support    Protocol VLAN Status
TxStatus----------------     -------    --------------------
--------
0                    Supported  Enabled                  Disabled
-Vlan NameVlan Id        Vlan Name
TxStatus-------        ---------                          --------
1                                                Disabled
LLDP-MED Admin Status         : Disabled
-LLDP-MED Capability TLV
```

```
    LLDP-MED Tx Supported         : MedCapability, NetworkPolicy,
    LocationIdentity,
    Ex-PowerViaMDI-PSE, Inventory
    LLDP-MED Tx Enabled           :

    -LLDP-MED Network Policy TLV
    Application Type              :
    Unknown Policy Flag           :
    VlanType                      :
    VlanID                        :
    Priority                      :
    Dscp                          :

    -LLDP-MED Location TLV Info
    Location Subtype              :
    Location Info                 :

    -LLDP-MED Ex-PowerViaMDI TLV Info
    Power Priority                : Critical
    Power Value                   : 1000
```

iS5comm# show lldp local mgmt-addr

```
    Management Address              TxEnabledPorts
    ------------------              --------------
    192.168.10.1                    Gi0/1, Gi0/2, Gi0/3, Gi0/4
    Gi0/5, Gi0/6, Gi0/7, Gi0/8
    Gi0/9, Gi0/10, Gi0/11, Gi0/12
    Gi0/13, Gi0/14, Gi0/15, Gi0/16
    Gi0/17, Gi0/18, Gi0/19, Gi0/20
    Gi0/21, Gi0/22, Gi0/23, Gi0/24
```

iS5comm# show lldp neighbors

```
    Capability Codes   :(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS
    Cable Device,(W) WLAN Access Point, (P) Repeater, (S) Station, (O)
    OtherChassis ID          Local Intf    Hold-time   Capability      Port
    Id----------          ----------    ---------   ----------      -------
    54:e1:ad:07:0d:87    Gi0/10        3601
    54:e1:ad:07:0d:87

    Total Entries Displayed : 1
```

iS5comm# show lldp peers gi 0/1

```
    Capability Codes   :
```

```
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

    Chassis ID           Local Intf    Hold-time   Capability      Port
    Id----------           ----------    ---------   ----------      -------
    Total Entries Displayed : 0
```

iS5comm# show lldp traffic

```
    Total Frames Out : 19
    Total Tagged Frames Out : 0
    Total Entries Aged : 0
    Total Frames In : 1
    Total Frames Received In Error : 0
    Total Frames Discarded : 0
    Total TLVS Unrecognized : 0
    Total TLVs Discarded : 0
    Total PDU length error Drops : 0
    Total LLDP-MED Frames Out : 0
    Total LLDP-MED Frames In : 0
    Total LLDP-MED Frames Discarded : 0
    Total LLDP-MED TLVs Discarded : 1
    Total Media Capability TLVs Discarded : 1
    Total Network Policy TLVs Discarded : 0
    Total Inventory TLVs Discarded : 0
    Total Location TLVs Discarded : 0
    Total Ex-PowerViaMDI TLVs Discarded : 0
    Med-Capability TLV Discard Reason : Not Applicable
    Nw-Policy TLV Discard Reason : Not Applicable
    Inventory TLV Discard Reason : Not Applicable
    Location-ID TLV Discard Reason : Not Applicable
    Ex-PowerViaMDI TLV Discard Reason : Not Applicable
```

PNAC

20. PNAC

PNAC (Port Based Network Access Control) is a portable implementation of the IEEE Std 802.1x PNAC.

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are properly authenticated. The authentication server authenticates each client connected to a port before making available any services offered by the device or the network.

Until the client is authenticated, IEEE 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

When the command **aaa authentication dot1x default** is used to enable the dot1x local authentication or RADIUS server / TACACS PLUS server (authentication server) based remote authentication method for all ports, the router initiates authentication

- when the link state changes from down to up, or
- periodically if the port remains up and unauthenticated.

When the device that requests access to LAN and a switch (supplicant) supplies its identity, the router begins its role as the intermediary, passing EAP frames between the supplicant and the authentication server until authentication succeeds or fails.

20.1. aaa authentication dot1x default

To configure the dot1x local authentication or RADIUS server /TACACS+ server-based remote authentication method for all ports, use the command **aaa authentication dot1x default** in Global Configuration Mode.

aaa authentication dot1x default

```
aaa authentication dot1x default {group {radius | tacacs+ | tacacsplus} |
local}
```

Parameters

Parameter	Type	Description
group		Enter to configure server based authentication.
radius		Enter to configure RADIUS as the authentication server. RADIUS offers Authentication, Authorization and Accounting management for computers to access a network.
tacacs+		Enter to configure TACACS+ as the authentication server. This feature has been included to adhere to the Industry Standard CLI syntax.
tacacsplus		Enter to configure TACACS+ as the remote authentication server. Tacacs offers Authentication, Authorization and Accounting management for computers to access a network. This is mainly used for backward compatibility.
local		Enter to configure local authentication as authentication mode. It provides authentication based on user names and password using EAP-MD5 authentication mechanism.

Mode

Global Configuration Mode

Default

local

Examples

iS5comm(config)# aaa authentication dot1x default group radius

20.2. dot1x

To set the dot1x network access server (NAS) ID, use the command **dot1x** in Global Configuration Mode. The no form of the command resets periodic sync timer and max alive count for distributed PNAC to their default values, deletes an entry from the dot1x authentication server database, and disables dot1x in the switch.

dot1x

```
dot1x {distributed {max-keep-alive-count <short<0-300)> | periodic-sync-time
<short(1-5))>}
 | init {aa:aa:aa:aa:aa:aa | session-reauth aa:aa:aa:aa:aa:aa}
```

```
 | init-session aa:aa:aa:aa:aa:aa

 | local-database <username> password <string (20)> permission {allow |
deny} [auth-timeout <(value(1-7200)>] [interface {Extreme-Ethernet <inter-
face-id> | gigabitethernet <interface-id>}]

 | mode {centralized | distributed}

 | system-auth-control}
```

no dot1x

```
no dot1x {distributed | local-database | system-auth-control}
```

Parameters

Parameter	Type	Description
distributed		Enter to configure periodic sync timer and max alive count for distributed PNAC (D-PNAC).
periodic-sync-time		Enter to configure the D-PNAC sync timer used in distributed -PNAC. The Periodic sync timer is used to configure the transmission interval of D-PNAC periodic-sync PDUs. In the master node, this timer expiry is used to identify the slave down and remove the slave node information. **NOTE:** The configured value of this timer is applicable only from the next start/re-start of the timer. **NOTE:** If the configured value is '0', then no periodic-sync messages will be sent from that D-PNAC node.
<short<0-300)>	Integer	Enter a value for the periodic sync timer. This runs individually in each D-PNAC node, and the value ranges from 0 to 300 seconds.
max-keep-alive-count		Enter to configure keep alive mechanism when distributed-PNAC status is enabled. This is maintained by Master Node. **NOTE:** The keep alive count of all remote D-PNAC nodes is incremented every time when the periodic-sync timer expires. **NOTE:** The value resets to zero for a particular D-PNAC node, only on receiving periodic-sync/ event-update message from that particular remote D-PNAC node. **NOTE:** If keep alive count of any of the Remote D-PNAC node reaches the maximum keep alive count, the Remote D-PNAC node is declared as operationally down/dead
<short<1-5)>	String	Enter a value for the keep alive count. The value ranges from 1 to 5.
init		Enter to initiate dot1x re-authentication session for the specified MAC address. When the supplicant has exceeded the time limit for accessing the protected network, the supplicant is forced for re-authentication. This is to ensure that the supplicant is the same entity that was initially authenticated. **NOTE:** On execution of this command, the authenticator initiates re-authentication for the specified supplicant MAC address.
aa:aa:aa:aa:aa:aa		Enter a MAC address of the supplicant.
session-reaut		Enter to configure Reauthentication session initiation.

Parameter	Type	Description
init-session		Enter to initiate dot1x authentication session for the given MAC address of the supplicant. The supplicant requests for access to the protected network. It sends EAPOL (Extensible Authentication Protocol) frames to the authenticator. When the supplicant is authorized by the remote server, the session is initiated. **NOTE:** The supplicant MAC address must be authorized prior to the execution of this command.
aa:aa:aa:aa:aa:aa		Enter a MAC address of the supplicant.
local-database		Enter to configure dot1x authentication server local database with user name and password.
<username>		Enter an user name for the new entry in the database.
password		Enter to configure dot1x authentication server local database with user name and password.
<string (20)>		Enter a password for the user.
permission		Enter to configure the permission for access for the user on a set of ports.
allow		Enter to provide the user with access.
deny		Enter to deny access to the user.
interface		Enter to configure the interface type for the specified interface.
Gigabitethernet		Enter to configure gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to configure a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to configure the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to configure a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.

Parameter	Type	Description
mode		Enter to set the PNAC (Port based Network Access Control) mode as centralized or distributed- PNAC feature in the system. D-PNAC comprises of Master and Slave functionality. It is an extension of PNAC which provides ability to extend the access control in the system working over a single card to multiple cards with each operating in a distributed fashion.
centralized		Enter to configure PNAC.
distributed		Enter to configure distributed- PNAC.
system-auth-control		Enter to enable dot1x in the switch. The dot1x is an authentication mechanism. It acts as mediator between the authentication server and the supplicant (client). If the client accesses the protected resources, it contacts the authenticator with EAPOL frames.

Mode

Global Configuration Mode

Default

dot1x is enabled

Examples

iS5comm(config)# dot1x distributed periodic-sync-time 300 max-keep-alive-count 2

iS5comm(config)# dot1x mode distributed

iS5comm(config) dot1x init session-reauth 00:1e:58:a7:f3:93

iS5comm(config)# dot1x init-session 00:1e:58:a7:f3:93

iS5comm(config)# dot1x local-database IS5Com password admin123 permission allow auth-timeout 6000

iS5comm(config)# dot1x system-auth-control

20.3. dot1x

To clear dot1x statistics information, initialize the state machines, set up the environment for fresh authentication, and initiate re-authentication of all dot1x-enabled ports or the specified dot1x-enabled port, use the command **dot1x** in Privileged EXEC Mode.

dot1x

```
clear statistics [interface {Extreme-Ethernet <interface-id> | gigabiteth-
ernet <interface-id>}] [mac-statistics address <mac_addr>]

 | initialize [interface {Extreme-Ethernet <interface-id> | gigabitethernet
<interface-id>}]

 | re-authenticate [interface {Extreme-Ethernet <interface-id> | gigabiteth-
ernet <interface-id>}
```

Parameters

Parameter	Type	Description
clear		Enter to start clearing statistics information for the switch or the specified interface.
statistics		Enter to configure statistics related configuration.
interface		Enter to configure the interface type for the specified interface.
Gigabitethernet		Enter to configure Gigabit Ethernet type of interface. Gigabit Ethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to configure a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to configure the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gbits per second and only full duplex links
<interface-id>		Enter to configure a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
mac-statistic		Enter to configure clearing dot1x MAC statistics information for all MAC sessions or the specified MAC address.
address		Enter to configure specific MAC address for which the dot1x information will be cleared.
<mac_addr>		Enter a MAC address for which the dot1x information will be cleared.
initialize		Enter to configure initializing of the state machines and setting up the environment for fresh authentication. This initiates re-authentication of all dot1x-enabled ports or the specified dot1x-enabled port. Re-authentication is manually configured if periodic re-authentication is not enabled. Re-authentication is requested by the authentication server from the supplicant to furnish the identity without waiting for the configured number of seconds (re-authperiod). If no interface is specified, re-authentication is initiated on all dot1x ports This command is a standardized implementation of the existing command; dot1x re-authenticate. It operates similar to the existing command.

Parameter	Type	Description
re-authenticate		Enter to configure initiating of re-authentication of all dot1x-enabled ports or the specified dot1x-enabled port. This initializes the state machines and sets up the environment for fresh authentication. Re-authentication is manually configured if periodic re-authentication is not enabled. Re-authentication is requested by the authentication server to the supplicant to furnish the identity without waiting for the configured number of seconds (re-authperiod). If no interface is specified, re-authentication is initiated on all dot1x ports

Mode

Privileged EXEC Mode

Default

dot1x is enabled

Examples

iS5comm# dot1x clear statistics

```
Interface and MAC Statistics cleared successfully
```

iS5comm# dot1x clear statistics interface gigabitethernet 0/1

```
Interface Statistics cleared successfully
```

iS5comm# dot1x clear statistics mac-statistics address 00:1e:58:a7:f3:93

```
MAC Statistics cleared successfully
```

iS5comm# dot1x re-authenticate interface gigabitethernet 0/1

iS5comm# dot1x initialize interface gigabitethernet 0/1

20.4. dot1x

To set the PNAC related information or configure the dot1x parameters for a specified port, use the command **dot1x** in Interface Configuration Mode. The no form of the command resets the parameters to their default value or to no authentication, and disables periodic re-authentication from authenticator to client.

dot1x

```
dot1x {access-control {active | inactive}
 | auth-mode {port-based | mac-based}
```

```
 | control-direction {in | both}
 | default
 | disable
 | enable
 | host-mode {multi-host | single-host}
 | max-req <count(1-10)>
 | max-start <count (1-65535)>
 | port-control {auto | force-authorized} | force-unauthorized}
 | reauth-max <count(1-10)>
 | reauthentication
 | timeout {auth-period | held-period | quiet-period | reauth-period |
server-timeout | start-period | supp-timeout | tx-period} <value (1-65535)>
```

no dot1x

```
no dot1x {access-control | auth-mode | control-direction | max-req |
max-start | port-control | reauth-max | reauthentication | timeout
```

Parameters

Parameter	Type	Description
access-control		Enter to configure the supplicant access control. This setting is for the application of the Supplicant authorization state when the port is operating as both Supplicant and Authenticator.
active		Enter to configure the port to apply both the Supplicant authorization state and Authenticator authorization state
inactive		Enter to configure the port to use only the Authenticator authorization state to restrict access to the port and not the Supplicant authorization state. This is the default option
auth-mode		Enter to configure the authentication mode of a port as either port-based (which is also known as multi-host) or mac-based (which is also known as single-host). Port based authentication has different modes of authentication. MAC based authentication allows secured mac addresses to pass through the port. Non-secure MAC addresses are dropped.
port-based		Enter to configure the port's authentication mode as port-based. The port authenticates the host to use the restricted resource. The port state is changed to authorize. The traffic flows through the port without any access restriction till any event that causes the port state to become unauthorized. This is default option.
mac-based		Enter to configure the port's authentication mode as MAC-based. Upon receiving tagged/untagged data/control frames from the CFA Module, it checks if the source MAC is present in the Authenticator Session Table and if it is authorized. • If it is present in the table and is authorized, the result is passed to CFA, which then forwards the frame to the appropriate destination module. • If it is present in the table but not authorized, the CFA Module is intimated and the frame is dropped at the CFA Module. • If neither of the above occurs, the Authenticator will initiate a new authentication session for that source MAC address and return the unauthorized status to the CFA Module, which then drops the frame.

Parameter	Type	Description
control-direction		Enter to configure configures port control direction. The switch port authenticates incoming packets and outgoing packets. The direction can be configured manually by selecting either in or both.
in		Enter to configure the port to authenticate only the incoming packets.
both		Enter to configure the port to authenticate both incoming and outgoing packets. This is the default option.
default		Enter to configure dot1x with default values for this port. The previous configurations on this port are reset to the default values. These details are not displayed but are the basic settings for a port.
disable		Enter to disable dot1x on the specified port.
enable		Enter to enable dot1x on the specified port.
host-mode		Enter to configure the port authentication mode of a port as either multi-host (which is also known as port-based) or single-host (which is also known as mac-based). Multi host authentication has different Modes of authentication. Single host authentication allows secured mac addresses to pass through the port. Non-secure mac addresses are dropped. ***NOTE:*** *This command is a standardized implementation of the existing command; dot1x auth-mode. It operates similar to the existing command.*
multi-host		Enter to configure the port to multi host authentication mode and perform port-based authentication. With this option, more than one host can be connected to the port using an Ethernet hub attached to the port. This is the default option.
single-host		Enter to configure the port to single host authentication Mode and perform MAC-based authentication. With this option, only one host can be connected to the port. **NOTE:** To configure the auth Mode of a port as single-host, port control of the port must be set as auto.
max-req		Enter to set the maximum number of EAP (Extensible Authentication Protocol) retries to the client by the authenticator before restarting authentication process.

Parameter	Type	Description
<count (1-10)>	Integer	Enter a value for maximum number of EAP retries to the client by the authenticator before restarting authentication process. The count value ranges between 1 and 10. The default is 2.
max-start		Enter to set the maximum number of EAPOL retries to the authenticator.
<count (1-65535)>	Integer	Enter a value for maximum number of EAP retries to the authenticator. The count value ranges between 1 and 65535. The default is 3.
port-control		Enter to configure the authenticator port control parameter. The dot1x exercises port based authentication to increase the security of the network. The different modes employed to the ports offer varied access levels. The 802.1x protocol is supported on both Layer 2 static-access ports and Layer 3 routed ports.
auto		Enter to configure the 802.1x authentication process in this port. Causes the port to begin the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The switch can uniquely identify each client attempting to access the network by the client's MAC address.
force-authorized		Enter to configure the port to allow all traffic through this port. Disables 802.1x authentication and causes the port to transit to the authorized state without requiring authentication exchange. The port transmits and receives normal traffic without 802.1x-based authentication of the client. This is the default option.
force-unauthorized		Enter to configure the port to block all traffic through this port. Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.

Parameter	Type	Description
reauth-max		Enter to configure the maximum number of EAP retries to the client. This variable can be tuned to make the port as unauthorized if the supplicant is not available when re-authentication reaches the maximum retry. Lower the value, the port is made unauthorized sooner.
<count (1-10)>	Integer	Enter a value for maximum number of EAP retries to the client. The count value ranges between 1 and 10. The default is 2.
reauthentication		Enter to enable periodic re-authentication from authenticator to client. The periodic re-authentication is requested to ensure if the same supplicant is accessing the protected resources. The amount of time between periodic re-authentication attempts can be configured manually. **NOTE:** This command will execute only if the authenticator port control parameter is auto.
timeout		Enter to set the dot1x timers. The timer module manages timers, creates memory pool for timers, creates timer list, starts and stops timer. It provides handlers to respective expired timers. **NOTE:** Only one timer can be configured using this command, that is, the user can configure either the quiet-period or tx-period, but not both.
auth-period		Enter to configure the number of seconds that the supplicant waits before timing-out the authenticator. The default is 30 seconds.
held-period		Enter to configure the number of seconds that the supplicant waits before trying to acquire the authenticator.The default is 60 seconds.
quiet-period		Enter to configure the quiet-period or the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The default is 60 seconds.
reauth-period		Enter to configure the reath-period or the number of seconds between re-authentication attempts. The default is 3600 seconds.
server-timeout		Enter to configure the number of seconds that the switch waits for the retransmission of packets to the authentication server. The default is 30 seconds.

Parameter	Type	Description
start-period		Enter to configure the number of seconds that the supplicant waits between successive retries to the authenticator. The default is 30 seconds.
supp-timeout		Enter to configure the time that the switch waits for the retransmission of packets to the client. The default is 30 seconds.
tx-period		Enter to configure the number of seconds that the switch waits for a response to an EAP-request/identity frame, from the client before retransmitting the request. The default is 30 seconds.
<count ((1-65535)>	Integer	Enter a value for maximum number of EAP retries to the client. The count value ranges between 1 and 65535.

Mode

Interface Configuration Mode

Examples

iS5comm (config-if)# dot1x access-control active

iS5comm (config-if)# dot1x auth-mode mac-based

iS5comm(config-if)# dot1x control-direction in

iS5comm(config-if)# dot1x default

```
    Setting the Default Configuration for Dot1x on this interface
```

iS5comm(config-if)# dot1x disable

iS5comm(config-if)# dot1x enable

iS5comm(config-if)# dot1x host-mode single-host

iS5comm(config-if)# dot1x max-req 5

iS5comm(config-if)# dot1x max-start 2

iS5comm(config-if)# dot1x port-control auto

iS5comm(config-if)# dot1x reauth-max 5

iS5comm(config-if)# dot1x reauthentication

iS5comm(config-if)# dot1x timeout quiet-period 30

20.5. debug dot1x

To enable debugging of dot1x module, use the command **debug dot1x** in Privileged EXEC Mode. The no form of the command disables debugging of dot1x module.

debug dot1x

```
debug dot1x {all | errors | events | packets | redundancy | registry |
state-machine}
```

no debug dot1x

```
no debug dot1x {all | errors | events | packets | redundancy | registry |
state-machine}
```

Parameters

Parameter	Type	Description
`all`		Enter to configure generating of all dot1x debug messages.
`errors`		Enter to configure generating of debug statements for all failure traces of the below mentioned traces.
`events`		Enter to configure generating of debug statements for event handling traces. This trace is generated when there is a failure in state machine or event processing.
`packets`		Enter to configure generating of debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.
`redundancy`		Enter to configure generating of debug statements for redundancy code flow traces. This trace is generated when there is a failure in redundancy processing.
`registry`		Enter to configure generating of debug statements fordot1x registry debug traces.
`state-machine`		Enter to configure generating of debug statements for state machine handling traces. This trace is generated when there is an error condition in State Machine.

Mode

Privileged EXEC Mode

Default

Events Debugging is enabled

Examples

iS5comm# debug dot1x all

20.6. show dot1x

To display dot1x information, distributed dot1x authentication status and statistics information for the dot1x enabled ports, or distributed dot1x general information such as PNAC status, role played, periodic synchronous time, and maximum keep alive count, use the command **show dot1x** in Privileged EXEC Mode.

show dot1x

```
show dot1x [all]
 [distributed {auth-status slot <slot number (0-2147483647)> | detail |
statistics slot <slot number (0-2147483647)>}]
 [interface {Extreme-Ethernet <interface-id> | gigabitethernet <inter-
face-id>}]
 [local-database]
 [mac-info address <mac_addr (aa:bb:cc:dd:ee:ff)>]
 [mac-statistics address <mac_addr (aa:bb:cc:dd:ee:ff)>]
 [statistics [interface {Extreme-Ethernet <interface-id> | gigabitethernet
<interface-id>}]
 [supplicant-statistics [interface {Extreme-Ethernet <interface-id> | giga-
bitethernet <interface-id>}]
```

Parameters

Parameter	Type	Description
distributed		Enter to display distributed dot1x authentication status and statistics information for the dot1x enabled port.
auth-status		Enter to display the authentication status of each port belonging to the slot.
slot		Enter to identify the slot identifier related information to be displayed.
<slot number (0-2147483647)>	Integer	Enter a slot identifier to be displayed. The range is from 0 to 2147483647.
detail		Enter to display Gigabitet Ethernet type of interface. Gigabit Ethertype is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
statistics		Enter to display a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
slot		Enter to identify the slot identifier related information to be displayed.
<slot number (0-2147483647)>	Integer	Enter a slot identifier to be displayed. The range is from 0 to 2147483647.
interface		Enter to display the dot1x parameters for the specified interface.
Extreme-Ethernet		Enter to configure the Extreme-Ethernet type of interface to be displayed. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gbits per second and only full duplex links
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Gigabitethernet		Enter to configure Gigabit Ethernet type of interface to be displayed. Gigabit Ethernet is a version of LAN standard architecture that supports data transfer up to 1 Gbit per second.
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
mac-info		Enter to display dot1x information for all MAC sessions or the specified MAC address.

Parameter	Type	Description
address		Enter to configure having specific MAC address displayed.
<mac_addr>		Enter a MAC address for which the dot1x information will be displayed. The format is aa.aa.aa.aa.aa.aa.
mac-statistics		Enter to display dot1x MAC statistic for all MAC session or the specified MAC address.
address		Enter to configure having specific MAC address displayed.
<mac_addr>		Enter a MAC address for which the dot1x information will be displayed. The format is aa.aa.aa.aa.aa.aa.
statistics		Enter to display dot1x authenticator port statistics parameters for the switch or the specified interface.
interface		Enter to display the dot1x parameters for the specified interface.
Extreme-Ethernet		Enter to configure the Extreme-Ethernet type of interface to be displayed. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links.
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Gigabitethernet		Enter to configure Gigabit Ethernet type of interface to be displayed. Gigabit Ethernet is a version of LAN standard architecture that supports data transfer up to 1 Gbit per second.
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
supplicant-statistics		Enter to display dot1x supplicant statistics parameters for the switch or the specified interface.
interface		Enter to display the dot1x parameters for the specified interface.
Extreme-Ethernet		Enter to configure the Extreme-Ethernet type of interface to be displayed. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.

Parameter	Type	Description
Gigabitethernet		Enter to configure Gigabit Ethernet type of interface to be displayed. Gigabit Ethernet is a version of LAN standard architecture that supports data transfer up to 1 Gbit per second.
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.

Mode

Privileged EXEC Mode

Default

dot1x is enabled

Examples

iS5comm# show dot1x

```
    Sysauthcontrol                    = Enabled
    Module Oper Status                = Enabled
    Dot1x Protocol Version            = 2
    Dot1x Authentication Method       = Radius
    Nas ID                            = Identifier
```

iS5comm# show dot1x local-database

```
    PNAC Authentication Users Database
```

iS5comm# show dot1x all (only Gi0/1 shown)

```
    Dot1x Info for Gi0/1----------------------
    AuthMode              = PORT-BASED
    AuthPaeStatus         = ENABLED
    PortStatus            = AUTHORIZED
    AccessControl         = INACTIVE
    AuthSM State          = INITIALIZE
    SuppSM State          = DISCONNECTED
    BendSM State          = INITIALIZE
    AuthPortStatus        = AUTHORIZED
    SuppPortStatus        = UNAUTHORIZED
    AdminControlDirection = BOTH
    OperControlDirection  = BOTH
```

```
MaxReq                = 2
ReAuthMax             = 2
Port Control          = Force Authorized
QuietPeriod           = 60 Seconds
Re-authentication     = Disabled
ReAuthPeriod          = 3600 Seconds
ServerTimeout         = 30 Seconds
SuppTimeout           = 30 Seconds
Tx Period             = 30 Second
```

iS5comm# show dot1x distributed auth-status

```
DPNAC Authentication Information: Slot 0
-------------------------------------------------
             Port         Authentication   Control
Port       Property     Status           Direction
--------   ---------    ---------------  ------------
Gi0/1      Local       Authorized       BOTH
DPNAC Authentication Information: Slot 1
-------------------------------------------------
             Port         Authentication   Control
Port       Property     Status           Direction
--------   ---------    ---------------  ------------
Gi1/1      Remote       Authorized       BOTH
```

iS5comm # show dot1x distributed detail

```
DPNAC Detail information
-------------------------
PNAC Status              : Centralized
Role-Played              : None
Periodic Sync-Timer      : 300 Seconds
Maximum Keep Alive Count : 2
```

20.7. set nas-id

To set the dot1x network access server (NAS) ID, use the command **set nas-id** in Global Configuration Mode.

set nas-id

```
set nas-id <identifier>
```

Parameters

Parameter	Type	Description
<identifier>	String	Enter a value for dot1x network access server (NAS) ID. The NAS ID is set in the RADIUS packets sent to the Remote Authentication Server. The maximum length of the string is 16.

Mode

Global Configuration Mode

Default

fsNas1

Prerequisites

NAS ID can be configured only if the remote authentication server is RADIUS or TACACS.

Examples

iS5comm(config)# set nas-id Identifier

VLAN

21. VLAN

VLANs (Virtual LANs) can be viewed as a group of devices on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment. That is, in VLAN, a network of computers behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, and that make them extremely flexible.

VLAN provides the following benefits for switched LANs:

- Improved administration efficiency
- Optimized broadcast/multicast activity
- Enhanced network security

The prompt for the Config VLAN mode is:

iS5comm(config-vlan)#

21.1. base

To configure the base mode as 802.1Q vlan-aware bridge mode in which the VLAN feature should operate on the switch or set the bridge mode as transparent, use the command **base** in Global Configuration Mode. This configuration is globally applied on all ports of the switch.

base

```
base bridge-mode {dot1d-bridge dot1q-vlan}
```

Parameters

Parameter	Type	Description
`bridge-mode`		Enter for bridge mode related configuration.
`dot1d-bridge`		Enter to configure the bridge mode as transparent.
`dot1q-vlan`		Enter to configure the bridge mode as VLAN-aware bridge.

Mode

Global Configuration Mode

Default

dot1q-vlan (VLAN-aware bridging)

Prerequisites

The VLAN mode can be configured, only if the VLAN switching feature is started and enabled in the switch.

Examples

iS5comm(config)# base bridge-mode dot1q-bridge

21.2. clear garp counters

To clear GARP counters for all ports on the switch, use the command **clear garp counters** in Global Configuration Mode.

clear garp counters

```
clear garp counters {all | port <ifXtype> <ifnum>}
```

Parameters

Parameter	Type	Description
`all`		Enter to specify clearing all port information on the switch.
`port`		Enter to configure the GARP counters port's details. The unicast packets received only on this specified port are processed.
`<ifXtype>`		Enter to set the type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
`<ifnum>`		Enter to set the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided, for interface types internal-lan and port-channel.

Examples

iS5comm (config)# clear garp counters all

21.3. clear mac-address-table

To clear the dynamically learnt MAC Addresses, use the command **clear mac-address-table** in Global Configuration Mode.

clear mac-address-table

```
clear mac-address-table {dynamic [interface {port-channel <port-channel-id
(1-65535)> | {Extreme-Ethernet <interface-id> | gigabitethernet <inter-
face-id>} [vlan <vlan_vfi_id>] | remote}
```

Parameters

Parameter	Type	Description
dynamic		Enter to clear dynamically learnt MAC Addresses.
interface		Enter to clear the FDB entries for the specified type of interface. The interface can beExtreme-Ethernet and Gigabitethernet.
port-channel		Enter to clear the FDB entries for the specified port channel interface. Port-Channel are logical interfaces that represents an aggregator which contains several ports aggregated together.
<port-channel-id (1-65535)>	Integer	Enter a value to specify a port channel interface. This value ranges from 1 to 65535.
Extreme-Ethernet		Enter to configure the Extreme-Ethernet type of interface to be cleared. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to configure a specific slot number / port number to be cleared. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Gigabitethernet		Enter to configure gigabitetethernet type of interface to be cleared. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to configure a specific slot number / port number to be cleared. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
vlan		Enter to clear the FDB entries for the specified VLAN / VFI ID.

Parameter	Type	Description
<vlan_vfi_id>	Integer	Enter a value for the interface identifier of the specified type of interface. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan ID is provided, for interface types i-lan. • <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535. **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW. **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range
remote		Enter to clear all remote FDB entries.

Mode

Global Configuration Mode

Examples

iS5comm (config) # clear mac-address-table dynamic

21.4. clear vlan statistics

To clear VLAN counters that maintain statistics information on a per VLAN basis, use the command **clear vlan statistics** in Global Configuration Mode. The counter is cleared for all available VLANs or for the

specified VLAN. The statistics information contains number of unicast, broadcast and unknown unicast packets flooded.

clear vlan statistics

```
clear vlan statistics [vlan <vlan_vfi_id>]
```

Parameters

Parameter	Type	Description
vlan		Enter to configure a VLAN / VFI ID.
<vlan_vfi_id>	Integer	Enter a value for VLAN or VFI ID: • <vlan –id> - This is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id>- VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535 **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

Mode

Global Configuration Mode

Prerequisites

The information is the VLAN counters can be deleted, only if the VLAN switching feature is started and enabled in the switch.

Examples

iS5comm (config)# clear vlan statistics vlan 1

21.5. debug garp

To enable the tracing of the GARP sub module as per the configured debug levels, use the command **debug garp** in Privileged EXEC Mode. This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled).The no form of the command disables the tracing of the GARP sub module as per the configured debug levels. The trace statements are not generated for the configured trace levels.

debug garp

```
debug garp {global | [{protocol | gmrp | gvrp | redundancy} [initshut]
[mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all] [switch <contex-
t_name>]} [{<short (0-7)> | alerts | critical | debugging | emergencies |
errors | informational | notification | warnings}]
```

no debug garp

```
no debug garp {global | [{protocol | gmrp | gvrp | redundancy} [initshut]
[mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all] [switch <contex-
t_name>]}
```

Parameters

Parameter	Type	Description
global		Enter to generate debug statements for all kinds of traces.
protocol		Enter to set the submodule as GARP module, for which the tracing is to be done as per the configured debug levels
gmrp		Enter to set the submodule as GMRP module, for which the tracing is to be done as per the configured debug levels.
gvrp		Enter to set the submodule as GVRP module, for which the tracing is to be done as per the configured debug levels
redundancy		Enter to set the submodule as GARP redundancy module, for which the tracing is to be done as per the configured debug levels
initshut		Enter to generate debug statements for init and shutdown traces. This trace is generated on failed initialization and shutting down of VLAN related entries.
mgmt		Enter to generate debug statements for management traces. This trace is generated during failure in configuration of any of the VLAN feature.
data		Enter to generate debug statements for data path traces. This trace is generated during failure in packet processing.
ctpl		Enter to generate debug statements for control path traces. This trace is generated during failure in modification or retrieving of VLAN entries.
dump		Enter to generate debug statements for packet dump traces. This trace is currently not used in GARP module
os		Enter to generate debug statements for OS resource related traces. This trace is generated during failure in message queues.
failall		Enter to generate debug statements for all kind of failure traces.
buffer		Enter to generate debug statements for GARP buffer related traces. This trace is currently not used in GARP module.
all		Enter to generate debug statements for all kinds of traces.
switch		Enter to configure the tracing of the GARP submodule for the specified context.
<context_name>		Enter a value for context name. This value represents unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.

Parameter	Type	Description
<short (0-7)		Enter to generate debug statements for the Severity level value.This value ranges from 0 to 7.
alerts		Enter to generate debug statements for immediate action.
critical		Enter to generate debug statements for critical conditions.
debugging		Enter to generate debug statements for debugging messages.
emergencies		Enter to generate debug statements when system is unusable.
errors		Enter to generate debug statements for error conditions.
informational		Enter to generate debug statements for information messages.
notification		Enter to generate debug statements for when normal but significant messages.
warnings		Enter to generate debug statements for warning conditions.

Mode

Privileged EXEC Mode

Default

Tracing of the GARP sub module is disabled.

Prerequisites

The GARP sub module tracing can be configured in the switch, only if the GARP module is started and enabled in the switch on all ports.

Examples

iS5comm# debug garp redundancy ctpl switch default debugging

```
    GARP_TRC_LVL : 255, i4CliDebugLevel: 7
    % GARP is disabled
```

21.6. debug vlan

To enable the tracing of the VLAN sub module as per the configured debug levels, use the command **debug vlan** in Privileged EXEC Mode. This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled).The no form of the command disables

the tracing of the VLAN sub module as per the configured debug levels. The trace statements are not generated for the configured trace levels.

debug vlan

```
debug vlan global [all-debug] [all-module] [buffer] [ctpl] [data] [dump]
[failall] [fwd] [initshut] [mgmt] [os] [priority] [redundancy] [switch
<context_name>]
```

no debug vlan

```
no debug vlan global [all-debug] [all-module] [buffer] [ctpl] [data] [dump]
[failall] [fwd] [initshut] [mgmt] [os] [priority] [redundancy] [switch
<context_name>]
```

Parameters

Parameter	Type	Description
global		Enter to generate debug statements for Global-related traces.
all-debug		Enter to generate debug statements for all kinds of traces.
all-module		Enter to generate debug statements for submodule such as VLAN Forwarding, Priority and Redundancy.
buffer		Enter to generate debug statements for VLAN buffer related traces.
ctpl		Enter to generate debug statements for control path traces. This trace is generated during failure in modification or retrieving of VLAN entries.
data		Enter to generate debug statements for data path traces. This trace is generated during failure in packet processing.
dump		Enter to generate debug statements for packet dump traces. This trace is currently not used in VLAN module.
failall		Enter to generate debug statements for all kind of failure traces.
fwd		Enter to generate debug statements for the VLAN forward module.
initshut		Enter to generate debug statements for init and shutdown traces. This trace is generated on failed initialization and shutting down of VLAN related entries.
mgmt		Enter to generate debug statements for management traces. This trace is generated during failure in configuration of any of the VLAN feature.
os		Enter to generate debug statements for OS resource related traces. This trace is generated during failure in message queues.
priority		Enter to generate debug statements for VLAN priority module.
redundancy		Enter to generate debug statements for VLAN redundancy module.
switch		Enter to configure the tracing of the VLAN submodule for the specified context.
<context_name>		Enter a value for context name. This value represents unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.

Mode

Privileged EXEC Mode

Default

Tracing of the VLAN sub module is disabled.

Prerequisites

The VLAN sub module tracing related configuration takes effect in the switch, only if the VLAN switching feature is started and enabled in the switch.

Examples

iS5comm# debug vlan fwd all-module switch default

```
    VLAN_TRC_LVL : 97
```

21.7. forward-all

To configure the forward-all port details for a VLAN to specify the ports that forward or do not forward all multicast group-addressed frames, use the command **forward-all** in VLAN Configuration Mode. The VLAN can also be activated using the vlan active command.The no form of the command deletes the forward-all port details for the VLAN and sets as none.

forward-all

```
forward-all [static-ports ([<interface-type> <0/a-b,0/c,...>] ([<inter-
face-type> <0/a-b,0/c,...>] [ac <a,b,c-d>]] [port-channel <a,b,c-d>] [pw
<a,b,c-d>] [none]] [forbidden <interface-type> <0/a-b,0/c,...>] [<inter-
face-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>] [ac
<a,b,c-d>]]
```

no forward-all

```
no forward-all
```

Parameters

Parameter	Type	Description
`static-ports`		Enter to configure the ports to which all multicast group-addressed frames are to be forwarded. This configuration is restored once the switch is reset.
`<interface-type>`		Enter to set the type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan - Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together • attachment circuit interface
`<0/a-b, 0/c, ...>`		Enter to configure the list of port channel interfaces or a specific port channel identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided, for interface types internal-lan and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
`ac <a,b, c-d>`		Enter to set the AC interface as a port that should never receive packets from the VLAN. This value ranges from 1 to 65535. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
`port-channel <a,b,c-d>`		Enter to set the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3
`pw <a,b,c-d>`		Enter to set the Pseudo wire interface as member port. When the pseudo wire interface is mapped to a specific VLAN, the interface structures are created. This value ranges from 1 to 65535. **NOTE:** Maximum number of PseudoWire interfaces supported in the system is 100.

Parameter	Type	Description
none		Enter to configure none of the ports as static forward-all ports for the VLAN.
forbidden		Enter to configure the ports for which GMRP should not dynamically register the service requirement attribute forward all multicast groups. This configuration is restored once the switch is reset.
<interface-type>		Enter to set the type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • xl-ethernet • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together • attachment circuit interface (ac)
<0/a-b, 0/c, ...>		Enter to configure the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
port-channel <a,b,c-d>		Enter to set the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
pw <a,b,c-d>		Enter to set the Pseudo wire interface as member port. When the pseudo wire interface is mapped to a specific VLAN, the interface structures are created. This value ranges from 1 to 65535. **NOTE:** Maximum number of PseudoWire interfaces supported in the system is 100.
ac <a,b, c-d>		Enter to set the AC interface as a port that should never receive packets from the VLAN. This value ranges from 1 to 65535. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.

Mode

VLAN Configuration Mode

Default

Both forward all static ports and forward-all forbidden ports are not set (that is, set as none) for the active VLANs.

Prerequisites

The forward-all port details can be configured only in the VLANs that are activated

Examples

iS5comm(config-vlan)# forward-all static-ports gigabitethernet 0/1 forbidden-ports gigabitethernet 0/2

21.8. forward-unregistered

To configure the forward-unregistered port details for a VLAN to specify the ports that forward or do not forward multicast group-addresses frames for which no more specific forwarding information applies, use the command **forward-unregistered** in VLAN Configuration Mode. The VLAN can also be activated using the vlan active command.The no form of the command sets the forward-unregistered port details for all VLAN to default value.

forward-unregistered

```
forward-unregistered [static-ports ([<interface-type> <0/a-b,0/c,...>]
([<interface-type> <0/a-b,0/c,...>] [ac <a,b,c-d>]] [port-channel <a,b,c-d>]
[pw <a,b,c-d>] [none]] [forbidden <interface-type> <0/a-b,0/c,...>] [<inter-
face-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>] [ac
<a,b,c-d>]]
```

no forward-unregisteredl

```
no forward-unregistered
```

Parameters

Parameter	Type	Description
`static-ports`		Enter to configure the ports to which all multicast group-addressed frames are to be forwarded. This configuration is restored once the switch is reset.
`<interface-type>`		Enter to set the type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan - Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together • attachment circuit interface
`<0/a-b, 0/c, ...>`		Enter to configure the list of port channel interfaces or a specific port channel identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided, for interface types internal-lan and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
`ac <a,b, c-d>`		Enter to set the AC interface as a port that should never receive packets from the VLAN. This value ranges from 1 to 65535. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
`port-channel <a,b,c-d>`		Enter to set the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3
`pw <a,b,c-d>`		Enter to set the Pseudo wire interface as member port. When the pseudo wire interface is mapped to a specific VLAN, the interface structures are created. This value ranges from 1 to 65535. **NOTE:** Maximum number of PseudoWire interfaces supported in the system is 100.

Parameter	Type	Description
none		Enter to configure none of the ports as static forward-all ports for the VLAN.
forbidden		Enter to configure the ports for which GMRP should not dynamically register the service requirement attribute forward all multicast groups. This configuration is restored once the switch is reset.
<interface-type>		Enter to set the type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • xl-ethernet • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together • attachment circuit interface (ac)
<0/a-b, 0/c, ...>		Enter to configure the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
port-channel <a,b,c-d>		Enter to set the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
pw <a,b,c-d>		Enter to set the Pseudo wire interface as member port. When the pseudo wire interface is mapped to a specific VLAN, the interface structures are created. This value ranges from 1 to 65535. **NOTE:** Maximum number of PseudoWire interfaces supported in the system is 100.
ac <a,b, c-d>		Enter to set the AC interface as a port that should never receive packets from the VLAN. This value ranges from 1 to 65535. Use comma as a separator without space while configuring list of interfaces. Example: 1,3. **NOTE:** Maximum number of PseudoWire interfaces supported in the system is 100. **NOTE:** The configured forward-unregistered forbidden ports should not be a member of the forward-unregistered static port.

Mode

VLAN Configuration Mode

Default

- All the ports available in the switch are set as forward-unregistered static ports and forward-unregistered forbidden ports for the default VLAN (VLAN 1).
- Both forward-unregistered static ports and forward-unregistered forbidden ports are not set (that is, set as none) for the active VLANs other than the default VLAN (VLAN 1).

Prerequisites

The forward-unregistered port details can be configured only in the VLANs that are activated

Examples

iS5comm(config-vlan)# forward-unregistered static-ports gigabitethernet 0/2 forbidden-ports gigabitethernet 0/1 pw 2

21.9. group restricted

To configure the restricted group registration feature in a port, use the command **group restricted** in Interface Configuration Mode. This feature enables you to restrict the multicast groups learnt through GMRP learning.

group restricted

```
group restricted {disable | enable}
```

Parameters

Parameter	Type	Description
disable		Enter to disable restricted group registration feature in the port. The GMRP packets are processed normally and the multicast group attribute/service requirement attribute are learnt dynamically even if they are not statically configured in the switch
enable		Enter to enable restricted group registration feature in the port. The multicast group attribute / service requirement attribute is learnt dynamically from the GMRP frame only if the specific attribute is statically configured in the switch.

Mode

Interface Configuration Mode

Default

disable

Prerequisites

The restricted group registration feature can be configured in the port, only if the GARP module is started and enabled in the switch.

Examples

iS5comm (config-if)# group restricted enable

21.10. interface range

To select the range of physical interfaces and VLAN interfaces to be configured, use the command **interface range** in Global Configuration Mode. The no form of the command selects the range of VLAN interfaces to be removed.

interface range

```
interface range {<interface-type> <0/a-b,0/c,...> | vlan <vlan-id(1-4094)> -
<vlan-id(1-4094)>]}
```

no interface range

```
no interface range vlan <vlan-id(1-4094)> - <vlan-id(1-4094)>]}
```

Parameters

Parameter	Type	Description
<interface-type>		Enter to set the type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
<slot/port-port>		Enter to configure the range of the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. An example is 0/1-2.
vlan		Enter to select the range of the specified VLAN ID (the range of L2 and IVR interfaces to be configured). This is a unique value that represents the specific VLAN created and activated.
<vlan-id(1-4094)>	Integer	Enter a value for VLAN-ID start of range. This value ranges from 1 to 4094. **NOTE:** Maximum number of PseudoWire interfaces supported in the system is 100.
-		Enter a hyphen in to separate both values in the range. **NOTE:** Space should be provided before and after the hyphen (i.e. the command interface range vlan 1 – 4 is valid, whereas the command interface range vlan 1– 4 is not valid.
<vlan-id(1-4094)>	Integer	Enter a value for VLAN-ID start of range. This value ranges from 1 to 4094. **NOTE:** Maximum number of PseudoWire interfaces supported in the system is 100.

Mode

Global Configuration Mode

Default

default

Prerequisites

For port channel range, the specified range must be configured using the interface command.

Examples

iS5comm(config)# interface range gigabitethernet 0/1-2

iS5comm(config-if-range)#

iS5comm(config)# interface range vlan 1 - 2

iS5comm(config-if-range)#

21.11. mac-address-table

To configure a static unicast or multicast MAC address in the forwarding database or configure the timeout period (in seconds) for aging out of dynamically learned forwarding information entry and static entry in the MAC address table, use the command **mac-address-table** in Global Configuration Mode. The no form of the command deletes a configured static Multicast or Unicast MAC address from the forwarding database, or resets the maximum age of an entry in the MAC address table to its default value.

mac-address-table

```
mac-address-table {aging-time <time (10-1000000)>
 | static
 {multicast <aa:aa:aa:aa:aa:aa> {interface {Extreme-Ethernet <interface-id>
| gigabitethernet <interface-id>} | vlan <vlan_vfi_id>}
 | unicast <aa:aa:aa:aa:aa:aa> {interface {Extreme-Ethernet <interface-id> |
gigabitethernet <interface-id>} | status {deleteOnReset | deleteOnTimeout |
permanent} | vlan <vlan_vfi_id>}}
```

no mac-address-table

```
no mac-address-table {aging-time
 | static {multicast <aa:aa:aa:aa:aa:aa> | vlan <vlan_vfi_id>} | unicast
<aa:aa:aa:aa:aa:aa> | vlan <vlan_vfi_id>}}
```

Parameters

Parameter	Type	Description
aging-time		Enter to configure the timeout period (in seconds) for aging out dynamically learned forwarding information entry and static entry in the MAC address table. That is, the entry is deleted once the aging timer expires. **NOTE:** Traffic class feature is used to meet the latency and throughput requirement of time-critical traffic in a LAN environment, where both time-critical and non-time-critical traffic compete for the network band-width.
<time (10-1000000)>	Integer	Enter a value for the aging time. The range is from 10 to 1000000 seconds. High value for the aging time helps to record dynamic entries for a longer time, if traffic is not frequent. This reduces the possibility of flooding. The default is 300 seconds
static		Enter to configure a static MAC address in the forwarding database.
multicast		Enter to configure a static MAC address in the forwarding database.
<aa:aa:aa:aa:aa:aa>		Enter a value for the static multicast destination MAC address. The received packets having the specified MAC address are processed.
interface		Enter to configure the interface type for the member ports.
Gigabitethernet		Enter to configure gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to configure a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to configure the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to configure a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
vlan		Enter to create a VLAN / VFI ID and enters into the config-VLAN mode in which VLAN specific configurations are done. This command directly enters into the config-VLAN mode for the specified VLAN / VFI ID, if the VLAN is already created

Parameter	Type	Description
<vlan_vfi_id>	Integer	Enter a value for VLAN or VFI ID: • <vlan –id> - This is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535 **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
unicast		Enter to configure a static MAC address in the forwarding database.
<aa:aa:aa:aa:aa:aa>		Enter a value for the static unicast destination MAC address. The received packets having the specified MAC address are processed.
interface		Enter to configure the interface type for the member ports.
Gigabitethernet		Enter to configure gigabitetethernet type of interface. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to configure a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Extreme-Ethernet		Enter to configure the Extreme-Ethernet type of interface. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to configure a specific slot number / port number. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
status		Enter to specify the status of the static unicast entry. The options are:
permanent		Enter to specify that the entry remains even after the next reset of the bridge

Parameter	Type	Description
deleteOnReset		Enter to specify that the entry remains even after the next reset of the bridge
deleteOnTimeout		Enter to specify that the entry remains even after the next reset of the bridge
vlan		Enter to create a VLAN / VFI ID and enters into the config-VLAN mode in which VLAN specific configurations are done. This command directly enters into the config-VLAN mode for the specified VLAN / VFI ID, if the VLAN is already created
<vlan_vfi_id>	Integer	Enter a value for VLAN or VFI ID: • <vlan –id> - This is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535 **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

Mode

Global Configuration Mode

Default

aging time - 300 seconds

static mulitcast -status permanent

Prerequisites

Aging time:

- The aging timer is applied to the static entry in the MAC address table, only if static entry status is set as deleteOnTimeout.

- The MAC address table maximum age can be configured in the switch, only if the VLAN switching feature is started and enabled in the switch.

Static:

- VLAN must have been configured and member ports must have been configured for the specified VLAN
- The VLAN value in a configured static MAC entry must be active
- The new configured ports are appended to the existing member port list of the vlan
- The Egress port value in a configured static MAC entry must be a member of the configured VLAN.

Examples

iS5comm (config)# mac-address-table aging-time 200

iS5comm(config)# mac-address-table static multicast 01:02:03:04:05:06 vlan 1 interface gigabitethernet 0/1

S5comm(config)# mac-address-table static unicast 00:11:22:33:22:11 vlan 1 interface gigabitethernet 0/1 status deleteOnTimeout

iS5comm(config)# mac-address-table static unicast 00:11:22:33:22:11 vlan 1 interface gigabitethernet 0/1 pw

21.12. mac-map

To configure VLAN-MAC address mapping that is used only for MAC-based VLAN membership classification, use the command **mac-map** in Interface Configuration Mode. The no form of the command deletes the specified VLAN-MAC address mapping entry.

mac-map

```
mac-map <aa:aa:aa:aa:aa:aa> vlan <vlan-id/vfi_id> [mcast-bcast {discard | allow}]
```

no mac-map

```
no mac-map <aa:aa:aa:aa:aa:aa>
```

Parameters

Parameter	Type	Description
<aa:aa:aa:aa:aa:aa>		Enter an unicast MAC address for to the specified VLAN and used for MAC based VLAN membership classification.
vlan		Enter to map the MAC Address to the specified VLAN / VFI ID.
<vlan-id/vfi_id>		Enter to map the MAC Address to the specified VLAN / VFI ID. • <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id>- VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535. **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries. **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW. **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
mcast-bcast		Enter to configure the way of handling of broadcast and multicast traffic for packets received from source.
discard		Enter to process all multicast / broadcast untagged frames that contain the specified MAC address as the source address.
allow		Enter to drops all multicast / broadcast untagged frames that contain the specified MAC address as the source address. This is the default option.

Mode

Interface Configuration Mode

Default

mcast-bcast - allow

Prerequisites

- Only the VLANs that are activated in the switch can be mapped to the specified MAC address.
- VLAN-MAC address mapping can be configured in the port, only if the VLAN switching feature is started and enabled in the switch.

Examples

iS5comm(config-if)# mac-map 00:11:22:33:44:55 vlan 1 mcast-bcast discard

21.13. map protocol

To create a protocol group with a specific protocol and encapsulation frame type combination, use the command **map protocol** in Global Configuration Mode. The no form of the command deletes all groups that have the specified protocol and encapsulation frame type combination. The created protocol group is used for protocol-VLAN based membership classification. The specified protocol is applied above the data-link layer in a protocol template, and the frame type is applied in the template.

map protocol

```
map protocol {appletalk | ip | netbios | novell | other <aa:aa or
aa:aa:aa:aa:aa>}
 {enet-v2 | llcOther | snap | snap8021H | snapOther}
 protocols-group <Group id integer(0-2147483647)>
```

no map protocol

```
no map protocol {appletalk | ip | netbios | novell | other <aa:aa or
aa:aa:aa:aa:aa>} {enet-v2 | llcOther | snap | snap8021H | snapOther}
```

Parameters

Parameter	Type	Description
appletalk		Enter to configure AppleTalk protocol, which is a proprietary suite of protocols developed by Apple Inc. The corresponding octet string is 80:9b.
ip		Enter to configure Internet Protocol, , which is used for communicating data across network using TCP / IP. The corresponding octet string is 08:00.
netbios		Enter to configure NetBIOS protocol ver TCP/IP, which allows legacy application relying on NetBIOS API to be used on modern TCP/IP networks. The corresponding octet string is f0:f0. This protocol can be set only for the encapsulation frame type llcOther.
novel		Enter to configure Novell Netware protocol suite, which is developed by Novell Inc. The corresponding octet string is ff:ff.
other		Enter to set the protocol type using its corresponding octet string. This value is used to configure protocols other than ip, novell, netbios and appletalk and also the listed protocol types. This value is set as: 16-bit (2 octet) IEEE 802.3 type field, if the frame type is set as enet-v2, snap and snap8021H; 40-bit (5 octet) PID, if the frame type is set as “snapOther”; or 2 octet IEEE 802.2 LSAP pair, if the frame type is set as llcother. The first octet is used for DSAP and the second octet is used for SSAP.
<aa:aa or aa:aa:aa:aa:aa>		Enter an octet string to identify protocol type.
enet-v2		Enter to apply the standard IEEE 802.3 frame format. This format contains: • Preamble – 7 byte value that allows the Ethernet card to synchronize with the beginning of a frame. • SFD – 1 byte value that indicates the start of a frame. • Destination – 6 byte MAC address of the destination. • Source – 6 byte MAC address of the source or a broadcast. • Length – 2 byte value representing the number of bytes in the data fields. • Data – 46 to 1500 bytes higher layer information containing protocol information or user data. • FCS – 4 byte value representing the cyclic redundancy check used by source and destination to verify a successful transmission.

Parameter	Type	Description
llcOther		Enter to apply the LLC format. This format contains the same structure as IEEE 802.3 frame except the following additional fields added before the data field: • DSAP – 1 byte value representing destination service access point to determine the protocol used for the upper layer. • SSAP – 1 byte value representing source service access point to determine the protocol used for the upper layer. • Control – 1 byte value that is used by certain protocols for administration.
snap		Enter to apply the sub-network access protocol format. This format contains the same structure as LLC format except the following additional fields added before the data field • OUI – 3 byte value representing organizational unique ID assigned to vendors for differentiating protocols from different manufacturers. • Type – 2-byte value representing protocol type that defines a specific protocol in the SNAP. This maintains compatibility with Ethernet v2.
snap8021H		Enter to apply the sub-network access protocol format. This format contains the same structure as LLC format except the following additional fields added before the data field • 3 octet field having value 00:00:F8 signifying that next 2 octet field is the encoding of 802.3 Type field in an IEEE 802.2/SNAP Header. • 2 octet Type field - encoding of 802.3 Type field in an IEEE 802.2/SNAP Header
snapOther		Enter to apply the sub-network access protocol format. This format contains the same structure as LLC format except for an additional 5 octet SNAP Protocol Identifier (PID) added before the data field. The value of the PID is not in ether of the ranges used for RFC_1042(SNAP) or SNAP 802.1H. This frame type can be set only for some other protocol type other than IP, Novell, Netbios and Appletalk.
protocols-group		Enter to configure a unique group ID that is to be created with the specified protocol type and encapsulation frame type. This value represents a specific group of protocols that are associated together when assigning a VID to a frame.
<Group id integer(0-2147483647)>	Integer	Enter a value for the unique group ID. This value ranges from 0 to 2147483647.

Mode

Global Configuration Mode

Default

default

Prerequisites

Protocol group cannot be created and configured in the switch, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shut down in the switch.

Examples

iS5comm(config)# map protocol ip enet-v2 protocols-group 1

21.14. map subnet

To configure VLAN-IP subnet address mapping that is used only for subnet-VLAN based membership classification, use the command **map subnet** in Global Configuration Mode. The no form of the command deletes the VLAN-IP subnet address mapping entry. In subnet-VLAN based membership classification, the source IP address in received packet is matched to a VLAN ID using this mapping entry to perform VLAN membership classification.

map subnet

```
map subnet <ip-subnet-address> [vlan <vlan_vfi_id>] [arp {suppress | allow}]
[mask <subnet-mask>]
```

no map subnet

```
no map subnet <ip-subnet-address> [mask <subnet-mask>]
```

Parameters

Parameter	Type	Description
<ip-subnet-address>		Enter to configure the IP subnet address to be used for deciding on discarding / allowing of ARP frames. The format is A.B.C.D.
vlan	Integer	Enter to specify a VLAN / VFI ID.
<vlan_vfi_id>		Enter a value for VLAN or VFI ID: • <vlan –id> - This is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id>- VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535 **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
arp		Enter to configure the way of handling of ARP (Address Resolution Protocol) untagged frames on the specified VLAN.
suppress		Enter to discard ARP untagged frames on VLAN.
allow		Enter to allow ARP untagged frames on VLAN.
mask		Enter to configure the subnet mask address to be used for deciding on discarding / allowing of ARP frames.
<subnet-mask>		Enter a value for the subnet mask. The format is A.B.C.D

Mode

Global Configuration Mode / Interface Configuration Mode

Default

arp - Allow

Prerequisites

- This command is available only in the Global Configuration mode, if the switch BCMX_WANTED is set as yes during the compilation of the exe.
- This command is available only in the Interface Configuration mode, if the switch BCMX_WANTED is set as no during the compilation of the exe.
- Only the VLANs that are activated in the switch can be mapped to the specified IP subnet address.
- VLAN-IP subnet address mapping can be configured in the port, only if the VLAN switching feature is started and enabled in the switch

Examples

iS5comm (config)# map subnet 14.0.0.0 vlan 1 arp allow

21.15. name

To configure a name for the VLAN, use the command **name** in VLAN Configuration Mode. The no form of the command deletes the configured name for the VLAN.

name

```
name <vlan name string>
```

no name

```
no name
```

Mode

VLAN Configuration Mode

Parameters

Parameter	Type	Description
<vlan name string>		Enter a value to specify VLAN name. This value is a string of maximum size 32.

Examples

iS5comm(config-vlan)# name vlannew

21.16. port

To enable MAC-based VLAN, protocol-VLAN based, and subnet-based VLAN membership classification in a port, use the command **port** in Interface Configuration Mode. The no form of the command disables all types of VLAN membership classification or a specified VLAN membership classification in the port.

port

```
port {mac-vlan | protocol-vlan | subnet-vlan}
```

no port

```
no port [mac-vlan] [protocol-vlan] [subnet-vlan]
```

Parameters

Parameter	Type	Description
mac-vlan		Enter to enable MAC-based VLAN membership classification in a port. VLAN membership classification is done based on the MAC address of the source of the received packets. By default, MAC based VLAN classification is disabled on all ports. **NOTE:** MAC based VLAN membership classification can be enabled or disabled in the ports without depending on the global status of the MAC based VLAN membership classification. **NOTE:** The change in global MAC based VLAN membership classification overrides the port membership classification. For example, If the classification in the port is set as enabled while global classification is disabled, and if global classification is changed as enabled and once again to disabled, the classification in the port will be automatically set as disabled. **NOTE:** MAC based VLAN membership classification can be enabled / disabled in the switch, only if the VLAN switching feature is started and enabled in the switch
subnet-vlan		Enter to enable subnet-based VLAN membership classification in a port. The source IP address in received packet is matched to a VLAN ID using an administrator configured table to perform VLAN membership classification.
protocol-vlan		Enter to enable protocol-based VLAN membership classification in a port. VLAN membership classification is done for all untagged and priority-tagged frames based on the port-protocol group / higher layer protocol for the port.

Mode

Interface Configuration Mode

Prerequisites

- All types of VLAN based membership classification can be enabled or disabled in the ports without depending on the global status of the protocol-VLAN based membership classification.
- The change in all types global VLAN based membership classification overrides the port membership classification. For example, If the classification in the port is set as enabled while global classification is disabled, and if global classification is changed as enabled and once again to disabled, the classification in the port will be automatically set as disabled.All types of VLAN based membership classification can be enabled / disabled in the switch, only if the VLAN switching feature is started and enabled in the switch.

Examples

iS5comm(config-if)# port mac-vlan

iS5comm(config-if)# port subnet-vlan

iS5comm(config-if)# port protocol-vlan

iS5comm(config-if)# no port protocol-vlan

S5comm(config-if)# no ports

21.17. ports

To statically configure a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activate the VLAN, use the command **ports** in VLAN Configuration Mode. The VLAN can also be activated using the vlan active command.The configuration defines the tagged and untagged member ports that are used for egress tagging of a VLAN at a port. For ports in PBB bridge mode, this command is used to define member ports for a VLAN in a component. For backbone virtual local area networks (B-VLAN) in a B component, only the provider network ports (PNP) can be set as member ports.For a stacked virtual local area network (S-VLAN) in an I component, only the CNP-S tagged ports can be set as member ports. CNP stands for customer network port.For customer virtual local area network (C-VLAN) in an I component, only the CNP-C tagged ports can be set as member ports. The no form of the command deletes the specified port details for the VLAN. Static ARP cache entry related to the static MAC address of this specific port and VLAN should be removed while removing a port from the VLAN. The member ports cannot be set empty for the VLAN, once the member ports details are configured for that VLAN.

ports

```
ports [add] ([<interface-type> <0/a-b,0/c,...>] ([<interface-type>
<0/a-b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>] [pw <a,b,c-d>]
[untagged (<interface-type> <0/a-b,0/c,...> (<interface-type>
<0/a-b,0/c,...> [port-channel <a,b,c-d>] [pw <a,b,c-d>] [ac <a,b,c-d>]
[all]) [forbidden ([<interface-type> <0/a-b,0/c,...>] [<interface-type>
<0/a-b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>] [ac <a,b,c-d>]]
```

no ports

```
no ports [add] ([<interface-type> <0/a-b,0/c,...>] ([<interface-type>
<0/a-b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>] [pw <a,b,c-d>]
[untagged (<interface-type> <0/a-b,0/c,...> (<interface-type>
<0/a-b,0/c,...> [port-channel <a,b,c-d>] [pw <a,b,c-d>] [ac <a,b,c-d>]
[all]) [forbidden ([<interface-type> <0/a-b,0/c,...>] [<interface-type>
<0/a-b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>] [ac <a,b,c-d>]]
```

Parameters

Parameter	Type	Description
`add`		Enter to append the new configured ports to the existing member port list of the vlan.
`<interface-type>`		Enter to set the type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • xl-ethernet • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together • attachment circuit interface
`<0/a-b, 0/c, ...>`		Enter to configure the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
`port-channel <a,b,c-d>`		Enter to set the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
`pw <a,b,c-d>`		Enter to set the Pseudo wire interface as member port. When the pseudo wire interface is mapped to a specific VLAN, the interface structures are created. This value ranges from 1 to 65535. **NOTE:** Maximum number of PseudoWire interfaces supported in the system is 100.
`untagged`		Enter to configure the ports that should be used for the VLAN to transmit egress packets as untagged packets

Parameter	Type	Description
<interface-type>		Enter to set the type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • xl-ethernet • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together • pseudowire • attachment circuit interface
<0/a-b, 0/c, ...>		Enter to configure the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
port-channel		Enter to set the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
pw <a,b,c-d>		Enter to set the Pseudo wire interface as member port. When the pseudo wire interface is mapped to a specific VLAN, the interface structures are created. This value ranges from 1 to 65535. **NOTE:** Maximum number of PseudoWire interfaces supported in the system is 100.
ac <a,b, c-d>		Enter to set the AC interface as a port that should never receive packets from the VLAN. This value ranges from 1 to 65535. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
all		Sets all configured member ports as the untagged ports for the VLAN. • The ports configured should be a subset of the member ports. • The ports that are attached to VLAN-aware devices should always be set as untagged ports only. • he ports can be set as untagged ports, only if they are not configured as trunk ports.

Parameter	Type	Description
forbidden		Enter to configure the ports that should never receive packets from the VLAN. These ports drops the packets received from this VLAN.
<interface-type>		Enter to set the type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • xl-ethernet • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together • attachment circuit interface
<0/a-b, 0/c, ...>		Enter to configure the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
port-channel <a,b,c-d>		Enter to set the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3
pw <a,b,c-d>		Enter to set the Pseudo wire interface as member port. When the pseudo wire interface is mapped to a specific VLAN, the interface structures are created. This value ranges from 1 to 65535. **NOTE:** Maximum number of PseudoWire interfaces supported in the system is 100.
ac <a,b, c-d>		Enter to set the AC interface as a port that should never receive packets from the VLAN. This value ranges from 1 to 65535. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.

Mode

VLAN Configuration Mode

Default

All ports available in the switch are configured as member ports and untagged ports of the default VLAN (VLAN 1). For other active VLANs, the member, untagged and forbidden ports are not set (that is, set as none).

Prerequisites

Protocol group cannot be created and configured in the switch if the base bridge mode is set as transparent bridging or the VLAN switching feature is shut down in the switch.

Examples

iS5comm(config-vlan)# ports gigabitethernet 0/1 untagged gigabitethernet 0/1 forbidden gigabitethernet 0/2

iS5comm(config-vlan)# ports add gigabitethernet 0/1 untagged gigabitethernet 0/1 forbidden gigabitethernet 0/

1

21.18. port-security trap-syslog

To configure the security violation trap and syslog with Max rate, use the command **port-security trap-syslog** in Global Configuration Mode.

port-security trap-syslog

```
port-security trap-syslog {enable [ rate < integer(1-10) > ] | disable}
```

Parameters

Parameter	Type	Description
`enable`		Enables syslogs and traps for port security violations
`rate`		The maximimum rate in seconds, followed by a value of 1 to 10.
`disable`		Disables syslogs and traps for port security violations

Examples

iS5comm (config)# port-security trap-syslog enable rate 3

iS5comm (config)# port-security trap-syslog disable

Syslogs

```
<130>Sep 20 10:35:20 ISS VLAN Port Security violation occurred on the
port : 9 for VLAN ID : 63 and for MAC addr : 00:00:00:00:10:64<130>Sep
20 10:35:20 ISS VLAN Port Security violation occurred on the port : 9
for VLAN ID : 63 and for MAC addr : 00:00:00:00:10:01
<130>Sep 20 10:35:20 ISS VLAN Port Security violation occurred on the
port : 9 for VLAN ID : 63 and for MAC addr : 00:00:00:00:10:02
<130>Sep 20 10:35:20 ISS VLAN Port Security violation occurred on the
port : 9 for VLAN ID : 63 and for MAC addr : 00:00:00:00:10:03
<130>Sep 20 10:35:20 ISS VLAN Port Security violation occurred on the
port : 9 for VLAN ID : 63 and for MAC addr : 00:00:00:00:10:04
<130>Sep 20 10:35:20 ISS VLAN Port Security violation occurred on the
port : 9 for VLAN ID : 63 and for MAC addr : 00:00:00:00:10:05
```

21.19. port-security violation

To configure the security violation status for the specified port, use the command **port-security violation** in Global Configuration Mode.

port-security violation

```
port-security violation {protect | restrict | shutdown}
```

Parameters

Parameter	Type	Description
violation		Enter to configure the security violation status for the specified switch port. **NOTE:** This command can be executed only if the port is created.
protect		Enter to set the port-security violation label (sav) as protected that sets strict security flag as false and only unknown MAC is treated as violation on all security configured ports.
restrict		Enter to set the port-security violation label (shv) as restricted that sets the security flag as true and configured MAC alone are alone treated as non violation on all security configured ports.
shutdown		Enter to set the port-security violation status as shutdown that disables all security. This is the default option.

Examples

iS5comm (config)# port-security violation protect

21.20. protocol-vlan

To enable protocol-VLAN based membership classification on all ports of the switch, use the command **protocol-vlan** in Global Configuration Mode. The no form of the command disables protocol-VLAN based membership classification on all ports of the switch. VLAN membership classification is done for all untagged and priority-tagged frames based on the port-protocol group / higher layer protocol for the port.

protocol-vlan

```
protocol-vlan
```

no protocol-vlan

```
no protocol-vlan
```

Mode

Global Configuration Mode

Default

Protocol-based VLAN membership classification is enabled on all ports of the switch.

Prerequisites

Protocol-VLAN based membership classification cannot be configured in the switch if the VLAN switching feature has been shut down in the switch.

Examples

iS5comm(config)# no protocol-vlan

21.21. set filtering-utility-criteria

To sets the filtering utility criteria to be applied on all ports, use the command **set filtering-utility-criteria** in Global Configuration Mode.

set filtering-utility-criteria

```
set filtering-utility-criteria {disable | enable}
```

Parameters

Parameter	Type	Description
`disable`		Enter to set default filtering utility criteria to be applied on all ports. If default filtering utility Criteria is selected on a port, then learning of source mac from a received packet on that port will be done only if there is at least on member port in that vlan.
`enable`		Enter to apply the filtering utility criteria configured on the port. It can be default or enhanced. If enhanced filtering utility criteria is selected on a port, then learning of source mac from a received packet on that port will be done if the following are satisfied: • If at least one VLAN that uses the FID includes the reception Port and at least one other Port with a Port State of Learning or Forwarding in its member set, and: – The operPointToPointMAC parameter is false for the reception Port; or – Ingress to the VLAN is permitted through a third Port. The third port can, but is not required to be in the member set.

Mode

Global Configuration Mode

Default

enable

Examples

iS5comm(config)# set filtering-utility-criteria enable

21.22. set garp timer

To enable or disable globally the GARP Multicast Registration Protocol (GMRP) feature on all ports, use the command **set garp timer** in Interface Configuration Mode. GMRP uses the services of GARP to propagate multicast information to the bridges in a LAN. This information allows GMRP aware devices to reduce the transmission of multicast traffic to the LANs, which do not have any members of that multicast group. GMRP registers and de-registers the group membership information and group service requirement information with the GARP.

set garp timer

```
set garp timer {join <time in milli seconds> | leave <time in milli seconds>
| leaveall <time in milli seconds>}
```

Parameters

Parameter	Type	Description
`join`		Enter to configure the time interval (in milli-seconds) till which a GARP participant should wait for its join message to be acknowledged before re-sending the join message. The join message is re-transmitted only once, if the initial message is not acknowledged. This time is started, once the initial join message is sent. The join message is sent by a GARP participant to another GARP participant for registering: • Its attributes with another participant • Its manually configured attributes • Attributes received from a third GARP participant
`<time in milli seconds>`	Integer	Enter a value for the time interval. This value can be multiple of tens only (that is, as 210, 220, 230 and so on) This value should satisfy the condition: GarpJoinTime > 0 and (2*GarpJoinTime) < GarpLeaveTime.
`leave`		Enter to configure the time interval (in milli-seconds) till which a GARP participant should wait for any join message before removing attribute details (that is, waiting time for a registrar to move from empty state (MT) to leave state (LV)). This time is started, once a leave message is sent to de-register the attribute details. The leave messages are sent from a GARP participant to another participant, when: • Its attributes should be de-registered • Its attributes are manually de-registered • It receives leave messages from a third GARP participant
`<time in milli seconds>`	Integer	Enter a value for the time interval. This value can be multiple of tens only (that is, as 610, 620, 630 and so on). The leave time should be greater than or two times as that of the GarpJoinTime. That is, the maximum value of the leave time cannot be more than two times of the join time. For example, if you configure join time as 500 milliseconds, then the leave time value can be from 510 milliseconds to 1000 milliseconds only.
`leaveall`		Enter to configure the time interval (in milli-seconds) till which the details of the registered attributes are maintained. The attribute details should be re-registered after this time interval. A leaveall message is sent from a GARP participant to other GARP participants, after this time interval. This time is started, once a GARP participant starts/once re-registration is done. The leaveall messages are sent from a GARP participant to other participants for: • De-registering all registered attributes • Re-registering all attributes with each of the participants

Parameter	Type	Description
<time in milli seconds>	Integer	Enter a value for the time interval. This value can be multiple of tens only (that is, as 10010, 10020 and so on). The “leaveall time” should be greater than 0 and greater than GarpLeaveTime.

Mode

Interface Configuration Mode

Default

- join - 200
- leave - 600
- leaveall - 10000

Prerequisites

- The GARP timers cannot be set as zero.
- The GARP timers can be configured, only if the GARP module is not shutdown.

Examples

iS5comm(config)# set garp timer join 250

21.23. set gmrp

To enable or disable globally the GARP Multicast Registration Protocol (GMRP) feature on all ports, use the command **set gmrp** in Global Configuration Mode. GMRP uses the services of GARP to propagate multicast information to the bridges in a LAN. This information allows GMRP aware devices to reduce the transmission of multicast traffic to the LANs, which do not have any members of that multicast group. GMRP registers and de-registers the group membership information and group service requirement information with the GARP.

set gmrp

```
set gmrp {disable | enable}
```

Parameters

Parameter	Type	Description
`disable`		Enter to disable GMRP feature in the switch on all ports.
`enable`		Enter to enable GMRP feature in the switch on all ports and also starts the GARP in the switch if the GARP is disabled.

Mode

Global Configuration Mode

Default

enable

Prerequisites

- GMRP feature can be globally enabled, only if VLAN feature is globally enabled in the switch.
- GMRP feature should be globally disabled before globally disabling the VLAN feature in the switch.
- GMRP feature cannot be enabled in the switch, if the VLAN switching feature is shutdown in the switch.

Examples

iS5comm(config)# set gmrp disable

21.24. set gvrp

To enable or disable globally the GVRP feature on all ports, use the command **set gvrp** in Global Configuration Mode. GVRP uses the services of GARP to propagate VLAN registration information to other VLAN aware bridges in a LAN. This information allows GVRP aware devices to dynamically establish and update the information about the existence of the VLANs in a topology. The GVRP registers the created VLANs with GARP and de-registers the deleted VLANs from the GARP.

set gvrp

```
set gvrp {disable | enable}
```

Parameters

Parameter	Type	Description
`disable`		Enter to disable GVRP feature in the switch on all ports.
`enable`		Enter to enable GVRP feature in the switch on all ports and also starts the GARP in the switch if the GARP is disabled.

Mode

Global Configuration Mode

Default

enable

Prerequisites

- GVRP feature can be globally enabled, only if VLAN feature is globally enabled in the switch.
- GVRP feature should be globally disabled before globally disabling the VLAN feature in the switch.
- GVRP feature cannot be enabled in the switch, if is shutdown in the switch.

Examples

iS5comm(config)# set gvrp disable

21.25. set mac-learning

To configure the global MAC learning status, use the command **set mac-learning** in Global Configuration Mode.

set mac-learning

```
set mac-learning {enable | disable}
```

Parameters

Parameter	Type	Description
`enable`		Enter to enable the global MAC learning.
`disable`		Enter to disable the global MAC learning.

Mode

Global Configuration Mode

Default

enable

Examples

iS5comm (config)# set mac-learning enable

21.26. set packet-reflection

To enable or disable reflection status for the port, use the command **set packet-reflection** in Interface Configuration Mode.

set packet-reflection

```
set packet-reflection {disable | enable}
```

Parameters

Parameter	Type	Description
`disable`		Enter to disable reflection status for the port. This is the default.
`enable`		Enter to enable reflection status for the port.

Mode

Interface Configuration Mode

Default

disable

Examples

iS5comm (config-if)# set packet-reflection enable

21.27. set port

To enable or disable globally the GMRP or GVRP feature on a specified interface, use the command **set port** in Global Configuration Mode.

set port

```
set port gmrp <interface-type> <interface-id> {disable | enable}
 gvrp <interface-type> <interface-id> {disable | enable}
 gvrp {disable | enable} <string(4)>
```

Parameters

Parameter	Type	Description
gmrp		Enter to disable / enable GMRP feature on the specified interface. GMRP uses the services of GARP to propagate multicast information to the bridges in a LAN. This information allows GMRP aware devices to reduce the transmission of multicast traffic to the LANs, which do not have any members of that multicast group. GMRP registers and de-registers the group membership information and group service requirement information with the GARP. **NOTE:** The GMRP feature can be configured on the specified interface, only if the GARP module is not shutdown. **NOTE:** Any GMRP packet received is discarded and no GMRP registrations are propagated from other ports, if GMRP is globally disabled or GMRP is disabled in the interface.
<interface-type>		Enter to configure the GVRP feature for the specified type of interface. The interface can be as following parameters. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
<interface-id>		Configures the GVRP feature for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan and port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.
disable		Enter to disable GMRP feature ion the specified interface
enable		Enter to enable GMRP feature in the switch on all ports and also starts the GARP in the switch if the GARP is disabled.

Parameter	Type	Description
gvrp		Enter to disable / enable GVRP feature ion the specified interface. VRP uses the services of GARP to propagate VLAN registration information to other VLAN aware bridges in a LAN. This information allows GVRP aware devices to dynamically establish and update the information about the existence of the VLANs in a topology. The GVRP registers the created VLANs with GARP and de-registers the deleted VLANs from the GARP. **NOTE:** The GVRP feature can be configured on the specified interface, only if the GARP module is not shutdown. **NOTE:** Any GVRP packet received is discarded and no GVRP registrations are propagated from other ports, if GVRP is globally disabled or GVRP is disabled in the interface
<interface-type>		Enter to configure the GVRP feature for the specified type of interface. The interface can be as following parameters. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
<interface-id>		Configures the GVRP feature for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan and port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.
disable		Enter to disable GVRP feature on the specified interface.
enable		Enter to enable GVRP feature in the switch on all ports and also starts the GARP in the switch if the GARP is disabled.
gvrp		Enter to disable / enable GVRP feature on the specified interface. **NOTE:** The value enable indicates that GVRP is enabled on the current port, as long as global GVRP status is also enabled for the device. **NOTE:** If port GVRP state is disabled, but global GVRP status is still enabled, then GVRP is disabled on current port. Any received GVRP packets will be discarded and no GVRP registrations will be propagated from other ports.
disable		Enter to disable GVRP feature in the switch on the specified interface
enable		Enter to enable GVRP feature in the switch on the specified interface. This is the default.

Parameter	Type	Description
<string (4)>	Integer	Enter an Interface identifier.

Mode

Global Configuration Mode

Default

enable

Examples

iS5comm(config)# set port gmrp gigabitethernet 0/1 disable

iS5comm(config)# set port gvrp gigabitethernet 0/1 disable

iS5comm(config)# set port gvrp disable 0/1

21.28. set sw-stats

To set the software statistics collection globally in the switch, use the command **set sw-stats** in Global Configuration Mode.

set sw-stats

```
set sw-stats {disable | enable}
```

Parameters

Parameter	Type	Description
`disable`		Enter to disable software statistics collection globally in the switch. The statistics collection will be done by the hardware and will not be stored in software.
`enable`		Enter to enable software statistics collection globally in the switch and the statistics will be stored in the software. This value can be set only if data switching is done by the software.

Mode

Global Configuration Mode

Default

If data switching is done by software, then the default value is enabled else by default statistics collection by the software is disabled.

Examples

iS5comm(config)# set sw-stats enable

21.29. set unicast-mac learning

To enable or disable unicast-MAC learning feature for a VLAN, use the command **set unicast-mac learning** in VLAN Configuration Mode. The source MAC learning is not done in the switch when this feature is disabled for the VLAN.

set unicast-mac learning

```
set unicast-mac learning {enable | disable | default}
```

Parameters

Parameter	Type	Description
`enable`		Enter to enable unicast-MAC learning feature for a VLAN.
`disable`		Enter to disable unicast-MAC learning feature for a VLAN.
`default`		Enter to set the unicast-MAC learning feature of the VLAN to its default state. When this feature is set to Default, this feature inherits the value configured for Global mac learning status as Enable/Disable.

Mode

VLAN Configuration Mode

Default

default

Prerequisites

Global MAC learning status will override the VLAN unicast-MAC learning status only when the VLAN unicast-MAC learning status is default.

VLAN unicast-MAC learning can be configured as Enable/Disable even when the Global Mac learning status is Disabled.

VLAN unicast-MAC learning feature can be configured only in the VLANs that are activated.

Examples

iS5comm (config-vlan)# set unicast-mac learning disable

21.30. set vlan traffic-classes

To enable or disable the traffic class feature on all ports, use the command **set vlan traffic-classes** in Global Configuration Mode.

set vlan traffic-classes

```
set vlan traffic-classes {enable | disable}
```

Parameters

Parameter	Type	Description
`enable`		Enter to enable traffic class feature in the switch on all ports. User priority to the particular traffic class can be enabled. **NOTE:** Traffic class feature is used to meet the latency and throughput requirement of time-critical traffic in a LAN environment, where both time-critical and non-time-critical traffic compete for the network bandwidth.
`disable`		Enter to disable the traffic class feature in the switch on all ports. The switch operates with a single priority level for all traffic

Mode

Global Configuration Mode

Default

enable

Prerequisites

The traffic class feature cannot be configured in the switch if the VLAN switching feature is shut down in the switch.

Examples

iS5comm (config)# set vlan traffic-classes disable

21.31. show forward-all

To display all entries in the VLAN forward all table, use the command **show forward-all** in Privileged EXEC Mode. These entries contain forward-all details of all active VLANs in the switch. The details have VLAN ID and information regarding forwarding to all ports, all static ports, and all forbidden ports assigned to the VLAN.

show forward-all

```
show forward-all [switch <context_name>]
```

Parameters

Parameter	Type	Description
switch		Enter to specify switch name.
<context_name>		Enter a context name.

Mode

Privileged EXEC Mode

Prerequisites

This command can be executed in the switch, only if the VLAN switching feature is started and enabled in the switch.

Examples

iS5comm# show forward-all switch default

```
Vlan Forward All Table
----------------------
Vlan ID : 1
ForwardAll Ports          : Gi0/1
ForwardAll Static Ports   : Gi0/1
ForwardAll ForbiddenPorts : Gi0/2
-------------------------------------------------------
```

21.32. show forward-unregistered

To display all entries in the VLAN forward unregistered table, use the command **show forward-unregistered** in Privileged EXEC Mode. These entries contain forward-unregistered port details of all active VLANs in the switch. The details have VLAN ID and information regarding unregistered ports, unregistered static ports and unregistered forbidden ports assigned to the VLAN.

show forward-unregistered

```
show forward-unregistered [switch <context_name>]
```

Parameters

Parameter	Type	Description
switch		Enter to specify switch name.
<context_name>		Enter a context name.

Mode

Privileged EXEC Mode

Prerequisites

This command can be executed in the switch, only if the VLAN switching feature is started and enabled in the switch.

Examples

iS5comm# show forward-unregistered

```
Vlan Forward Unregistered Table
--------------------------------

Vlan ID : 1Unreg ports           : Gi0/1, Gi0/2, Gi0/3, Gi0/4, Gi0/5,
Gi0/6
Gi0/7, Gi0/8, Gi0/9, Gi0/10, Gi0/11, Gi0/12
Gi0/13, Gi0/14, Gi0/15, Gi0/16, Gi0/17, Gi0/18
Gi0/19, Gi0/20, Gi0/21, Gi0/22, Gi0/23, Gi0/24
Ex0/1, Ex0/2, Ex0/3, Ex0/4
Unreg Static Ports   : Gi0/1, Gi0/2, Gi0/3, Gi0/4, Gi0/5, Gi0/6
Gi0/7, Gi0/8, Gi0/9, Gi0/10, Gi0/11, Gi0/12
Gi0/13, Gi0/14, Gi0/15, Gi0/16, Gi0/17, Gi0/18
Gi0/19, Gi0/20, Gi0/21, Gi0/22, Gi0/23, Gi0/24
Ex0/1, Ex0/2, Ex0/3, Ex0/4
Unreg Forbidden Ports : None
-----------------------------------------------------
```

21.33. show garp timer

To display the GARP timer information of all interfaces available in the switch / all contexts, use the command **show garp timer** in Privileged EXEC Mode.

show garp timer

```
show garp timer [{port <interface-type> <interface-id> [switch <string (32)>]
```

Parameters

Parameter	Type	Description
port		Enter to display the GARP timer information of the specified interface.
<interface-type>		Enter to specify type of interface to be displayed. The interface can be as following parameters. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
<interface-id>		Enter to specify interface identifier of the interface to be displayed. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan and port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.
switch		Enter to display the GARP timer information of all interfaces, for the specified context. This value represents unique name of the switch context.
<string(32)>		Enter a value for an Interface identifier. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature. For now switch should be only default.

Mode

Privileged EXEC Mode

Prerequisites

This command can be executed in the switch, only if the GARP module is not shut down and VLAN switching feature is started and enabled in the switch.

Examples

iS5comm# show garp timer port gigabitethernet 0/1

```
    Garp Port Timer Info (in milli seconds)
    ---------------------------------------
    Port      Join-time      Leave-time      Leave-all-time
    -----     ---------      ----------      --------------
    Gi0/1     200            600             10000
```

21.34. show gmrp statistics

To display GMRP statistics for the specified port, use the command **show gmrp statistics** in Privileged EXEC Mode.

show gmrp statistics

```
show gmrp statistics [{port <interface-type> <interface-id>}]
```

Parameters

Parameter	Type	Description
port		Enter to display the GMRP statistics for the specified interface.
<interface-type>		Enter to specify type of interface to be displayed. The interface can be as following parameters. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
<interface-id>		Enter to specify interface identifier of the interface to be displayed. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan and port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

Mode

Privileged EXEC Mode

Examples

iS5comm# show gmrp statistics port gigabitethernet 0/1

```
    GMRP Statistics for Port Gi0/1
    ---------------------------------------
    Total valid GMRP Packets Received 0:
    Join Emptys             0
    Join In                 0
    Leave In                0
    Leave All               0
    Leave Empty             0
    Empty                   0
    Total valid GMRP Packets Transmitted:0
    Join Emptys             0
    Join In                 0
    Leave In                0
    Leave All               0
    Leave Empty             0
    Empty                   0
```

21.35. show gvrp statistics

To display GVRP statistics in the system or for the specified port, use the command **show gvrp statistics** in Privileged EXEC Mode.

show gvrp statistics

```
show gvrp statistics [{port <interface-type> <interface-id>}]
```

Parameters

Parameter	Type	Description
port		Enter to display the GVRP statistics for the specified interface.
<interface-type>		Enter to specify type of interface to be displayed. The interface can be as following parameters. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. • pw - Pseudowire (PW) is an emulation of a point-to-point connection over a packet-switching network (PSN). This value ranges from 1 to 65535. Maximum number of PseudoWire interfaces supported in the system is 100. • ac - Attachment Circuit (AC) is a physical or virtual circuit attaching a Customer Edge to a Provider Edge port. This value ranges from 1 to 65535.
<interface-id>		Enter to specify interface identifier of the interface to be displayed. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan and port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

Mode

Privileged EXEC Mode

Examples

iS5comm# show gvrp statistics port gigabitethernet 0/1

```
GVRP Statistics for Port Gi0/1
---------------------------------------
Total valid GVRP Packets Received 0:
Join Emptys             0
Join In                 0
```

```
    Leave In                0
    Leave All               0
    Leave Empty             0
    Empty                   0
    Total valid GVRP Packets Transmitted:0
    Join Emptys             0
    Join In                 0
    Leave In                0
    Leave All               0
    Leave Empty             0
    Empty                   0
```

21.36. show mac-address-table

To display all static / dynamic unicast or multicast MAC entries created in the MAC address table, use the command **show mac-address-table** in Privileged EXEC Mode. These entries contain VLAN ID, unicast / multicast MAC address, unicast backbone MAC address of peer backbone edge bridge, member ports, the type of entry (i.e. static, learn, etc.), and total number of entries displayed.

show mac-address-table

```
show mac-address-table[address <aa:aa:aa:aa:aa:aa>]

 [aging-time [switch <context_name>]

 [count [vlan <vlan-range>] [switch <context_name>]

 [dynamic multicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>]
{Extreme-Ethernet <interface-id> | gigabitethernet <interface-id>} | switch
<context_name>]

 [dynamic unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>]
{Extreme-Ethernet <interface-id> | gigabitethernet <interface-id>} | switch
<context_name>]

 hardware

 [static multicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>]
{Extreme-Ethernet <interface-id> | gigabitethernet <interface-id>} | switch
<context_name>]

 [static unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>]
{Extreme-Ethernet <interface-id> | gigabitethernet <interface-id>} | switch
<context_name>]

 [vlan <vlan-range>] [{interface {Extreme-Ethernet <interface-id> | giga-
bitethernet <interface-id>} | switch <context_name>]
```

Parameters

Parameter	Type	Description
address		Enter to display all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified unicast / multicast MAC address.
<aa:aa:aa:aa:aa:aa>		Enter a MAC address.
aging-time		Enter to display the maximum age of a Mac address table entry.
switch		Enter to specify switch name.
<context_name>		Enter to specify context name.
count		Enter to display the number of MAC addresses present on all VLANs or on a specified VLAN
vlan		Enter to display all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified VLANs alone.
<vlan-range>		Enter a VLAN range value that denotes the VLAN ID range for which the entries need to be displayed. This value ranges from 1 to 4094. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to 4010.
switch		Enter to specify switch name.
<context_name>		Enter to specify context name.
dynamic		Enter to display all dynamically learnt entries from the MAC address table.
multicast		Enter to display all dynamically learnt multicast entries. These entries contain VLAN ID for which multicast MAC address entry is learnt, multicast MAC address, ports through which the entry is learnt, the status of entry (that is permanent, static and so on), the unicast backbone MAC address of peer backbone edge bridge, and total number of entries displayed.
vlan		Enter to display all dynamically learnt multicast entries from the MAC address table for the specified VLANs alone
<vlan-range>		Enter a value for vlan range that denotes the VLAN ID range for which the entries need to be displayed. This value ranges from 1 to 4094. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to 4010.

Parameter	Type	Description
address		Enter to display all dynamically learnt multicast entries from the MAC address table for the specified unicast MAC address.
<aa:aa:aa:aa:aa:aa>		Enter a MAC address.
interface		Enter to specify the type of interface.
Extreme-Ethernet		Enter to configure the Extreme-Ethernet type of interface to be displayed. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Gigabitethernet		Enter to configure gigabitetethernet type of interface to be displayed. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
switch		Enter to specify switch name.
<context_name>		Enter to specify context name.
dynamic		Enter to display all dynamically learnt entries from the MAC address table.
unicast		Enter to display all dynamically learnt unicast entries. These entries contain VLAN ID for which unicast MAC address entry is learnt, unicast MAC address, ports through which the entry is learnt, the status of entry (that is permanent, static and so on), the unicast backbone MAC address of peer backbone edge bridge, and total number of entries displayed.
vlan		Enter to display all dynamically learnt unicast entries from the MAC address table for the specified VLANs alone
<vlan-range>		Enter a value for vlan range that denotes the VLAN ID range for which the entries need to be displayed. This value ranges from 1 to 4094. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to 4010.

Parameter	Type	Description
address		Enter to display all dynamically learnt unicast entries from the MAC address table for the specified unicast MAC address.
<aa:aa:aa:aa:aa:aa>		Enter a MAC address.
interface		Enter to specify the type of interface.
Extreme-Ethernet		Enter to configure the Extreme-Ethernet type of interface to be displayed. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Gigabitethernet		Enter to configure gigabitetethernet type of interface to be displayed. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
switch		Enter to specify switch name.
<context_name>		Enter to specify context name.
static		Enter to display static multicast MAC address entries created in the FDB table.
hardware		Enter to display all MAC addresses programmed in hardware.
multicast		Enter to display all static multicast MAC address entries created in the FDB table. These entries contain VLAN ID for which multicast MAC address entry is learnt, multicast MAC address, ports through which the entry is learnt, the status of entry (that is permanent, static and so on), the unicast backbone MAC address of peer backbone edge bridge, and total number of entries displayed.
vlan		Enter to display all static multicast MAC address entries created in the FDB table for the specified VLANs alone

Parameter	Type	Description
<vlan-range>		Enter a value for vlan range that denotes the VLAN ID range for which the entries need to be displayed. This value ranges from 1 to 4094. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to 4010.
address		Enter to display all static unicast MAC address entries created in the FDB table for the specified unicast MAC address.
<aa:aa:aa:aa:aa:aa>		Enter a MAC address.
interface		Enter to specify the type of interface.
Extreme-Ethernet		Enter to configure the Extreme-Ethernet type of interface to be displayed. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Gigabitethernet		Enter to configure gigabitetethernet type of interface to be displayed. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
switch		Enter to specify switch name.
<context_name>		Enter to specify context name.
static		Enter to display static unicast MAC address entries created in the FDB table.
unicast		Enter to display all static unicast MAC address entries created in the FDB table. These entries contain VLAN ID for which unicast MAC address entry is learnt, unicast MAC address, ports through which the entry is learnt, the status of entry (that is permanent, static and so on), the unicast backbone MAC address of peer backbone edge bridge, and total number of entries displayed.
vlan		Enter to display all static unicast MAC address entries created in the FDB table for the specified VLANs alone

Parameter	Type	Description
<vlan-range>		Enter a value for vlan range that denotes the VLAN ID range for which the entries need to be displayed. This value ranges from 1 to 4094. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to 4010.
address		Enter to display all static unicast MAC address entries created in the FDB table for the specified unicast MAC address.
<aa:aa:aa:aa:aa:aa>		Enter a MAC address.
interface		Enter to specify the type of interface.
Extreme-Ethernet		Enter to configure the Extreme-Ethernet type of interface to be displayed. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Gigabitethernet		Enter to configure gigabitetethernet type of interface to be displayed. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
switch		Enter to specify switch name.
<context_name>		Enter to specify context name.

Mode

Privileged EXEC Mode

Prerequisites

This command can be executed in the switch, only if the VLAN switching feature is started and enabled in the switch.

Examples

iS5comm# show mac-address-table

```
Vlan    Mac Address         Type     ConnectionId       Ports
----    -----------         ----     ------------       -----
1       54:e1:ad:07:0d:87   Learnt                       Gi0/9

Total Mac Addresses displayed: 1
```

iS5comm# show mac-address-table aging-time

```
Mac Address Aging Time: 300
```

iS5comm# show mac-address-table count

```
Mac Entries for Vlan 1:
-------------------------
Dynamic Unicast Address Count    : 0
Dynamic Multicast Address Count  : 0
Static Unicast Address Count     : 0
Static Multicast Address Count   : 0
---------------------------------------
```

show mac-address-table hardware

```
MAC addresses programmed in hardware
-----------------------------------------------------------
Index   |  MAC addr             |  VLAN |  Interface
-----------------------------------------------------------
2592    |  54:e1:ad:07:0d:87    |  1    |       0/9
-----------------------------------------------------------
6092    |  e8:e8:75:90:0b:01    |  1    |       0/0
-----------------------------------------------------------
16384   |  e8:e8:75:90:0b:01    |  1    |       0/0
-----------------------------------------------------------
```

iS5comm# show mac-address static multicast

```
Static Multicast Table----------------------
Total Mac Addresses displayed: 0
```

iS5comm# show mac-address static unicast

```
Vlan  Mac Address        RecvPort Status        Connection ID
Ports
----  -----------        -------- ------        ------------
-----
Total Mac Addresses displayed: 0
```

21.37. show port-security

To display port security related information for the specified interface or all interfaces created in the system, use the command **show port-security** in Privileged EXEC Mode.

show port-security

```
show port-security [{interface <interface-type> <interface-id> | switch
<context_name>]
```

Parameters

Parameter	Type	Description
interface		Enter to display the port security related information for the specified interface.
<interface-type>		Enter to configure the type of interface to be displayed. The types of interface are as follows: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. • sisp – <ifnum> interface number • pw -<ifnum> interface number • ac - <ifnum> interface number
<interface-id>		Enter to configure a specific slot number / port number to be displayed. For interface type other than internal-lan, virtual and port-channel, the format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1. Only i-lan, virtual or port-channel ID is provided, for interface types internal-lan, virtual and port-channel.
switch		Enter to specify switch name.
<context_name>		Enter to specify context name.

Mode

Privileged EXEC Mode

Examples

iS5comm# show port-security interface gigabitethernet 0/1

```
---------------------------
interface gigabitethernet 0/1
---------------------------
```

```
MAC learning : enable
port security violation type : Shutdown
```

iS5comm# show port-security

```
----------------------------
interface gigabitethernet 0/2
----------------------------
Port-Security Status : enable
port security violation type : Shutdown
Port Mac Learning Limit Status      : disabled
Security Violation Count            : 0
Port-security trap-syslog Status : DISABLED
```

21.38. show unicast port-security

To display port security related information for the specified MAC address and interface, use the command **show unicast port-security** in Privileged EXEC Mode.

show unicast port-security

```
show unicast port-security [address <aa:aa:aa:aa:aa:aa>] [{interface <inter-face-type> <interface-id> | switch <context_name>]
```

Parameters

Parameter	Type	Description
address		Enter to display static unicast MAC address for the specified interface
<aa:aa:aa:aa:aa:aa>		Enter a MAC address to identify the interface to be displayed.
interface		Enter to display the port security related information for the specified interface.
<interface-type>		Enter to configure the type of interface to be displayed. The types of interface are as follows: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. • sisp – <ifnum> interface number • pw -<ifnum> interface number • ac - <ifnum> interface number
<interface-id>		Enter to configure a specific slot number / port number to be displayed. For interface type other than internal-lan, virtual and port-channel, the format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1. Only i-lan, virtual or port-channel ID is provided, for interface types internal-lan, virtual and port-channel.
switch		Enter to specify switch name.
<context_name>		Enter to specify context name.

Mode

Privileged EXEC Mode

Examples

iS5comm# show unicast port-security

```
    Vlan  Mac Address        RecvPort Status Connection ID Ports
    ----  -----------        -------- ------ ------------ -----
    1     00:11:22:33:44:55           Permanent Gi0/1

    Total Mac Addresses displayed: 1
```

show unicast port-security address 00:11:22:33:44:55

```
    Vlan  Mac Address RecvPort Status Connection ID Ports
    ----  ----------- -------- ------ ------------ -----
    1     00:11:22:33:44:55           Permanent Gi0/1

    Total Mac Addresses displayed: 1
```

21.39. show vlan

To display all types of vlan information, use the command **show vlan** in Privileged EXEC Mode.

show vlan

```
show vlan [brief | id <vlan-range> | summary | ascending] [switch <contex-
t_name>]
 [device {capabilities | info [switch <context_name>]
 [learning params [vlan <vlan-range>] [switch <string(32)>]
 [port config [{port {Extreme-Ethernet <interface-id> | gigabitethernet
<interface-id>} | switch <context_name>]
 protocols-group [switch <context_name>]
 statistics [vlan <vlan-range>] [switch <context_name>]
 traffic-classes [{port {Extreme-Ethernet <interface-id> | gigabitethernet
<interface-id>} | switch <context_name>}]
```

Parameters

Parameter	Type	Description
brief		Enter to display the VLAN entry related information of all active VLANs and VLANs (that are not active) for which the port details are configured.
id		Enter to display the VLAN entry related information for specified VLANs alone.
<vlan-range>		Enter a value that denotes the VLAN ID range for which the information needs to be displayed. This value ranges from 1 to 4094. For example, the value is provided as 4000-4010 to display the information for VLANs IDs from 4000 to 4010. The information is displayed only for the active VLANs and VLANs (that are not active) for which the port details are configured.
summary		Enter to display only the total number of VLANs existing in the switch. This includes only the active VLANs and VLANs (that are not active) for which the port details are configured. The VLAN entry related information is not displayed.
ascending		Enter to display the VLAN entry related information in ascending order.
switch		Enter to specify switch name.
<context_name>		Enter to specify context name.
device		Enter to display VLAN global information / capabilities that are applicable to all VLANs created in the switch / all contexts.
capabilities		Enter to display only the list of VLAN features such as traffic class feature, supported in the switch / all contexts..
info		Enter to display the VLAN global information that is applicable to all VLANs created in the switch / all contexts.
switch		Enter to specify switch name.
<context_name>		Enter to specify context name.
learning		Enter to display the VLAN learning parameter details for all active VLANs and VLANs (that are not active) for which the port details are configured, available in all contexts / in the switch.
params		Enter to display VLAN learning status and learning limit with details such as admin status of unicast MAC learning feature and value representing MAC learning limit and operational status of learning feature.

Parameter	Type	Description
vlan		Enter to display the protocol specific configuration for VLAN.
<vlan-range>		Enter a value that denotes the VLAN ID range for which the information needs to be displayed. This value ranges from 1 to 4094. For example, the value is provided as 4000-4010 to display the information for VLANs IDs from 4000 to 4010. The information is displayed only for the active VLANs and VLANs (that are not active) for which the port details are configured.
switch		Enter to specify switch name.
<context_name>		Enter to specify context name.
port		Enter to display the VLAN related port specific information for all interfaces available in the switch / all contexts.
config		Enter to display the VLAN related port specific information for all interfaces available in the switch / all contexts. The information contains PVID, acceptable frame type, port mode, filtering utility criteria, default priority value and status of ingress filtering feature, GVRP module, GMRP module, restricted VLAN registration feature, restricted group registration feature, MAC-based VLAN membership, subnet based VLAN membership, protocol-VLAN based membership and port protected feature.
Extreme-Ethernet		Enter to configure the Extreme-Ethernet type of interface to be displayed. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Gigabitethernet		Enter to configure gigabitetethernet type of interface to be displayed. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
switch		Enter to specify switch name.
<context_name>		Enter to specify context name.

Parameter	Type	Description
protocols-group		Enter to display all entries in the protocol group table. These entries contain protocol group information of the switch / all contexts. The information contains ID of a group, protocol assigned to the group, and frame type assigned to the group.
switch		Enter to specify switch name.
<context_name>		Enter to specify context name.
statistics		Enter to display information about Protocol specific statistics for VLAN.
vlan		Enter to display the protocol specific configuration for VLAN.
<vlan-range>		Enter a value that denotes the VLAN ID range for which the information needs to be displayed. This value ranges from 1 to 4094. For example, the value is provided as 4000-4010 to display the information for VLANs IDs from 4000 to 4010. The information is displayed only for the active VLANs and VLANs (that are not active) for which the port details are configured.
switch		Enter to specify switch name.
<context_name>		Enter to specify context name.
traffic-classes		Enter to display the evaluated user priority and traffic class mapping information of all interfaces available in the switch / all context
port		Enter to display the evaluated user priority and traffic class mapping information of the specified interface.
Extreme-Ethernet		Enter to configure the Extreme-Ethernet type of interface to be displayed. Extreme Ethernet is a version of Ethernet that supports data transfer up to 10 Gigabits per second and only full duplex links
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.
Gigabitethernet		Enter to configure gigabitetethernet type of interface to be displayed. Gigabitethernet is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
<interface-id>		Enter to configure a specific slot number / port number to be displayed. The format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1.

Parameter	Type	Description
switch		Enter to specify switch name.
<context_name>		Enter to specify context name.

Mode

Privileged EXEC Mode

Prerequisites

This command can be executed in the switch, only if the VLAN switching feature is started and enabled in the switch.

Examples

iS5comm# show vlan

```
Vlan database
-------------
Vlan ID             : 1
Member Ports        : Gi0/1, Gi0/2, Gi0/3, Gi0/4, Gi0/5, Gi0/6
                      Gi0/7, Gi0/8, Gi0/9, Gi0/10, Gi0/11, Gi0/12
Gi0/13, Gi0/14, Gi0/15, Gi0/16, Gi0/17, Gi0/18
Gi0/19, Gi0/20, Gi0/21, Gi0/22, Gi0/23, Gi0/24
Ex0/1, Ex0/2, Ex0/3, Ex0/4
Untagged Ports      : Gi0/1, Gi0/2, Gi0/3, Gi0/4, Gi0/5, Gi0/6
                 Gi0/7, Gi0/8, Gi0/9, Gi0/10, Gi0/11, Gi0/12
Gi0/13, Gi0/14, Gi0/15, Gi0/16, Gi0/17, Gi0/18
               Gi0/19, Gi0/20, Gi0/21, Gi0/22, Gi0/23, Gi0/24
Ex0/1, Ex0/2, Ex0/3, Ex0/4
Forbidden Ports     : None
Name                :Status              : Permanent
Egress Ethertype    : 0x8100
Service Loopback Status   : Disabled
-----------------------------------------------------
```

iS5comm# show vlan device info

```
Vlan device configurations
--------------------------
Vlan Status                       : Enabled
Vlan Oper status                  : Enabled
Gvrp status                       : Disabled
```

```
    Gmrp status                         : Disabled
    Gvrp Oper status                    : Disabled
    Gmrp Oper status                    : Disabled
    Mac-Vlan Status                     : Disabled
    Subnet-Vlan Status                  : Disabled
    Protocol-Vlan Status                : Enabled
    Bridge Mode                         : Customer Bridge
    Base-Bridge Mode                    : Vlan Aware Bridge
    Traffic Classes                     : Enabled
    Vlan Operational Learning Mode      : IVL
    Hybrid Default Learning Mode        : IVL
    Version number                      : 1
    Max Vlan id                         : 4094
    Max supported vlans                 : 4094
    Global mac learning status          : Enabled
    Filtering Utility Criteria          : Enabled
    Unicast mac learning limit          : 0
```

iS5comm# show vlan device capabilities

```
    Vlan device capabilities
    -------------------------

    Extended filtering services
    Traffic classes
    Static Entry Individual port
    IVL capable
    SVL capable
    Hybrid capable
    Configurable Pvid Tagging
```

iS5comm# show vlan learning params

```
    Unicast MAC Learning Parameters
    -----------------------------------
    Vlan Id                  : 1
    Mac Learning Admin-Status : Default
    Mac Learning Oper-Status  : Enable
    Mac Learning Limit        : 1500
    -----------------------------------
```

iS5comm# show vlan protocols-group

```
    Protocol Group Table --------------------
    ----------------------------------------
    Frame Type      Protocol             Group
```

show vlan traffic-classes port gi 0/1

```
Max Vlan Traffic Class table
-------------------------
Port     Max Traffic Class
-----    -----------------
Gi0/1    7
Traffic Class table
--------------------
Port     Priority    Traffic Class
-----    ---------   -------------
Gi0/1    0           1
Gi0/1    1           0
Gi0/1    2           2
Gi0/1    3           2
Gi0/1    4           3
Gi0/1    5           4
Gi0/1    6           5
Gi0/1    7           6
```

iS5comm# show vlan traffic-classes

```
Max Vlan Traffic Class table
-------------------------
Port     Max Traffic Class
-----    -----------------
Gi0/1    7
Gi0/2    8
Gi0/3    8
Gi0/4    8
Gi0/5    8
Gi0/6    8
Gi0/7    8
Gi0/8    8
Gi0/9    8
Gi0/10    8
Gi0/11    8
Gi0/12    8
Gi0/13    8
Gi0/14    8
Gi0/15    8
Gi0/16    8
Gi0/17    8
```

```
Gi0/18    8
Gi0/19    8
Gi0/20    8
Gi0/21    8
Gi0/22    8
Gi0/23    8
Gi0/24    8
Ex0/1    8
Ex0/2    8
Ex0/3    8
Ex0/4    8

Traffic Class table
---------------------
Port     Priority    Traffic Class
-----    ---------   -------------
Gi0/1    0           1
Gi0/1    1           0
Gi0/1    2           2
Gi0/1    3           2
Gi0/1    4           3
Gi0/1    5           4
Gi0/1    6           5
Gi0/1    7           6
Gi0/2    0           2
Gi0/2    1           0
Gi0/2    2           1
Gi0/2    3           3
Gi0/2    4           4
Gi0/2    5           5
Gi0/2    6           6
Gi0/2    7           7
Gi0/3    0           2
Gi0/3    1           0
Gi0/3    2           1
Gi0/3    3           3
Gi0/3    4           4
Gi0/3    5           5
Gi0/3    6           6
Gi0/3    7           7
```

```
Gi0/4    0            2
Gi0/4    1            0
Gi0/4    2            1
Gi0/4    3            3
Gi0/4    4            4
Gi0/4    5            5
Gi0/4    6            6
Gi0/4    7            7
Gi0/5    0            2
Gi0/5    1            0
Gi0/5    2            1
Gi0/5    3            3
Gi0/5    4            4
Gi0/5    5            5
Gi0/5    6            6
Gi0/5    7            7
Gi0/6    0            2
Gi0/6    1            0
Gi0/6    2            1
Gi0/6    3            3
Gi0/6    4            4
Gi0/6    5            5
Gi0/6    6            6
Gi0/6    7            7
Gi0/7    0            2
Gi0/7    1            0
Gi0/7    2            1
Gi0/7    3            3
Gi0/7    4            4
Gi0/7    5            5
Gi0/7    6            6
Gi0/7    7            7
Gi0/8    0            2
Gi0/8    1            0
Gi0/8    2            1
Gi0/8    3            3
Gi0/8    4            4
Gi0/8    5            5
Gi0/8    6            6
Gi0/8    7            7
```

```
Gi0/9    0            2
Gi0/9    1            0
Gi0/9    2            1
Gi0/9    3            3
Gi0/9    4            4
Gi0/9    5            5
Gi0/9    6            6
Gi0/9    7            7
Gi0/10    0            2
Gi0/10    1            0
Gi0/10    2            1
Gi0/10    3            3
Gi0/10    4            4
Gi0/10    5            5
Gi0/10    6            6
Gi0/10    7            7
Gi0/11    0            2
Gi0/11    1            0
Gi0/11    2            1
Gi0/11    3            3
Gi0/11    4            4
Gi0/11    5            5
Gi0/11    6            6
Gi0/11    7            7
Gi0/12    0            2
Gi0/12    1            0
Gi0/12    2            1
Gi0/12    3            3
Gi0/12    4            4
Gi0/12    5            5
Gi0/12    6            6
Gi0/12    7            7
Gi0/13    0            2
Gi0/13    1            0
Gi0/13    2            1
Gi0/13    3            3
Gi0/13    4            4
Gi0/13    5            5
Gi0/13    6            6
Gi0/13    7            7
```

```
Gi0/14    0           2
Gi0/14    1           0
Gi0/14    2           1
Gi0/14    3           3
Gi0/14    4           4
Gi0/14    5           5
Gi0/14    6           6
Gi0/14    7           7
Gi0/15    0           2
Gi0/15    1           0
Gi0/15    2           1
Gi0/15    3           3
Gi0/15    4           4
Gi0/15    5           5
Gi0/15    6           6
Gi0/15    7           7
Gi0/16    0           2
Gi0/16    1           0
Gi0/16    2           1
Gi0/16    3           3
Gi0/16    4           4
Gi0/16    5           5
Gi0/16    6           6
Gi0/16    7           7
Gi0/17    0           2
Gi0/17    1           0
Gi0/17    2           1
Gi0/17    3           3
Gi0/17    4           4
Gi0/17    5           5
Gi0/17    6           6
Gi0/17    7           7
Gi0/18    0           2
Gi0/18    1           0
Gi0/18    2           1
Gi0/18    3           3
Gi0/18    4           4
Gi0/18    5           5
Gi0/18    6           6
Gi0/18    7           7
```

```
Gi0/19    0           2
Gi0/19    1           0
Gi0/19    2           1
Gi0/19    3           3
Gi0/19    4           4
Gi0/19    5           5
Gi0/19    6           6
Gi0/19    7           7
Gi0/20    0           2
Gi0/20    1           0
Gi0/20    2           1
Gi0/20    3           3
Gi0/20    4           4
Gi0/20    5           5
Gi0/20    6           6
Gi0/20    7           7
Gi0/21    0           2
Gi0/21    1           0
Gi0/21    2           1
Gi0/21    3           3
Gi0/21    4           4
Gi0/21    5           5
Gi0/21    6           6
Gi0/21    7           7
Gi0/22    0           2
Gi0/22    1           0
Gi0/22    2           1
Gi0/22    3           3
Gi0/22    4           4
Gi0/22    5           5
Gi0/22    6           6
Gi0/22    7           7
Gi0/23    0           2
Gi0/23    1           0
Gi0/23    2           1
Gi0/23    3           3
Gi0/23    4           4
Gi0/23    5           5
Gi0/23    6           6
Gi0/23    7           7
```

```
Gi0/24    0            2
Gi0/24    1            0
Gi0/24    2            1
Gi0/24    3            3
Gi0/24    4            4
Gi0/24    5            5
Gi0/24    6            6
Gi0/24    7            7
Ex0/1    0            2
Ex0/1    1            0
Ex0/1    2            1
Ex0/1    3            3
Ex0/1    4            4
Ex0/1    5            5
Ex0/1    6            6
Ex0/1    7            7
```

21.40. shutdown garp

To shut down the Generic Attribute Registration Protocol (GARP) module in the switch on all ports and release all memories used for the GARP module, use the command **shutdown garp** in Global Configuration Mode. The no form of the command starts and enables the GARP module in the switch on all ports. GMRP and GVRP are enabled explicitly, once the disabled GARP is enabled. GARP Multicast Registration Protocol (GMRP) is a Generic Attribute Registration Protocol application that provides a constrained multicast flooding facility similar to IGMP snooping. GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is the GARP -based protocol mechanism, maintaining the VLAN information in the switch dynamically. GARP is used to synchronize attribute information between the bridges in the LAN. It allows registering and unregistering of attribute values, which are disseminated into the backbone of the GARP participants.

shutdown garp

```
shutdown garp
```

Mode

Global Configuration Mode

Default

GARP module is started and enabled in the switch on all ports.

Prerequisites

- GARP can be started, only if VLAN switching feature is started in the switch.
- GARP can be shutdown, only if GVRP and/or GMRP are disabled.

Examples

iS5comm (config)# shutdown garp

21.41. shutdown vlan

To shut down the VLAN switching feature in the switch and release all resources allocated to the VLAN, use the command **shutdown vlan** in Global Configuration Mode. The no form of the command starts and enables VLAN switching feature in the switch. The resources required for the VLAN feature are also allocated to it.The VLAN feature allows to segment logically a shared media LAN for forming virtual work groups.

shutdown vlan

no shutdown vlan

Mode

Global Configuration Mode

Default

VLAN switching feature is started and enabled in the switch.

Prerequisites

VLAN module can be shut down, only if the GARP module is shutdown. VLAN switching configuration is not allowed in the switch if the base bridge mode is set as transparent bridging.

Examples

iS5comm(config)# no shutdown vlan

21.42. switchport

To configure switch port related information, use the command **switchport** in Interface Configuration Mode. The no form of the command resets the configuration to default or disables the features.

switchport

```
switchport [dot1q] {ingress | egress} ether-type <size(1-65535)>
 [acceptable-frame-type {all | tagged | untaggedAndPrioritytagged}
 [access vlan <vlan-id(1-4094)>]
 [egress TPID-type {portbased | vlanbased}
 [encapsulation dot1ad vlan-type {tpid1 <CTAG | STAG > [tpid2] [tpid3]}
 [filtering-utility-criteria {default | enhanced}] [ingress-filter]
 [map protocols-group <Group id integer(0-2147483647)> vlan
<vlan-id/vfi_id>]
 [mode {access | trunk | hybrid | {dynamic | tagged {auto | desirable}}}]
 [port-security {unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id/vfi_id> | viola-
tion {{protect | restrict | shutdown}| [recovery { automatic recovery-time
<integer 0-300> | manual }]]
 [priority default <priority value(0-7)>
 [protected]
 [pvid vlan <vlan-id/vfi_id>]
 [unicast-mac learning {enable | disable}
```

no switchport

```
no switchport [dot1q] {ingress | egress} ether-type} [acceptable-frame-type]
 [access vlan] [egress TPID-type]
 [encapsulation dot1ad vlan-type [tpid1] [tpid2] [tpid3]} [ingress-filter]
 [map protocols-group <Group id integer(0-2147483647)> vlan
<vlan-id(1-4094)>]
 [mode] [priority default <priority value(0-7)>] [protected] [pvid]
```

Parameters

Parameter	Type	Description
dot1q		Enter to put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration and configure port Ingress/Egress Ethertype. Dot1q shows tunneling related information. **NOTE:** This command executes only if the bridge port type is set as CBP (Customer Backbone Port).
ingress		Enter to configure ingress Ethertype and hence allows the service provider to support tunneling. Packets received on a port are considered tagged when the packet Ethertype matches the Ethertype configured on the port.
egress		Enter to configure egress Ethertype. This object indicates the Ethertype of the S-VLAN tag that has to be applied for all outgoing packets on this port. If a valid value is in this object, all packets which are outgoing on this port will contain the Ethertype as configured in this object
Ethertype		Enter to configure the size of Ethertype.
<size(1-65535)>	Integer	Enter a value for Ethertype. This value ranges from 1 to 65535 with a default of 33024.
<vlan-id(1-4094)>	Integer	Enter a value for VLAN-ID start of range. This value ranges from 1 to 4094.
acceptable-frame-type		Enter to configure the type of VLAN dependent BPDU frames such as GMRP BPDU that the port should accept during the VLAN membership configuration.
all		Enter to configure the acceptable frame type as all. All tagged, untagged and priority tagged frames received on the port are accepted and subjected to ingress filtering.
tagged		Enter to configure the acceptable frame type as tagged.Only the tagged frames received on the port are accepted and subjected to ingress filtering. The untagged and priority tagged frames received on the port are rejected. For ports in PBB bridge mode, for the following Port types, the TAG descriptions are as follows • for CNP S Tagged - S-Tag • for CNP C Tagged - C-Tag • for CNP Port Based - S-Tag • PIP - I-Tag • CBP - I-Tag • PNP - B-tab or S-Tag.

Parameter	Type	Description
untaggedAndPrioritytagged		Enter to configure the acceptable frame type as untagged and priority tagged. Only the untagged or priority tagged frames received on the port are accepted and subjected to ingress filtering. The tagged frames received on the port are rejected.
access		Enter to configure the PVID (Port VLAN Identifier) on a port.
vlan		Enter to configure the PVID (Port VLAN Identifier) on a port.
<vlan-id(1-4094)>	Integer	Enter a value for PVID (Port VLAN Identifier). This value ranges from 1 to 4094. **NOTE:** If the frame (untagged/priority tagged/customer VLAN tagged) is received on a "tunnel" port, then the default PVID associated with the port is used **NOTE:** If the received frame cannot be classified as MAC-based or port-and-protocol-based, then the PVID associated with the port is used. **NOTE:** For ports in PBB bridge mode, PVID can be configured on CNP (Customer Network Port) and CBP (Customer Backbone Port). **NOTE:** Usage is based on acceptable frame type of the port. Packets will be either dropped or accepted at ingress. Once a packet is accepted, if the packet is having a tag, it will be processed against that tag. Otherwise, the packet will be processed against PVID.
egress		Enter to set the egress TPID-type for the port
TPID-type		Enter to configure the egress TPID-type on a port
portbased		Enter to set egress TPID-type as portbased. The egress TPID of the packet is selected from the Egress Port Table.
vlanbased		Enter to configure the egress TPID-type as vlan-based. The egress TPID is selected from the egress VLAN Table.
encapsulation		Enter to configure standard/user defined TPID for a port.
dot1ad		Enter for DOT1AD configuration. IEEE 802.1ad implements standard protocols for double tagging of data. The data traffic coming from the customer side are double tagged in the provider network where the inner tag is the customer-tag (C-tag) and the outer tag is the provider-tag(S-tag). A service provider's Layer 2 network transports the subscriber's Layer 2 protocols transparently.
vlan-type		Enter to set VLAN TYPE.

Parameter	Type	Description
tpid1		Enter to configure standard allowable TPID for a Port, either C-Tag or S-Tag. **NOTE:** The TPID1 value should be configured as a value different from the default ingress Ethertype. If the ingress Ethertype is 0x8808, then TPID CTAG should be configured using this command. if the ingress Ethertype is 0x8100, TPID STAG should be configured.
CTAG		Enter to configure standard allowable TPID for C-tag (i.e. inner or Customer tag) is used to uniquely identify a customer and typically is used on a per port basis. This indicates the secondary Ethertype that is allowable for a port. The configurable value for this object is 0x8100. For Ethertypes numbers see https://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.xhtml#ieee-802-numbers-1
STAG		Enter to configure standard allowable TPID for S-TAG (i.e. outer, Service Provider tag). This indicates a secondary Ethertype that is allowable for a port. The configurable value for this object is 0x88A8.
tpid2		Enter to set standard allowable TPID for a port. This indicates the standard Ethertype that is allowable for a port. The configurable value for this object is Q-in-Q Ethertype [0x9100].
tpid3		Enter to configure the user defined allowable TPID for a port.
filtering-utility-criteria		Enter to configure filtering utility criteria for the port. This utility criteria are used to reduce the capacity requirement of the filtering database and to reduce the time for which service is affected, by retaining the filtering information learnt prior to a change in the physical topology of the network. **NOTE:** The filtering utility criteria cannot be configured in the switch, if the VLAN switching feature is shutdown in the switch. **NOTE:** This command is applicable only for the port configured as switch port.
default		Enter to allow learning of source MAC from a packet received on the port, only if there is at least one member port for a VLAN mentioned in the packet. This is the default option.

Parameter	Type	Description
enhanced		Enter to allow learning of source MAC from a packet received on the port, only if the following conditions are satisfied: • At least one VLAN that uses the FID includes the reception port and at least one other Port with a port state of Learning or Forwarding in its member set. • The operPointToPointMAC parameter is false for the reception port. Or Ingress to the VLAN is permitted through a port other than source and reception. This port can be or not be in the member set for the VLAN.
ingress-filter		Enter to enable ingress filtering feature on the port. The ingress filtering is applied for the incoming frames received on the port. Only the incoming frames of the VLANs that have this port in its member list are accepted. This configuration does not affect VLAN independent BPDU frames such as GVRP BPDU and STP BPDU. It affects only the VLAN dependent BPDU frames GMRP BPDU. By default, the ingress filtering feature is disabled on the port. • **NOTE:** Prerequisites: • This command is applicable only for the port configured as switch port. • The ingress filtering cannot be configured on the port, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch. • The ingress-filtering feature cannot be configured and is always enabled on the port, if the bridge port type is set as customer network port – S tagged.
map		Enter to map the configured protocol group to a particular VLAN ID for an interface. This configuration is used during protocol-VLAN based membership classification.
protocols-group		Enter to map the configured protocol group to a particular VLAN ID for an interface.
<Group id integer(0-2147483647)>	Integer	Specify a unique group ID that is already created with the specified protocol type and encapsulation frame type. This value represents a specific group that should be associated with a VID. This value ranges from 0 to 2147483647.

Parameter	Type	Description
vlan		Enter to map the configured protocol group to the specified VLAN / VFI ID. **NOTE:** The protocol group should have been already created with a specific protocol and encapsulation frame type combination before mapping it to a VID **NOTE:** This command is applicable only for the port configured as switch port **NOTE:** The protocol group mapping cannot be configured for the port, if the VLAN switching feature is shutdown in the switch.
<vlan-id/vfi_id>	Integer	Enter to configure the configured protocol group to the specified VLAN / VFI ID. This value ranges from 1 to 65535. • <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.<vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535. **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW. **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
mode		Enter to configure the mode of operation for a switch port. This mode defines the way of handling of traffic for VLANs.
access		Enter to configure the port as access port that accepts and sends only untagged packets. This kind of port is added as a member to a specific VLAN only and carries traffic only for the VLAN to which the port is assigned. The port can be set as access port, only if the following 3 conditions are met: • The GVRP is disabled for that port. • Acceptable frame type is set as “untagged AND priority” tagged. • Port is a not a tagged member of any VLAN.

Parameter	Type	Description
trunk		Enter to set the port as trunk port that accepts and sends only tagged frames. This kind of port is added as member of all existing VLANs and for any new VLAN created, and carries traffic for all VLANs. The trunk port accepts untagged frames too, if the acceptable frame type is set as all. The port can be set as trunk port, only if the port is not a member of untagged ports for any VLAN in the switch.
hybrid		Enter to configure the port as hybrid port that accepts and sends both tagged and untagged frames.
dynamic		Enter to configure the mode as Dynamic Mode. The Dynamic Mode can be auto and desirable.
auto		Enter to set the interface to convert the link to a trunk link.
desirable		Enter to set the interface to attempt actively to convert the link to a trunk link.
port-security		Enter to configure the unicast MAC address as a known frame in the port. The port-security command is used to enable/disable port-security on a port. Port-security needs to be enabled to configure trusted MAC addresses and MAC learn limit. By default port-security is be “disabled”. If port-security configuration is enabled, the Port Security MACs limit(trusted MACs) would be limited to 3K per device. This valud is hardcoded and not configurable.
unicast		Enter to configure the static unicast MAC address for the specified interface.
<aa:aa:aa:aa:aa:aa>		Enter an unicast MAC address. This address should be in the format of aa:bb:cc:dd:ee:ff.
vlan		Enter to set VLAN Interface configuration for the specified VLAN / VFI ID.

Parameter	Type	Description
<vlan-id/vfi_id>	Integer	Enter set VLAN Interface configuration for the specified VLAN / VFI ID. This value ranges from 1 to 6553. • <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id>- VFI ID is for a VLAN created in the system with a value ranging from 4096 to 65535. **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wild-card match for the VID in management operations or Filtering Database entries. **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW. **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
violation		Enter to configure the security violation status for the specified switch port. **NOTE:** This command can be executed only if the interface created is mapped to a context.
recovery		The default state is manual recovery. The user needs to manually change the admin status to the UP (no shutdown) state to recover the port.
automatic		If port recovery is configured as “automatic”, based on the “timer” value configured, the port will change its status to UP automatically. The timer value to be configured will be in “seconds”. The default recovery timer value is 5 secs.
protect		Enter to set the port-security violation label (sav) as protected, which sets strict security flag as false, and only unknown MAC is treated as violation on all security configured ports. Drops packets with unknown source addresses until secure MAC addresses drop below the maximum value.
restrict		Enter to set the port-security violation label (shv) as restricted, which sets the security flag as true, and configured MAC alone are alone treated as non violation on all security configured ports.Restrict drops packets with unknown source addresses until the number of secure MAC addresses drop below the maximum value and causes the Security Violation counter to increment. If max value is reached all violated entries will flash out and the learning process will start again.

Parameter	Type	Description
shutdown		Enter to set the port-security violation status as shutdown which disables all security. This is the default option.
priority		Enter to configure the default ingress user priority for a port. This priority is assigned to frames received on the port that does not have a priority assigned to it. This priority value is useful only on media such as Ethernet that does not support native user priority. **NOTE:** This command is applicable only for the port configured as switch port. **NOTE:** The default user priority cannot be configured for the port, if the VLAN switching feature is shutdown in the switch
default		Enter to configure the default ingress user priority for a port.
<priority value(0-7)>	Integer	Enter a value for the default ingress user priority. This value ranges from 0 to 7. The value 0 represents the lowest priority and the value 7 represents the highest priority. 0 is also the default value.
protected		Enter to enable switchport protection feature for a port. This feature sets the particular port as protected so that the port does not forward frames received from another protected port present on the same switch. By default, the switchport protection feature is disabled in the port. **NOTE:** The switchport protection feature cannot be configured in the switch if the VLAN switching feature is shutdown in the switch. **NOTE:** This command is applicable only for the port configured as switch port.
pvid		Enter to configure the PVID on the specified port. PVID (Port VLAN ID) is a default VLAN id assigned to frames coming to the port. The PVID represents the VLAN ID/ VFI ID that is to be assigned to untagged frames or priority-tagged or C-VLAN frames received on the port. The PVID is used for port based VLAN type membership classification. The PVID configuration is used based on the acceptable frame type of the port. The packets are processed against PVID if the packets accepted at ingress are not having tags. **NOTE:** Only the IDs of the active VLAN can be used as PVIDs in the command. **NOTE:** This command is applicable only for the port configured as switch port. **NOTE:** The PVID cannot be configured for the port if the VLAN switching feature is shut down in the switch.

Parameter	Type	Description
<vlan-id/vfi_id>	Integer	Enter a value for the / VFI ID. This value ranges from 1 to 65535. • <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. The default is 1. • <vfi-id> - VFI ID is for a VLAN created in the system and ranges from 4096 to 65535. **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wild-card match for the VID in management operations or Filtering Database entries. **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW. **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
unicast-mac		Enter to enable / disable unicast-MAC learning for the port.
learning		Enter to enable / disable unicast-MAC learning for the port. The learning command allows users to enable/disable mac-learning on a specific port with the configured mac-learning count. There are no changes in standard MAC learning process, Upon the configuration of port-security users will be able to specify the max number of MAC addresses that may be learned by a port. When the number of MAC addresses learned exceeds the limit then entries in excess of the limit will be marked as DROPped.
enable		Enter to enable unicast-MAC learning for the port. When Mac Learning is enabled, unicast mac entries will be learnt on this port. Configuration of this object will not get affected by the Global Mac Learning Status. This is the default option.
disable		Enter to disable unicast-MAC learning for the port. When Unicast Mac Learning is disabled, no unicast mac entry will be learnt on this port.

Mode

Interface Configuration Mode (Physical / Port Channel)

Examples

iS5comm(config)# int port-channel 1

iS5comm(config-if)# switchport access vlan 3

iS5comm(config-if)# switchport dot1q ingress ether-type 33024

iS5comm(config-if)# switchport egress TPID-type vlanbased

iS5comm(config-if) switchport encapsulation dot1ad vlan-type tpid1 STAG tpid2 tpid3

iS5comm(config-if)# switchport filtering-utility-criteria enhanced

iS5comm(config-if)# switchport ingress-filter

iS5comm(config-if)# switchport map protocols-group 1 vlan 2

iS5comm(config-if)# switchport mode access

iS5comm (config-if)# switchport port-security unicast 00:11:22:33:44:55 vlan 1

iS5comm (config-if)# switchport port-security violation protect

iS5comm(config-if)# switchport priority default 5

iS5comm(config-if)# switchport protected

iS5comm(config-if)# switchport pvid 1

iS5comm(config-if)# switchport unicast-mac learning enable

iS5comm(config-if)# switchport port-security violation recovery automatic recovery-time 150

Enabling Port Security

iS5comm# config terminal

iS5comm(config)# int gi 0/7

iS5comm(config-if)# switchport port-security enable

MAC learning

iS5Comm(config)# int gi 0/17

iS5Comm(config-if)# switchport unicast-mac learning enable mac-limit 3

iS5Comm(config-if)# end

iS5Comm# show mac-address

Vlan Mac Address Type ConnectionId Ports

---- ----------- ---- ----------- -----

1 00:10:94:00:00:02 Learnt Gi0/17

1 00:10:94:00:00:03 Learnt Gi0/17

1 00:10:94:00:00:04 Learnt Gi0/17

1 00:10:94:00:00:05 Drop Gi0/17 ? DROP entries after 3 MACs.

1 00:10:94:00:00:06 Drop Gi0/17Total Mac Addresses displayed: 5

Unicast

iS5Comm(config-if)# switchport port-security unicast 12:23:34:34:34:34 vlan 1

The above command allows the user to configure the trusted MAC-address in the VLAN, this will be the only MAC address that will be allowed for this interface.

This is an optional configuration, if the MAC address is not specified, then the first learned MAC addresses will be allowed until the configured limit is reached.

To remove the trusted MAC address from the interface use the following command:

iS5Comm(config-if)# no switchport port-security unicast 12:23:34:34:34:34 vlan 1

21.43. unicast-mac learning limit

To configure the unicast-MAC learning limit for a switch, use the command **unicast-mac learning limit** in VLAN Configuration Mode. The no form of the command resets the unicast-MAC learning limit for the switch to its default value.

unicast-mac learning limit

```
unicast-mac learning limit <limit value(0-4294967295)>
```

no unicast-mac learning limit

```
unicast-mac learning limit
```

Parameters

Parameter	Type	Description
<limit value(0-4294967295)>	Integer	Enter a value for the learning limit. The limit represents the maximum number of distinct unicast MAC addresses that can be learnt in the switch. This value ranges from 0 to 4294967295.

Mode

VLAN Configuration Mode

Default

The maximum limit supported by the switch.

Prerequisites

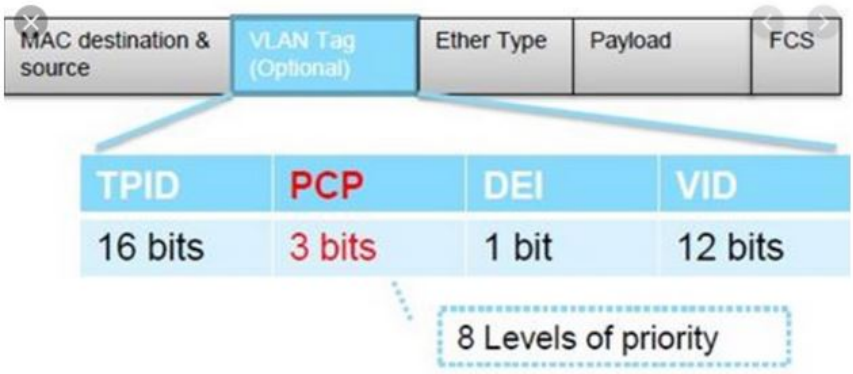
- The limiting value should not be less than the unicast MAC learning limit set for any of the VLAN.
- Unicast-MAC learning limit cannot be configured in the switch, if the VLAN switching feature is shutdown in the switch.

Examples

iS5comm (config-vlan)# vlan unicast-mac learning limit 300

21.44. user-defined TPID

To configure user defined TPID (Tag Protocol Identifier) allowable for Port/Egress VLAN, use the command **user-defined TPID** in Global Configuration Mode. The no form of this command deletes the configured user defined TPID allowable for a port/ Egress VLAN Ethertype.



user-defined TPID

```
user-defined TPID <size (1-65535)>
```

Parameters

Parameter	Type	Description
<size (1-65535)>	Integer	Enter a value for the Ethertype.This Ethertype value ranges from 1 to 65535.

Mode

Global Configuration Mode

Default

0

Prerequisites

The VLAN mode can be configured, only if the VLAN switching feature is started and enabled in the switch.

Examples

iS5comm(config)# user-defined TPID 200

21.45. vlan

To map an evaluated user priority to a traffic class on a port, configure the maximum number of traffic classes supported on a port, or set a restricted feature configuration, use the command **vlan** in Interface Configuration Mode. The maximum number of traffic classes supported on the port can be configured, only if the VLAN switching feature is started and enabled in the switch. The no form of the command resets the maximum traffic class value on the port to its default value andmaps the default traffic class to the specified priority value on the port.

vlan

```
vlan {map-priority <priority value(0-7)> traffic-class <traffic class
value(0-7)>
 | max-traffic-class <max traffic class value(1-8)>
 | restricted} {disable | enable}
```

no vlan

```
no vlan {map-priority <priority value(0-7)> | max-traffic-class}
```

Parameters

Parameter	Type	Description
`map-priority`		Enter to map an evaluated user priority to a traffic class on a port. The frame received on the interface with the configured priority is processed in the configured traffic class. Traffic class is used to meet the latency and throughput requirement of time-critical traffic in a LAN environment, where both time-critical and non-time-critical traffic compete for the network bandwidth.
`<priority value(0-7)`	Integer	Enter a priority value to be set for the specified traffic class. This value ranges from 0 to 7. The frames with the configured priority are mapped to the specified traffic class. The priority determined for the received frame is equivalent to the priority indicated in the received tagged frame or one of the evaluated priorities determined based on the media-type. The priority determined is equal to the Default User Priority value for the ingress port, if the untagged frames are received from Ethernet media. The priority determined is equal to the Regen user priority for the ingress port and media-specific user priority, if the untagged frames are received from non-Ethernet media.
traffic-class		Enter to configure the traffic class value to which the received frame of specified priority is to be mapped.

Parameter	Type	Description
<traffic-class value(0-7)	Integer	Enter a traffic class value to which the received frame of specified priority is to be mapped. This value ranges from 0 to 7. Each value represents the concerned traffic. They are: • 0 - Best effort. This represents all kinds of non-detrimental traffic that is not sensitive to QoS metrics such as jitter. • 1 - Background. This represents bulk transfers and other activities that are permitted on the network without impacting the network usage for users and applications. • 2 - Standard (spare traffic). This represents traffic of more importance than background but less importance than excellent load. • 3 - Excellent load. This represents the best effort type service that an information services organization should deliver to its most important customers. • 4 - Controlled load. This represents traffic subject to admission control to assure that the traffic is received even when the network is overloaded. • 5 - Interactive voice and video. This represents traffic having delay less than 100 milli-seconds. • 6 - Internetwork control-Layer 3 network control. This represents traffic having delay less than 10 milli-seconds. • 7 - Network control-Layer 2 network control reserved traffic. This represents traffic that demands special treatment based on its requirements and relative importance. The configured traffic class value should be less than the maximum number of traffic classes in the port.
max-traffic-class		Enter to configure the maximum number of traffic classes supported on a port
<max-traffic-class value(1-8)	Integer	Enter a value for the maximum number of traffic classes supported on a port. The number of traffic classes supported depends on the hardware used, which can limit the number of traffic classes to a lower number. Eight traffic classes for handling priority traffic are supported. Each traffic is assigned a traffic type based on the time sensitiveness of the traffic. This value ranges from 1 to 8. The default is 8.
restricted		Enter to configure the restricted feature configuration.
disable		Enter to disable the restricted VLAN registration.
enable		Enter to enable the restricted VLAN registration.

Mode

Interface Configuration Mode

Default

The default traffic classes that are mapped to the priority is listed below:

Priority Traffic Class

1 0

2 1

3 3

4 4

5 5

6 6

7 7

Prerequisites

- The default traffic classes mapped to the priority value depends upon the maximum traffic classes supported on the port.
- The evaluated user priority can be mapped to the traffic class, only if the VLAN switching feature is started and enabled in the switch.
- Mapping packets to a queue based on the COS value in the packet can be achieved by mapping the packets COS value to internal priority and then the internal priority to a Queue Id. Since the Cos mapping to a queue is not directly supported in bcm, alternate command has to be configured for achieving this based on the internal priority

Examples

iS5comm (config-if)# vlan map-priority 2 traffic-class 2

21.46. vlan

To activate a VLAN in the switch, set the VLAN egress Ethertype, set the loopback-related configuration, and unicast-mac learning limit for a Dynamic VLAN, use the command **vlan** in VLAN Configuration Mode. The no form of this command resets the VLAN egress Ethertype and the unicast-MAC learning limit for the VLAN to the default values.

vlan

```
vlan {active
```

```
| egress ether-type | QINQ | STAG | QINQ | user-defined}
| loopback {enable | disable}
| unicast-mac learning limit <limit value(0-4294967295)>}
```

Parameters

Parameter	Type	Description
active		Enter activate a VLAN in the switch. **NOTE:** Only default VLAN (VLAN 1) is activated once the switch is started.
egress		Enter to set the VLAN Egress Ethertype.
ether-type		Enter to set the VLAN Egress Ethertype.
CTAG		Enter to configure the secondary Ethertype as 0x8100. This is the default option of CTAG (C-tag) (0x8100).
STAG		Enter to configure the secondary Ethertype as 0x9100.
QINQ		Enter to configure the secondary Ethertype as
user-defined		Enter to configure the user-defined TPID as VLAN Egress Ethertype. **NOTE:** This value can be set only if user-defined TPID is configured.
loopback		Enter to sets the loopback status for the VLAN interface
enable		Enter to enable loopback feature for the VLAN interface. When loopback is enabled, all data packets received in the vlan will be sent back in the same port from which the packets are received
disable		Enter to disable loopback feature for the VLAN interface. This is default.
unicast-mac		Enter to select unicast MAC.
learning		Enter to select unicast MAC learning. Note that: • VLAN unicast MAC learning limit configuration is allowed only in case of independent VLAN learning mode. • VLAN unicast-MAC learning limit cannot be configured for the VLAN, if the base bridge mode is set as transparent bridging. • The unicast-MAC learning limit set for the VLAN should not exceed the unicast MAC learning limit configured for the switch. • VLAN unicast-MAC learning limit can be configured only in the VLANs that are activated.

Parameter	Type	Description
limit		Enter to configure the unicast-MAC learning limit for a switch. The limit represents the maximum number of distinct unicast MAC addresses that can be learnt in the switch. **NOTE:** The limiting value should not be less than the unicast MAC learning limit set for any of the VLAN **NOTE:** Unicast-MAC learning limit cannot be configured in the switch, if the VLAN switching feature is shutdown in the switch.
<limit value(0-4294967295)>	Integer	Enter a value for the learning limit. The limit represents the maximum number of distinct unicast MAC addresses that can be learnt in the switch. This value ranges from 0 to 4294967295. he maximum number of unicast MAC addresses that can be learnt is 950. The maximum limit that can be configured for a VLAN is dependent on the total size available for dynamic unicast entries in the forwarding table and on the maximum number of VLANs that can be supported.

Mode

VLAN Configuration Mode

Examples

iS5comm(config-vlan)# vlan active

iS5comm(config-vlan)# unicast-mac learning limit 300

iS5comm(config-vlan)# vlan egress ether-type CTAG

iS5comm(config-vlan) # vlan loopback enable

21.47. vlan

To create a VLAN / VFI ID and enter into the config-VLAN mode in which VLAN specific configurations are done or configure the global MAC learning mode, use the command **vlan** in Global Configuration Mode. The no form of the command deletes the existing VLAN/ VFI and its corresponding configurations. Static ARP cache entry related to the static MAC address of this specific VLAN should be removed while removal of static VLAN.

vlan

```
vlan {learning mode {hybrid | svl | ivl} | <vlan_vfi_id>}
```

no vlan

```
no vlan <vlan_vfi_id>}
```

Parameters

Parameter	Type	Description
`learning`		Enter to configure the VLAN learning mode to be applied for all ports of the switch.
`mode`		Enter to configure the VLAN learning mode to be applied for all ports of the switch. This mode defines the forwarding database modes of operation to be implemented by the switch.
`hybrid`		Enter to set the VLAN learning mode as hybrid. Same forwarding database is created for some VLANs and separate forwarding database is used for some VLANs. The usage of same or separate forwarding database for the VLAN is decided based on the static unicast MAC address in the FDB table entries.
`ivl`		Enter to set the VLAN learning mode as Independent VLAN learning (IVL). Separate forwarding database is created for each VLAN. The information learnt from a VLAN is not shared among other relative VLANs during forwarding decisions. This mode is suitable in situations where the database size is not a constraint and end stations operate over multiple VLANs with the same MAC address. This is the default mode.
`svl`		Enter to set the VLAN learning mode as Shared VLAN learning (SVL). Single forwarding database is created for all VLANs. The information learnt from a VLAN is shared among all other relative VLANs during forwarding decision. This mode is suitable in situations where the learning database size is a constraint.

Parameter	Type	Description
<vlan_vfi_id>		Enter to create a VLAN / VFI ID and enters into the config-VLAN mode in which VLAN specific configurations are done. This command directly enters into the config-VLAN mode for the specified VLAN / VFI ID, if the VLAN is already created. • <vlan –id> - This is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535 **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wild-card match for the VID in management operations or Filtering Data-base entries **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the manage-ment interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

Mode

Global Configuration Mode

Default

By default, VLAN 1 is created

learning mode - ivl

Prerequisites

The VLAN learning mode cannot be configured in the switch, if the VLAN switching feature is shut down in the switch.The Native VLAN (VLAN 1) created by default cannot be deleted using the no form of the command.

For default VLAN 1, interface VLAN configuration alone is permitted and no other configuration on this VLAN is allowed, if the base bridge mode is set as transparent bridging. No new VLAN can be created, if the base bridge mode is set as transparent bridging

The creation of new VLAN and configuration of existing VLAN can be done, only if the VLAN switching feature is started and enabled in the switch.

Examples

iS5comm(config)# vlan 4

iS5comm(config)# vlan learning mode hybrid

iS5comm(config-vlan)#

IP

22. IP

IP (Internet Protocol) is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. example: 10.5.25.180.

Every computer that communicates over the Internet is assigned an IP address that uniquely identifies the device and distinguishes it from other computers on the Internet. Within an isolated network, IP addresses can be assigned at random if each one is unique. However, to connect a private network to the Internet, registered IP addresses must be used (called Internet addresses) to avoid duplicates. The four numbers in an IP address are used in different ways to identify a particular network and a host on that network.

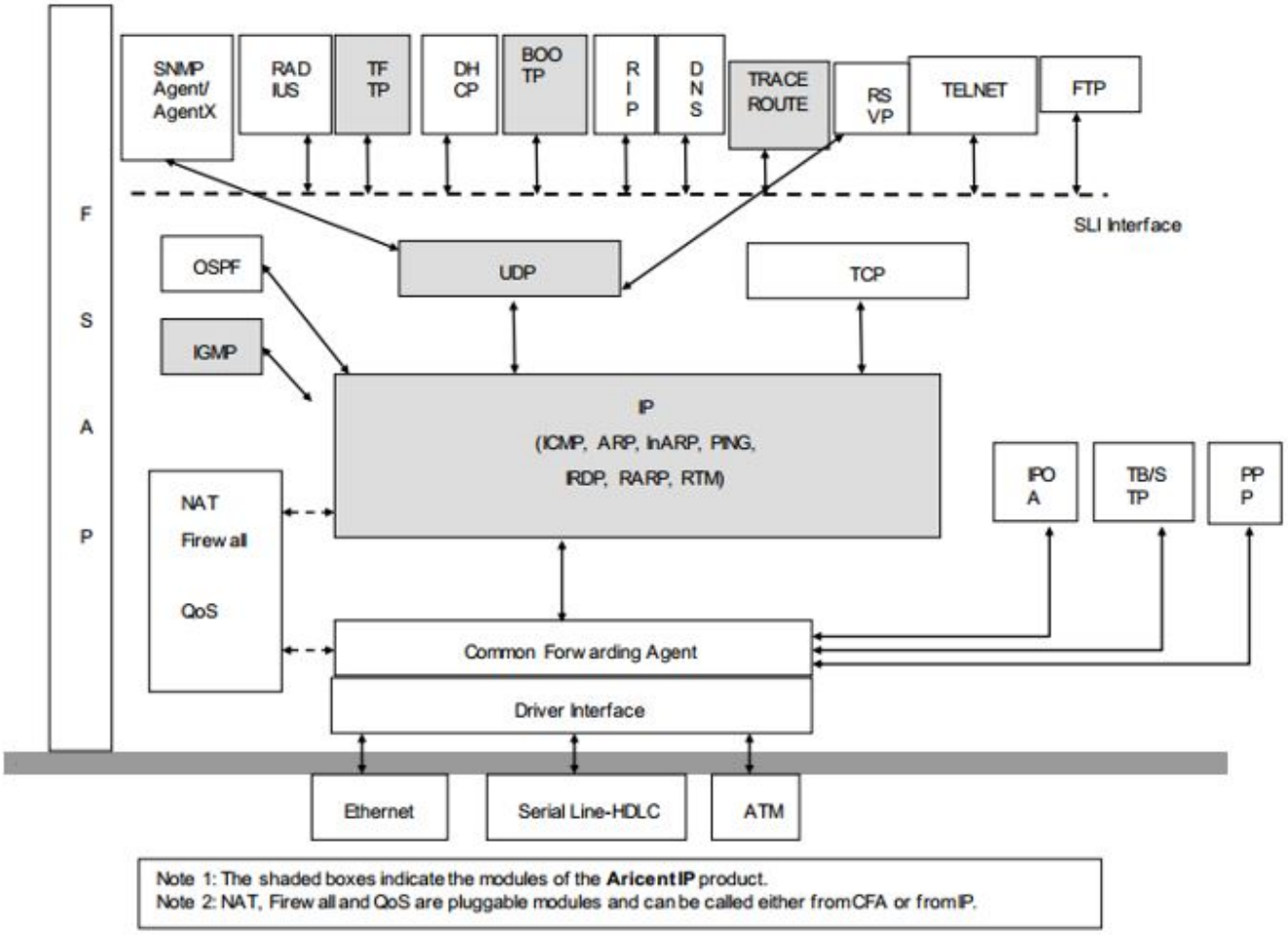
Four regional Internet registries—ARIN, RIPE NCC, LACNIC, and APNIC—assign Internet addresses from the following three classes.

- Class A - supports 16 million hosts on each of 126 networks
- Class B - supports 65,000 hosts on each of 16,000 networks
- Class C - supports 254 hosts on each of 2 million networks

The number of unassigned Internet addresses is running out, so a new classless scheme called CIDR (Classless Inter-Domain Routing) is gradually replacing the system based on classes A, B, and C and is tied to adoption of IPv6. ICMP (Internet Control Message Protocol) is an extension to the IP defined by RFC 792. ICMP supports packets containing error, control, and informational messages. For example, the ping command uses ICMP to test an Internet connection.

The IP implements all components required for IP forwarding. The various components of the IP include ARP, RARP, RTM, ICMP, IRDP, IGMP, InARP, BOOTP, TFTP, TRACE ROUTE, PING and UDP.

Figure 1: Product Positions in the IP Stack



22.1. arp

To add a static entry in the ARP cache or set the ARP (Address Resolution Protocol) cache timeout, use the command **arp** in Global Configuration Mode. The no form of this command resets ARP cache timeout to its default value or deletes a static entry from the ARP cache.

arp

```
arp {<ip address> <hardware address>
 | {Vlan <vlan-id/vfi-id>
 | <interface-type> <interface-id>
 | Linuxvlan <interface-name>
 | Cpu0
 | <IP-interface-type> <IP-interface-number>}
 | timeout <seconds (30-86400)>
```

no arp

```
no arp timeout {<ip address> | access-list <access-list-name>}
```

Parameters

Parameter	Type	Description
<ip address>		Enter a value to defines the IP address or IP alias to map to the specified MAC address.
<hardware address>		Enter a value to defines the MAC address to map to the specified IP address or IP alias. For example, aa:aa:aa:aa:aa:aa
vlan		Enter to create a VLAN / VFI ID and enters into the config-VLAN mode in which VLAN specific configurations are done. This command directly enters into the config-VLAN mode for the specified VLAN / VFI ID, if the VLAN is already created
<vlan_vfi_id>	Integer	Enter a value for VLAN or VFI ID: • <vlan –id> - This is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535 **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wild-card match for the VID in management operations or Filtering Database entries **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

Parameter	Type	Description
<interface-type>		Enter to add a static entry in the ARP cache for the specified interface. The types of interface are as follows: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. • sisp – <ifnum> interface number • pw -<ifnum> interface number • ac - <ifnum> interface number
<interface-id>		Enter to configure a specific slot number / port number to be added. For interface type other than internal-lan, virtual and port-channel, the format is <0>/<1-28> without spaces between Slot Number/Port Number. For example, 0/1. Only i-lan, virtual or port-channel ID is provided, for interface types internal-lan, virtual and port-channel.
Linuxvlan		Enter to configure the Linux VLAN Interface.
<interface-name>		Enter a value to configure the Linux VLAN Interface.
Cpu0		Enter to set the Out of Band Management Interface for the route.
<IP-interface-type>		Enter to add a static entry in the ARP cache for the specified L3 Pseudo wire interface in the system.
<IP-interface-number>		Enter a static entry in the ARP cache for the specified L3 Pseudo wire interface identifier. This is a unique value that represents the specific interface. This value ranges from 1 to 65535 for Pseudowire interface. **NOTE:** Maximum number of Pseudowire interfaces supported in the system is 100.
timeout		Enter to set the ARP (Address Resolution Protocol) cache timeout. The arp timeout defines the time period for which an ARP entry remains in the cache. When a new timeout value is assigned, it only affects the new ARP entries. All older entries retain their old timeout values.

Parameter	Type	Description
<seconds (30-86400)>		Enter a value to configure the ARP cache timeout value. This value ranges from 30 to 86400 seconds with a default of 7200. The timeout values can be assigned to dynamic ARP entries only.

Mode

Global Configuration Mode

Prerequisites

Interface must be a router port

Examples

is5comm(config)# arp timeout 35

is5comm(config)# arp 12.0.0.5 00:11:22:33:44:55 Vlan 1

22.2. clear ip arp

To clear dynamically learnt ARP entries, use the command **clear ip arp** in Global Configuration Mode.

clear ip arp

```
clear ip arp
```

Mode

Global Configuration Mode

Examples

iS5comm(config)# clear ip arp

22.3. ip aggregate-route

To set the maximum number of aggregate routes, use the command **ip aggregate-route** in Global Configuration Mode. The no form of this command sets the maximum number of aggregate routes to its default value. Aggregate Route-based IP switching is achieved by creating a virtual circuit along the network by selecting the forwarding paths used by routers that use OSPF (Open Shortest Path First Protocol). The

data is sent through these virtual circuit to the destination. The routing process is skipped along this circuit. The data is tagged with a label that is read by the switches and forwarded to the destination.

ip aggregate-route

```
ip aggregate-route <value(5-4095)>
```

no ip aggregate-route

```
no ip aggregate-route
```

Parameters

Parameter	Type	Description
<value (5-4095)>	Integer	Enter a value for the maximum number of aggregate routes. This value ranges from 5 to 4095.

Mode

Global Configuration Mode

Default

10

Examples

iS5comm(config)# ip aggregate-route 500

22.4. ip arp max-retries

To define the maximum number of ARP requests that the switch generates before deleting an unresolved ARP entry, use the command **ip arp max-retries** in Global Configuration Mode. The no form of this command sets the maximum number of ARP request retries to its default value.

ip arp max-retries

```
ip arp max-retries <value (2-10)>
```

no ip arp max-retries

```
no ip arp max-retries
```

Parameters

Parameter	Type	Description
<value (2-10)>		Enter a value for the maximum number of ARP request entries. This value ranges from 2 to 10.

Mode

Global Configuration Mode

Default

3

Examples

iS5comm(config)# ip arp max-retries 2

22.5. ip default-distance

To configure the default administrative distance for static IPv4 routes, use the command **ip default-distance** in Global Configuration Mode.

ip default-distance

```
ip default-distance <distance (1-255)>
```

Parameters

Parameter	Type	Description
<distance (1-255)>	Integer	Enter a value to configure the administrative distance for the specified next hop address or the interface. This value ranges from 1 to 255.

Mode

Global Configuration Mode

Default

1

Examples

iS5comm(config)# ip default-distance 10

22.6. ip default-ttl

To set the Time-To-Live (TTL) value, use the command **ip default-ttl** in Global Configuration Mode. The no form of this command sets the TTL to the default value.

ip default-ttl

```
ip default-ttl <value (1-255)>
```

no ip default-ttl

```
no ip default-ttl
```

Parameters

Parameter	Type	Description
<value (1-255)>	Integer	Enter a value for the Time-To-Live (TTL) value. TTL is the time set for a unit of data (a packet) to remain in the network or computer before it could be discarded. This value ranges from 1 to 255 seconds.

Mode

Global Configuration Mode

Default

64

Examples

iS5comm(config)# ip default-ttl 1

22.7. ip directed-broadcast

To enable forwarding of directed broadcasts, use the command **ip directed-broadcast** in Interface Configuration Mode. The no form of this command disables the forwarding of directed broadcasts. The IP directed broadcast is an IP packet whose destination is a valid IP subnet address, but with a source from a node outside the destination subnet. The routers from outside the subnet forward the IP directed broadcast like any other IP packet. When the directed packet reaches a router in the destination subnet,

the packet is exploded as a broadcast in the subnet. The header information on the broadcast packet is rewritten for the broadcast address in the subnet. The packet is sent as link-layer broadcast.

ip directed-broadcast

```
ip directed-broadcast
```

no ip directed-broadcast

```
no ip directed-broadcast
```

Mode

Interface Configuration Mode

Default

Disabled

Examples

iS5comm(config)# int vlan 1

is5comm(config-if)# ip directed-broadcast

22.8. ip echo-reply

To enable sending ICMP Echo Reply messages, use the command **ip echo-reply** in Global Configuration Mode. The no form of this command disables sending ICMP Echo Reply messages. The “ip echo reply” is a message sent by a device in response to a request sent by another device. This message is used to check if a device is able to communicate (send and receive data) with the destination device.

ip echo-reply

```
ip echo-reply
```

no ip echo-reply

```
no ip echo-reply
```

Mode

Global Configuration Mode

Default

Sending of ICMP Echo Reply messages is enabled.

Examples

iS5comm(config)# ip echo-reply

22.9. ip mask-reply

To enable sending ICMP Mask Reply messages, use the command **ip mask-reply** in Global Configuration Mode. The no form of this command disables sending ICMP Mask Reply messages. The IP mask reply is an ICMP message sent with the subnet mask of the network by the router to the host. This reply is in correspondence to a request sent by the host seeking the subnet mask of the network.

ip mask-reply

```
ip mask-reply
```

no ip mask-reply

```
no ip mask-reply
```

Mode

Global Configuration Mode

Default

Sending of ICMP Mask Reply messages is enabled.

Examples

iS5comm(config)# ip mask-reply

22.10. ip path

To initiate path MTU (Maximum Transmission Unit) discovery and configure the MTU for usage in path MTU (PMTU) discovery, use the command **ip path** in Global Configuration Mode. The no form of this command sets MTU for usage in PMTU Discovery and resets PMTU discovery to its default value.

ip path

```
ip path mtu {discover | <dest ip> <tos(0-255)> <mtu(68-65535)>}
```

no ip path

```
no ip path mtu {discover | <dest ip> <tos(0-255)>}
```

Parameters

Parameter	Type	Description
mtu		Enter to set the MTU for usage in PMTU discovery.
discover		Enter to initiate path MTU (Maximum Transmission Unit) discovery. When IP path MTU discover is set to disabled, PMTU-D is not done even if the application requests to do so. When MTU is set to discover, PMTU discovery is enabled.
<dest ip>		Enter a value to set the destination IP address. This is done to define the path between a source and destination.
<tos(0-255>	Integer	Enter a value to set the Type of Service of the configured route. This value ranges from 0 to 255.
<mtu(68-65535)>	Integer	Enter a value to set the Maximum Transmission Unit for the path from the source to the destination. This value ranges from 68 to 65535.

Mode

Global Configuration Mode

Default

Path MTU discovery is disabled.

Prerequisites

The command ip path mtu <dest ip> <tos(0-255)> <mtu(68-65535)> is executed only if,

- PMTU discovery is enabled, or the following command has been executed first:

iS5comm(config)# ip path mtu discover

Examples

iS5comm(config)# ip path mtu discover

is5comm(config)# ip path mtu 10.0.0.1 0 1800

22.11. ip proxy-arp

To enable proxy ARP for the interface, use the command **ip proxy-arp** in Interface Configuration Mode. The no form of this command disables proxy ARP for the interface.

ip proxy-arp

```
ip proxy-arp
```

no ip proxy-arp

```
no ip proxy-arp
```

Mode

Interface Configuration Mode

Default

Proxy ARP is disabled

Examples

iS5comm(config)# int vlan 2

is5comm(config-if)# ip proxy-arp

22.12. ip proxyarp-subnetoption

To enable proxy ARP subnet check, use the command **ip proxyarp-subnetoption** in Global Configuration Mode. When subnet check is enabled, iS5Com acts as ARP proxy for target address in different subnet. The no form of this command disables proxy ARP subnet check. iSS acts as ARP proxy for target address in same or different subnet that is used in IP-DSLAM (Digital Subscriber Line Access Multiplexer) case, when subnet check is disabled.

ip proxyarp-subnetoption

```
ip proxyarp-subnetoption
```

no ip proxyarp-subnetoption

```
no ip proxyarp-subnetoption
```

Mode

Global Configuration Mode

Default

Proxy ARP subnet check is enabled

Examples

is5comm(config)# ip proxyarp-subnetoption

22.13. ip rarp client

To enable RARP (Reverse Address Resolution Protocol) client, use the command **ip rarp client** in Global Configuration Mode. The no form of this command disables the RARP client. The RARP resolves an IP address from a given hardware address. The client that requests for the IP is the RARP client. The IP address of the default interface is obtained through RARP, when the IP address configuration mode is dynamic. After finishing the RARP Max retries, IP is obtained through DHCP (Dynamic Host Configuration Protocol).

ip rarp client

```
ip rarp client
```

no ip rarp client

```
no ip rarp client
```

Mode

Global Configuration Mode

Default

Enabled

Prerequisites

The RARP server must be disabled when the RARP client is enabled.

Examples

iS5comm(config)# ip rarp client

22.14. ip redirects

To enable sending Internet Control Message Protocol (ICMP Redirect) messages, use the command **ip redirects** in Global Configuration Mode. The no form of this command disables sending ICMP Redirect messages. The Redirect Message is an ICMP message which notifies a host to update its routing information to send packets on an alternate route when a packet enters an IP interface and exits the same interface. The redirect message is sent to inform the host of the presence of alternative route.

ip redirects

```
ip redirects
```

no ip redirects

```
no ip redirects
```

Mode

Global Configuration Mode

Default

Sending of ICMP Redirect messages is enabled.

Examples

iS5comm(config)# ip redirects

22.15. ip unreachables

To enable the router to send an ICMP unreachable message to the source if the router receives a packet that has an unrecognized protocol or no route to the destination address, use the command **ip unreachables** in Global Configuration Mode. The no form of this command disables sending ICMP unreachable messages. ICMP provides a mechanism that enables a router or destination host to report an error in data traffic processing to the original source of the packet. This informs the source that the packet is dropped.

ip unreachables

```
ip unreachables
```

no ip unreachables

```
no ip unreachables
```

Mode

Global Configuration Mode

Default

Sending of ICMP unreachable messages is enabled.

Examples

iS5comm(config)# ip unreachables

22.16. ipv4 enable

To enable IPv4 processing on the interface that has not been configured with an explicit IPv4 address, use the command **ipv4 enable** in Interface (VLAN) Configuration Mode. When subnet check is enabled, iS5Com acts as ARP proxy for target address in different subnet. The no form of this command disables IPv4 processing on the interface.

ipv4 enable

```
ipv4 enable
```

no ipv4 enable

```
no ipv4 enable
```

Mode

Interface (VLAN) Configuration Mode

Default

enable

Examples

is5comm(config-if)# ipv4 enable

22.17. maximum-paths

To set the maximum number of paths that can be connected to a host, use the command **maximum-paths** in Global Configuration Mode. The no form of this command sets the maximum number of paths to its default value. The command provides multiple forwarding paths for data traffic and enables load balancing. It improves the overall network fault tolerance, as a failure in one instance does not affect the other instances.

maximum-paths

```
maximum-paths <value (1-16)>
```

no maximum-paths

```
no maximum-paths
```

Parameters

Parameter	Type	Description
<value (1-16)>		Enter a value for the maximum number of multi paths.

Mode

Global Configuration Mode

Default

Maximum number of multi paths is set as 2.

Examples

iS5comm(config)# maximum-paths 15

22.18. ping

To send echo messages, use the command **ping** in Privileged EXEC Mode. The Packet Internet Groper (PING) module is built based on the ICMP echo request and ICMP echo response messages. The network administrator uses ping on a remote device to verify its presence. PING involves sending ICMP echo messages repeatedly and measuring the time between transmission and reception of message. The output displays the time taken for each packet to be transmitted, number of packets transmitted, number of packets received, and packet loss percentage.

ping

```
ping <IpAddress> cybsec
 [ip] {<IpAddress> | <dns_host_name>}
 [data <data (0-65535)>]
 [df-bit]
 [{repeat | count} <packet_count (1-10)>]
 [size <packet_size (36-2080)>]
 [timeout <time_out (1-100)>]
 [validate]
```

Parameters

Parameter	Type	Description
<IpAddress>		Enter an IP address to which the messages will be sent.
cybsec		Enter for cyber security application.
ip		Enter a value to set the destination IP address. This is done to define the path between a source and destination.
<dns_host_name>		Enter a value to configure the name of the host.
data		Enter to configure the size of data to be pinged.
<data (0-65535)>		Enter a value for the number of times the given node address is to be pinged. This value ranges from 68 to 65535.
df-bit		Enter to specify whether or not the Dont Fragment (DF) bit is to be set on the ping packet.
repeat		Enter to configure the number of ping messages to be repeated.
count		Enter to configure the number of times the given node address is to be pinged.
<packet_count (1-10)>		Enter a value for the number of times the given node address is to be pinged or the number of messages to be repeated. This value ranges from 1-10.
size		Enter to configure the size of the data portion of the PING PDU.
<packet_size (36-2080)>		Enter a value for the data portion of the PING PDU. This value ranges from 36 to 2080.
timeout		Enter to configure the time in seconds after which the entity waiting for the ping response times out.
<time_out (1-100)>		Enter a value to set the Maximum Transmission Unit for the path from the source to the destination. This value ranges from 68 to 65535.
validate		Enter to configure to validate the reply data.

Mode

Privileged EXEC Mode

Default

- size—64

- count—3
- timeout—1

Examples

iS5comm(config)# ping 192.168.10.10 validate

```
Reply Received From :192.168.10.10, TimeTaken : 3 msecs
Reply Received From :192.168.10.10, TimeTaken : 3 msecs
Reply Received From :192.168.10.10, TimeTaken : 5 msecs
--- 192.168.10.10 Ping Statistics ---
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
```

22.19. show ip default-distance

To display the default administrative distance for static IPv4 routes, use the command **show ip default-distance** in Privileged EXEC Mode.

show ip default-distance

```
show ip default-distance
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show ip default-distance

```
IP Default Administrative distance: 10
```

22.20. show ip proxy-arp

To display the status of the proxy ARP for all created interfaces, use the command **show ip proxy-arp** in Privileged EXEC Mode.

show ip proxy-arp

```
show ip proxy-arp
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show ip proxy-arp

```
PROXY ARP Status
----------------
vlan1      : Disabled
---------------------
```

22.21. traffic-share

To enable enables traffic sharing (load sharing of IP packets), use the command **traffic-share** in Global Configuration Mode. The no form of this command disables traffic sharing. Traffic sharing is the process by which the protocols select the route for traffic flow with regard to path cost calculation and load distribution. EIGRP (Enhanced Interior Gateway Routing Protocol) provides intelligent traffic sharing. Traffic sharing is controlled by selecting the mode of distribution. Traffic-share balanced distributes the traffic proportionately to the ratio of the metrics of different routes. The traffic-share min distributes the traffic in the route which has minimal cost path even if different paths are available.

traffic-share

```
traffic-share
```

no traffic-share

```
no traffic-share
```

Mode

Global Configuration Mode

Default

Load sharing is disabled

Examples

iS5comm(config)# traffic-share

22.22. debug ip arp

To set the debug level for ARP module and generate debug statements for the specified trace level or for all traces, use the command **debug ip arp** in Privileged EXEC Mode. The no form of the command disables the tracing in ARP module.

debug ip arp

```
debug ip arp {all | init | data | control | dump | os | mgmt | failure |
buffer}
```

no debug ip arp

```
no debug ip arp {all | init | data | control | dump | os | mgmt | failure |
buffer}
```

Parameters

Parameter	Type	Description
`all`		Enter to generate debug statements for all kinds of traces.
`init`		Enter to generate debug statements for initialization and shutdown traces.
`data`		Enter to generate debug statements for data path traces. T
`control`		Enter to generate debug statements for control path traces.
`dump`		Enter to generate debug statements for packet dump traces. This trace is currently not used in GARP module
`os`		Enter to generate debug statements for OS resource related traces. This trace is generated during failure in message queues.
`mgmt`		Enter to generate debug statements for management traces.
`failure`		Enter to generate debug statements for all kind of failure traces.
`buffer`		Enter to generate debug statements for buffer related traces.

Mode

Privileged EXEC Mode

Default

Tracing is disabled.

Examples

iS5comm# debug ip arp all

22.23. ip route

To add a static route, use the **ip route** command in Global Configuration Mode. The route defines the IP address or interface through which the destination can be reached. The no form of this command deletes a static route. If the static route is configured without any metric value, the route will be configured with metric value 1.

ip route

```
ip route <ucast_addr> <ip_mask> <next-hop> [<distance_value (1-255)>]
[cybsec] [private]

 <ucast_addr> <ip_mask> {<next-hop> | vlan <vlan-id/vfi-id> [switch
<switch-name>] [<next-hop>] | {Gigabitethernet <interface-id> |
Extreme-ethernet <interface-id> [<next-hop>] | Linuxvlan <interface-name> |
Cpu0 | tunnel <tunnel-id (0-128)> | <IP-interface-type> <IP-inter-
face-number> | ppp <1-10>} [<distance_value (1-255)>] [private] [permanent]
[name <nexthop-name>]
```

no ip route

```
no ip route <ucast_addr> <ip_mask> <next-hop> [<distance_value (1-255)>]
[cybsec] [private]

 <ucast_addr> <ip_mask> {<next-hop> | vlan <vlan-id/vfi-id> [switch
<switch-name>] [<next-hop>] | {Gigabitethernet <interface-id> |
Extreme-ethernet <interface-id> [<next-hop>] | Linuxvlan <interface-name> |
Cpu0 | tunnel <tunnel-id (0-128)> | <IP-interface-type> <IP-inter-
face-number> | ppp <1-10>} [<distance_value (1-255)>] [private] [permanent]
[name <nexthop-name>]
```

Parameters

Parameter	Type	Description
<ucast_addr>	A.B.C.D	Enter to configure unicast destination IP address; 0.0.0.0 is IP address for a default route
<ip_mask>	A.B.C.D	Enter to configure a subnet mask for the destination; 0.0.0.0 is subnet mask for a default route
<next-hop>		Enter to configure the IP address or IP alias of the next hop that can be used to reach that network
cybsec		Enter for configure security application
<distance_value (1-255)>	Integer	Enter to configure the Administrative distance for the specified next hop address or the interface. This value ranges from 1 to 255. The default is 1.
private		Enter to configure a private route
<ucast_addr>	A.B.C.D	Enter to define unicast destination IP address; 0.0.0.0 is IP address for a default route
<ip_mask>	A.B.C.D	Enter to configure a subnet mask for the destination; 0.0.0.0 is subnet mask for a default route
<next-hop>		Enter to configure the IP address or IP alias of the next hop that can be used to reach that network
vlan		Enter for configure a vlan option.
<vlan-id/vfi-id>		specify the range of the specified VLAN ID This is a unique value that represents the specific VLAN created and activated. The range (1-4094) is for VLAN ID and the range (4096 - 65535) is for VFI. Note that if router ports are used then correspondingly the last set of vlans will not be available. For example, if router ports is 24, then max VLAN number will be 4070 only
switch		Enter to configure name of the switch.
<switch-name>		Enter a name for the switch.
<next-hop>		Enter to configure the IP address or IP alias of the next hop that can be used to reach that network
Gigabitethernet <interface-id>		Enter to select Gigabit Ethernet interface. Gigabit Ethernet interface is a version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. Specify the interface ID with a format <0>/<1-28>—slot number/port number

Parameter	Type	Description
Extreme-Ethernet <interface-id>		Enter to select Extreme Ethernet interface. Extreme Ethernet interface is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. Specify the interface ID with a format <0>/<1-28>—slot number/port number
Linuxvlan		Enter to specify Linux VLAN interface related configuration.
<interface-name>		Enter a name for the Linux VLAN Interface.
Cpu0		Enter to set the Out of Band Management Interface for the route.
tunnel		Enter to configure the static route for the specified Tunnel Identifier.
<tunnel-id (0-128)>		Enter a value for tunnel Identifier. This value ranges from 0 to 128.
<IP-interface-type>		Enter to configures the static route for the specified L3 Pseudo wire interface in the system
<IP-interface-number>		Enter a value that represents the specific interface. This value ranges from 1 to 65535 for Pseudowire interface.
ppp		Enter to configure the PPP (point-to-point protocol) interface for the route.
<1-10>		Enter a value for PPP. The value ranges from 1 to 10
<distance_value (1-255)>	Integer	Enter to configure the Administrative distance for the specified next hop address or the interface. This value ranges from 1 to 255. The default is 1.
private		Enter to configure a private route
permanent		Enter to configure a switch name /context name; option default is available now.
name		Enter to configure a next hop name.
<nexthop-name>		Enter a next hop name.

Mode

Global Configuration Mode

Prerequisites

Interface must be a router port.

Examples

iS5comm (config)# ip route 30.0.0.2 255.255.255.255 vlan 1

iS5comm (config)# ip route 30.0.0.2 255.255.255.255 gi 0/2 12.2

22.24. ip routing

To enable IP routing, use the command **ip routing** in Global Configuration Mode. The no form of this command disables IP routing. IP routing is the path defined by set of protocols for the data to follow across multiple networks from source to its destination. When an IP packet is to be forwarded, the router uses its forwarding table to determine the next hop address. The header in the IP packet has the next hop information.

ip routing

```
ip routing
```

no ip routing

```
no ip routing
```

Mode

Global Configuration Mode

Default

IP routing is enabled

Examples

iS5comm(config)# ip routing

22.25. show ip arp

To display the IP ARP table, use the **show ip arp** command in Privileged EXEC Mode.

show ip arp

```
show ip arp [{vlan <vlan-id/vfi-id> [switch <switch-name>] | {Gigabiteth-
ernet <interface-id> | Extreme-ethernet <interface-id> | <ipiftype> <ifnum>
| <ip-address> | <mac-address> | summary | information | statistics}]
```

Parameters

Parameter	Type	Description
vlan		Enter for configure a vlan option to be displayed.
<vlan-id/vfi-id>	Integer	Enter to specify the range of the specified VLAN ID to be displayed. This is a unique value that represents the specific VLAN created and activated. The range (1-4094) is for VLAN ID and the range (4096 - 65535) is for VFI. Note that if router ports are used then correspondingly the last set of vlans will not be available. For example, if router ports is 24, then max VLAN number will be 4070 only
switch		Enter to configure name of the switch to be displayed.
<switch-name>		Enter a name for the switch to be displayed.
Gigabitethernet <interface-id>		Enter to select Gigabit Ethernet interface to be displayed. Gigabit Ethernet interface is a version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. Specify the interface ID with a format <0>/<1-28>—slot number/port number
Extreme-Ethernet <interface-id>		Enter to select Extreme Ethernet interface to be displayed. Extreme Ethernet interface is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. Specify the interface ID with a format <0>/<1-28>—slot number/port number
<ipiftype>		Enter to display the IP ARP information for the specified L3 Pseudo wire interface in the system.
<ifnum>	Integer	Enter to display the IP ARP information for the specified L3 Pseudo wire interface identifier. This is a unique value that represents the specific interface. This value ranges from 1 to 65535 for Pseudowire interface. **NOTE:** Maximum number of Pseudowire interfaces supported in the system is 100.
<ip-address>		Enter to display the IP Address of ARP Entry
<mac-address>		Enter to display the MAC Address of ARP Entry
summary		Enter to display IP ARP Table summary.
information		Enter to display the ARP Configuration information regarding maximum retries and ARP cache timeout.
statistics		Enter to display the ARP statistics.

Mode

Privileged EXEC Mode

Examples

iS5comm # show ip arp

```
Address          Hardware Address   Type  Interface  Mapping
-------          ----------------   ----  ---------  ----
192.168.10.10    54:e1:ad:07:0d:87  ARPA  vlan1   Dynamic
```

22.26. show ip information

To display IP configuration information, use the command **show ip information** in Privileged EXEC Mode.

show ip information

```
show ip information
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show ip information

```
Global IP Configuration:
------------------------
IP routing is enabled
Default TTL is 64
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP echo replies are always sent
ICMP mask replies are always sent
Number of aggregate routes is 50
Number of multi-paths is 2
Load sharing is disabled
Path MTU discovery is enabled
```

22.27. show ip pmtu

To display the configured PMTU entries, use the command **show ip pmtu** in Privileged EXEC Mode. The details include Destination IP address, Type of Service (ToS), and Path MTU.

show ip pmtu

```
show ip pmtu
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show ip pmtu

```
    Ip Path MTU Table
    -----------------

    Destination  ToS   PMTU
    -----------  ---   ----

    10.0.0.1         0       1800
```

22.28. show ip proxy-arp

To display the status of the proxy ARP for all created interfaces, use the command **show ip proxy-arp** in Privileged EXEC Mode.

show ip proxy-arp

```
show ip proxy-arp
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show ip proxy-arp

```
    PROXY ARP Status
    ----------------
    vlan1      : Disabled
```

```
--------------------
```

22.29. show ip rarp

To display RARP configurations' information such as maximum number of RARP request retransmission retries and RARP request retransmission timeout, use the command **show ip rarp** in Privileged EXEC Mode. The number of responses discarded are also displayed.

show ip rarp

```
show ip rarp
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show ip rarp

```
RARP Configurations:
--------------------
Maximum number of RARP request retransmission retries is 4
RARP request retransmission timeout is 100 seconds
RARP Statistics:
---------------
0 responses discarded
```

22.30. show ip route

To display the IP routing table, use the **show ip route** command in Privileged EXEC Mode.

show ip route

```
show ip route
 [{<ip-address> [<mask>] | bgp | connected | ospf [cybsec] | rip | static |
summary | details | isis | failed | cybsec}]
 hardware
```

Parameters

Parameter	Type	Description
<ip-address>		Enter to configure the IP routing table for the specified destination IP Address to be displayed.
mask		Enter for the IP routing table for the specified prefix mask address to be displayed.
bgp		Enter to specify the Border Gateway Protocol if it is used by the table to get route information to be displayed.
connected		Enter for the Directly Connected Network Routes to be displayed.
ospf		Enter to display the OSPF (Open Shortest Path First) protocol if it is used for getting route information.
rip		Enter to display the RIP (Routing Information Protocol) if it is used for getting route information.
static		Enter to display the Static Routes in the table.
summary		Enter to display the Summary of all routes.
details		Enter to display the information about route status (Route in Hardware, Route Reachable, Best route).
isis		Enter to display the information about the ISIS routes.
failed		Enter to display the NPAPI programming failed routes.
cybsec		Enter to display the cyber security routes including specific to OSPF.
hardware		Enter to display the routes programmed in hardware.

Mode

Privileged EXEC Mode

Examples

iS5comm # show ip route

```
Codes: C - connected, S - static, R - rip, B - bgp, O - ospf, I - isis,
E - ECMP

IA - OSPF inter area, N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
```

```
E2 - OSPF external type 2 L1 - ISIS Level1, L2 - ISIS Level2, ia - ISIS
Inter Ar
ea

---------
C 192.168.10.0/24 is directly connected, vlan1
```

iS5comm # show ip route

```
Cybsec OSPF routes
-------------------
Codes: O - OSPF, > - selected route, * - FIB route

O 192.168.50.0/24 [110/10] is directly connected to vlan50
```

22.31. show ip traffic

To display the IP protocol statistics, use the **show ip traffic** command in Privileged EXEC Mode.

show ip traffic

```
show ip traffic
 [interface {vlan <vlan-id/vfi-id> [switch <switch-name>] | tunnel
<tunnel-id (0-128)> | {Gigabitethernet <interface-id> | Extreme-ethernet
<interface-id> | Linuxvlan <interface-name> | <IP-interface-type> <IP-inter-
face-number>}] [hc]
```

Parameters

Parameter	Type	Description
interface		Enter to configure interface type and number to be displayed.
vlan		Enter for configure a vlan option to be displayed.
<vlan-id/vfi-id>	Integer	Enter to specify the range of the specified VLAN ID to be displayed. This is a unique value that represents the specific VLAN created and activated. The range (1-4094) is for VLAN ID and the range (4096 - 65535) is for VFI. Note that if router ports are used then correspondingly the last set of vlans will not be available. For example, if router ports is 24, then max VLAN number will be 4070 only
switch		Enter to configure name of the switch to be displayed.
<switch-name>		Enter a name for the switch to be displayed.
tunnel		Enter to configure the static route for the specified Tunnel Identifier to be displayed.
<tunnel-id (0-128)>	Integer	Enter a value for tunnel Identifier to be displayed. This value ranges from 0 to 128.
Gigabitethernet <interface-id>		Enter to select Gigabit Ethernet interface to be displayed. Gigabit Ethernet interface is a version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. Specify the interface ID with a format <0>/<1-28>—slot number/port number
Extreme-Ethernet <interface-id>		Enter to select Extreme Ethernet interface to be displayed. Extreme Ethernet interface is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. Specify the interface ID with a format <0>/<1-28>—slot number/port number
Linuxvlan		Enter to specify Linux VLAN interface related configuration to be displayed.
<interface-name>		Enter a name for the Linux VLAN Interface to be displayed.
<IP-interface-type>		Enter to the IP statistics for the specified L3 Pseudo wire interface in the system to be displayed.
<IP-interface-number>		Enter a value that represents the specific interface. This value ranges from 1 to 65535 for Pseudowire interface to be displayed.

Parameter	Type	Description
hc		Enter to display the high counters statistics.

Mode

Privileged EXEC Mode

Examples

iS5comm # show ip traffic

```
IP Statistics
--------------------
Rcvd: 10811 total, 0 header error discards
0 bad ip address discards, 0 unsupported protocol discards
Frags: 0 reassembled, 30 timeouts, 0 needs reassembly 0 fragmented, 0
couldn't fragment
Bcast: Sent: 0 forwarded, 14954 generated requests
Drop: 0 InDiscards 10811 InDelivers 202 InMcastPkts
0 InTruncated 850384 InOctets 0 InNoRoutes
0 ReasmFails 8288 InMcast Octets 0 InBcastPkts
0 OutDiscards 0 OutMcastPkts 0 OutFrgCreates
0 OutForwDgrms 14923 OutTrnsmits 0 OutFrgRqds
3839361 OutOctets 0 OutMcstOctets 0 OutBcstPkts
0 DiscntTime 1000 RefrshRate

ICMP Statistics:
----------------
Rcvd: 0 total, 0 InErrors, 0 unreachable, 0 redirects
0 time exceeded, 0 param problems, 0 quench
0 echo, 0 echo reply, 0 mask requests, 0 mask replies,
0 timestamp , 0 time stamp reply,
Sent: 0 total, 0 OutErrors, 0 unreachable, 0 redirects
0 time exceeded, 0 param problems, 0 quench
0 echo, 0 echo reply, 0 mask requests, 0 mask replies,
0 timestamp , 0 time stamp reply
```

iS5comm # show ip traffic hc

```
IP High Count Statistics
--------------------
34931   InRcvs          2129183 InOctets            0   InFwdDgrms
```

```
    34937   InDelivers      10228   OutRequests         0   OutFwdDgrms
    10217   OutTrnsmits     848106  OutOctets       28159   InMcstPkts
    1666345 InMcstOctets 0   OutMcstPkts         0   OutMcstOctets    0
    InBcast             0   OutBcast
```

22.32. traceroute

To trace a route to the destination IP, use the **traceroute** command in Privileged EXEC Mode.

traceroute

```
traceroute <ip-address> [min-ttl <value (1-99)>] [max-ttl <value (1-99)>]
```

Parameters

Parameter	Type	Description
<ip-address>		Enter to configure the destination IP address to which a route has to be traced.
min-ttl		Enter to configure the minimum value of the TTL (Time-to-Live) field to be filled up in the IP packets used for the trace route.
max-ttl		Enter to configure the maximum value of the TTL field to be filled up in the IP packets used for the trace route.
<value (1-99)>	Integer	Enter a minimum or maximum value of the TTL field to be filled up in the IP packets used for the trace route. This value ranges from 1 to 99 seconds.

Mode

Privileged EXEC Mode

Default

- min-ttl - 1
- max-ttl - 15

Prerequisites

The maximum value of the TTL field should be always greater than the minimum value of the TTL field.

Examples

iS5comm # traceroute ip 12.0.0.100 min-ttl 1 max-ttl 2

```
Tracing Route to 12.0.0.100 with 2 hops max and 1 byte packets

1     0.0.0.0               *               *         *

2     0.0.0.0
```

iS5comm# traceroute ipv6 ffff::dddd min-ttl 1 max-ttl 2

```
Tracing Route to ffff::dddd with 2 hops max and 1 byte packets

1     ::                    *               *               *

2     ::                    *               *               *
```

OSPF

23. OSPF

OSPF (Open Shortest Path First) protocol is an Interior Gateway Protocol used to distribute routing information within a single autonomous system. Routers use link-state algorithms to send routing information to all nodes in an inter-network by calculating the shortest path to each node based on topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations), which describes the state of its own links, and it also sends the complete routing structure (topography).

A router attempting a graceful restart originates link-local Opaque-LSAs, herein called Grace-LSAs, announcing its intention to perform a graceful restart within a specified amount of time or "grace period". During the grace period, its neighbors continue to announce the restarting router in their LSAs as if it were fully adjacent (i.e., OSPF neighbor state Full), but only if the network topology remains static (i.e., the contents of the LSAs in the link-state database having LS types 1-5,7 remain unchanged and periodic refreshes are allowed). There are two roles being played by OSPF routers during graceful restart. First there is the router that is being restarted. Then there are the router's neighbors, which must cooperate in order for the restart to be graceful. During graceful restart, we say that the neighbors are running in "helper mode". For more details, refer to RFC 3623.

The advantage of shortest path first algorithms is that they result in smaller more frequent updates everywhere. They converge quickly, thus preventing such problems as routing loops and count-to-infinity (when routers continuously increment the hop count to a particular network). This makes for a stable network.

Before configuring OSPF, Route Redistribution (RRD) must be enabled. In addition, all OSPF interface related configurations, can be done only when the global OSPF is enabled.

23.1. abr-type

To set alternative ABR (Area Border Router) types, use the command **abr-type** in OSPF Router Configuration Mode. The no form of this command resets the configured alternative ABR type.

abr-type

```
abr-type {cisco | ibm | standard}
```

no abr-type

```
no abr-type
```

Parameters

Parameter	Type	Description
cisco		Enter to configure to CISCO ABR type as defined in RFC 3509.
ibm		Enter to configure to IBM ABR type as defined in RFC 3509.
standard		Enter to configure to Standard ABR type as defined in RFC 2328.

Mode

OSPF Router Configuration Mode

Default

Standard

Prerequisites

- RFC 2328 – OSPF Version 2
- RFC-3509 -- Alternative Implementations of OSPF Area Border Routers.

Examples

iS5comm(config)# router ospf

is5comm(config-router)# abr-type standard

23.2. area

To area related configuration of the OSPF router, use the command **area** in OSPF Router Configuration Mode. The no form of this command deletes the area related configuration or removes OSPF virtual links.

area

```
area {<AreaId> range <Network> <Mask> {summary | Type7} [{advertise |
not-advertise}] [tag <tag-value>]}

 | <area-id>

 { default-cost <cost>[tos <value(0-30)>]

 | nssa [{no-summary | default-information-originate [metric <value
(0-16777215)>] [metric-type <Type(1-3)>] [tos <tos value (0-30)>] [no-redis-
tribution]}]

 | stability-interval <Interval-Value (0 - 0x7fffffff)>
```

```
 | stub [no-summary]

 | translation-role {always | candidate}

 | virtual-link <router-id>

 {[authentication {simple | message-digest | sha-1 | sha-224 | sha-256 |
sha384 | sha-512 |null}]

 [authentication-key <key (8)>

 [message-digest-key <Key-id (0-255)> {md5 | sha-1 | sha-224 | sha-256 |
sha-384 | sha-512} <key(16)>}]

 [dead-interval <value>]

 [hello-interval <value (1-65535)>]

 [key <Key-ID (0-255)> {start-accept <DD-MON-YEAR,HH:MM> | start-generate
<DD-MON-YEAR,HH:MM> | stop-accept <DD-MON-YEAR,HH:MM> | stop-generate
<DD-MON-YEAR,HH:MM>}

 [retransmit-interval <value (1-3600)>]

 [transmit-delay <value (1-3600)>]}

 }
```

no area

```
no area <AreaId> range <Network> <Mask> {summary | Type7}

 <area-id>

 { default-cost <cost>[tos <value(0-30)>]

 | nssa [{no-summary | default-information-originate [metric <value
(0-16777215)>] [metric-type <Type(1-3)>] [[no-summary]}]

 | stability-interval

 | stub [no-summary]

 | translation-role | {stub | nssa}]

 | virtual-link <router-id>

 {[authentication]

 [authentication-key | message-digest-key <Key-id (0-255)>] [dead-interval]
[hello-interval] [retransmit-interval [transmit-delay }
```

NOTE: The no area <area-id> [{stub | nssa}] command removes an area or converts stub/nssa to normal area.The backbone area cannot be set as Stub or NSSA.

Parameters

Parameter	Type	Description
<AreaId>		Enter either a decimal value or as an IP address to configure the area associated with the OSPF address range and the identifier of the area about which routes are to be summarized.
range		Enter to consolidate and summarize routes at an area boundary which is used only with Area Border Routers (ABRs). As a result, a single summary route is advertised to other areas by the ABR. **NOTE:** This command executes only if a particular area is configured as NSSA.
<Network>		Enter an IP address to configure the IP address of the network indicated by the range.
<Mask>		Enter the subnet mask that pertains to the range. The mask indicates the range of addresses being described by the particular route. For example, a summary-LSA for the destination 128.185.0.0 with a mask of 0xffff0000 actually is describing a single route to the collection of destinations 128.185.0.0 - 128.185.255.255.
summary		Enter to set the LSA type as summary LSA.
Type7		Enter to set the LSA type as Type-7 LSA.
advertise		Enter to set the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA). When associated area Id is 0.0.0.0, aggregated Type-5 are generated. For associated other than 0.0.0.0 aggregated Type-7 is generated in NSSA x.x.x.x.
not-advertise		Enter to set the address range status to Not Advertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks When associated area Id is 0.0.0.0, Type-5 is not generated for the specified range, while aggregated Type-7 are generated in all attached NSSA. For associated area Id x.x.x.x which is other than 0.0.0.0, Type-7 are not generated in NSSA x.x.x.x for the specified range.
tag		Enter to configure the Tag Type to describe whether Tags will be generated automatically or manually configured.
<tag-value>	Integer	Enter a tag value. This value ranges from 0 to 2147483647 with a default value of 2.
<area-id>		Enter either a decimal value or as an IP address to configure the identifier for the stub or NSSA. For example, Area ID 0.0.0.0 is used for the OSPF backbone.

Parameter	Type	Description
default-cost		Enter to specify a cost for the default summary route sent into a stub or NSSA. This command is used only on an Area Border Router (ABR) attached to a stub or NSSA. This command provides the metric for the summary default route generated by the ABR into the stub area. A default cost can be defined only for a valid area.
<cost>	Integer	Enter a value for cost of the default summary route used for a stub or NSSA. This value ranges from 0 to 16777215. The default is 1.
tos		Enter to configure the Type of Service of the route being configured. It can be configured only if the code is compiled with TOS Support.
<tos value(0-30)>	Integer	Enter a value for Type of Service of the route being configured. This value ranges from 0 to 30. The default value for TOS is 0.
nssa		Enter to configure a particular area as not-so-stubby area (NSSA).
no-summary		Enter to allow an area to be a not-so-stubby area but not have summary routes injected into it.
default-information-originate		Enter to configure the default route into OSPF used to generate a Type 7 default into the NSSA area.
metric		Enter to configure the Metric value applied to the route before it is advertised into the OSPF domain.
<value (0-16777215)>	Integer	Enter a value for the Metric value applied to the route before it is advertised into the OSPF domain. This value ranges from 0 to 16777215. The default is 10.
metric-type		Enter to configure the Metric Type applied to the route before it is advertised into the OSPF domain.
<Type(1-3)>	Integer	Enter a value for Metric Type applied to the route before it is advertised into the OSPF domain. This value ranges from 1 to 3.The default is 1
tos		Enter to configure the Type of Service of the route being configured. It can be configured only if the code is compiled with TOS Support
<tos value(0-30)>	Integer	Enter a value for Type of Service of the route being configured. This value ranges from 0 to 30. The default value for TOS is 0.
no-redistribution		Enter to disable redistribution of routes from the given protocol into OSPF.

Parameter	Type	Description
stability-interval		Enter to configure the stability interval for NSSA where the Information describing the configured parameters and cumulative statistics of one of the router's attached areas. **NOTE:** This command executes only if NSSA is configured.
<Interval-Value (0 - 0x7fffffff)>	Integer	Enter a value for are no longer required, that it must continue to perform its translation duties. The interval value ranges between 0-0x7fffffff in seconds. The OSPF Sequence Number is a 32 bit signed integer. It starts with the value '80000001'h, -- or -'7FFFFFFF', and increments until '7FFFFFFF'h. Thus, a typical sequence number will be very negative. The default value is 40 seconds.
stub		Enter to configure an area as a stub area and other parameters related to that area. This command is configured on all routers and access servers in the stub area.
no-summary		Enter to prevent an Area Border Router (ABR) from sending summary link advertisements into the stub area by neither originating nor propagating summary LSA into the stub area.
translation-role		Enter to configure the translation role for the NSSA or the NSSA Border router's ability to perform NSSA Translation of Type-7 to Type-5 LSAs. Type-5 LSAs originate from AS (Autonomous system) boundary routers and flood through and out the AS. Each AS-external-LSA describes a route to a destination in another Autonomous System. Default routes for the AS can also be described by AS-external-LSAs.
always		Enter to set a translator role to where the Type-7 LSAs are always translated into Type-5 LSAs.
candidate		Enter to set translator role where an NSSA border router participates in the translator election process. This is default.
virtual-link		Enter to define an OSPF virtual link and its related parameter. In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link. Hello-interval and dead-interval values must be the same for all routers and access servers on a specific network. **NOTE:** This command executes only if area is defined using the network command.
<router-id>		Enter a value for the router ID of the virtual neighbor.
authentication		Enter to configure the authentication type.

Parameter	Type	Description
simple		Enter to set the simple password authentication mechanism.
message-digest		Enter to set the authentication type as message digest authentication mechanism.
sha-1		Enter to set the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes.
sha-224		Enter to set the authentication type as Secure Hash Algorithm 224 (SHA224) authentication. SHA224 generates Authentication digest of length 28 bytes
sha-256		Enter to set the authentication type as Secure Hash Algorithm 256 (SHA256) authentication. SHA256 generates Authentication digest of length 32 bytes.
sha-384		Enter to set the authentication type as Secure Hash Algorithm 384 (SHA384) authentication. SHA384 generates Authentication digest of length 48 bytes
sha-512		Enter to set the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. SHA512 generates Authentication digest of length 64 bytes.
null		Enter to set the no password authentication. This is the default authentication method.
authentication-key		Enter to configure the authentication type.
<key (8)>		Enter to set the simple password authentication mechanism.
message-digest-key		Enter to configure the authentication type.
<Key-id (0-255)>		Enter to set the simple password authentication mechanism.
md5		Enter to set the authentication type as message digest authentication mechanism.
sha-1		Enter to set the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes.
sha-224		Enter to set the authentication type as Secure Hash Algorithm 224 (SHA224) authentication. SHA224 generates Authentication digest of length 28 bytes

Parameter	Type	Description
sha-256		Enter to set the authentication type as Secure Hash Algorithm 256 (SHA256) authentication. SHA256 generates Authentication digest of length 32 bytes.
sha-384		Enter to set the authentication type as Secure Hash Algorithm 384 (SHA384) authentication. SHA384 generates Authentication digest of length 48 bytes
sha-512		Enter to set the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. SHA512 generates Authentication digest of length 64 bytes.
<key(16)>		Enter a value to configure the cryptographic key value which is used to create the message digest appended to the OSPF packet. All neighboring routers on the same network must have the same key identifier and key to route OSPF traffic. This is a string with maximum 16 characters.
dead-interval		Enter to configure the interval at which hello packets must not be seen before its neighbors declare the router down. As with the hello interval, this value must be the same for all routers and access servers attached to a common network.
<value>	Integer	Enter a value for the interval at which hello packets must not be seen before its neighbors declare the router down. The default is 40 seconds.
hello-interval		Enter to configure the interval at which hello packets must not be seen before its neighbors declare the router down. As with the hello interval, this value must be the same for all routers and access servers attached to a common network.
<value (1-65535)>	Integer	Enter a value for the interval at which hello packets must not be seen before its neighbors declare the router down. This value ranges from 1 to 65535 in seconds with a default of 0 seconds.
key		Enter to configure the time the router starts accepting packets that is created with the configured key id.
<Key-ID (0-255)>		Enter a value for the secret key used to create the message digest appended to the OSPF packet. This value ranges from 0 to 255.

Parameter	Type	Description
start-accept		Enter to configure the time when the router will start accepting packets that have been created with the configured key-id. **NOTE:** This command executes only if, • Area is defined using the network command • Authentication key for Message Digest Authentication is configured for the specified area
<DD-MON-YEAR,HH:MM>		Enter a value for the time when the router will start accepting packets that have been created with the configured key-id. This value is the sum of configured time and the system time at which the start-accept value is configured and is configured in 24 hours format. **NOTE:** For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30
start-generate		Enter to configure the time when the router will start generating OSPF packets with the configured key id. **NOTE:** This command executes only if, • Area is defined using the network command • Authentication key for Message Digest Authentication is configured for the specified area
<DD-MON-YEAR,HH:MM>		Enter a value for the time when the router will start generating OSPF packets with the configured key id. This value is the sum of the configured time and the system time at which the start-generate value is configured. Start Generate Time value is configured in 24 hours format. Default value is set as current system time. **NOTE:** For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30
stop-generate		Enter to configure the time when the router will stop generating OSPF packets with the configured key id. **NOTE:** This command executes only if, • Area is defined using the network command • Authentication key for Message Digest Authentication is configured for the specified area

Parameter	Type	Description
<DD-MON-YEAR,HH:MM>		Enter a value for the time when the router will stop generating OSPF packets with the configured key id. Stop Generate value is configured in 24 hours format. Default value is set to the current system time. **NOTE:** For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30
stop-accept		Enter to configure the time when the router will stop accepting OSPF packets with specified key id. **NOTE:** This command executes only if, • Area is defined using the network command • Authentication key for Message Digest Authentication is configured for the specified area
<DD-MON-YEAR,HH:MM>		Enter a value for the time when the router will stop accepting OSPF packets with specified key id. Stop accept value is configured in 24 hours format. **NOTE:** For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30
retransmit-interval		Enter to configure the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPF virtual link interface.
<value (1-3600)>		Enter a value for the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPF virtual link interface. This value ranges from 1 to 3600 in seconds with a default of 5.
transmit-delay		Enter to configure the time in which the router will stop using this key for packets generation. Estimated time required to send a link-state update packet on the interface. Integer value that must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission
<value (1-3600)>		Enter a value for the time in which the router will stop using this key for packets generation. This value ranges from 1 to 3600 in seconds with a default of 1 second.

Mode

OSPF Router Configuration Mode

Examples

iS5comm(config)# router ospf

is5comm(config-router)# area 10.0.0.1 range 10.0.0.0 255.0.0.0 summary advertise tag 10

is5comm(config-router)# area 10.0.0.1 default-cost 5

is5comm(config-router)# area 10.0.0.1 nssa

is5comm(config-router)# area 10.0.0.1 stub

is5comm(config-router)# area 10.0.0.1 stability-interval 10000

is5comm(config-router)# area 10.0.0.1 translation-role always

is5comm(config-router)# area 1.1 virtual-link 0.0.0.1 authentication simple hello-interval 65 retransmit-interval 654 dead-interval 200 message-digest-key 20 sha-512 key11

is5comm(config-router)# area 1.1 virtual-link 0.0.0.1 key 20 start-accept 23-Jun-2014,19:18

is5comm(config-router)# area 1.1 virtual-link 0.0.0.1 key 20 start-generate 23-Jun-2014,19:18

is5comm(config-router)# area 1.1 virtual-link 0.0.0.1 key 20 stop-generate 26-Jun-2014,19:18

is5comm(config-router)# area 1.1 virtual-link 0.0.0.1 key 20 stop-accept 26-Jun-2014,19:18

23.3. ASBR Router

To specify a router as ASBR, use the command **ASBR Router** in OSPF Router Configuration Mode. The no form of this command disables the router as ASBR. A router that act as gateway (redistribution link) between OSPF and other routing protocols (IGRP, EIGRP, RIP, BGP, Static) or other instances of the OSPF routing process is called autonomous system boundary router (ASBR).

ASBR Router

```
ASBR Router
```

no ASBR Router

```
no ASBR Router
```

Mode

OSPF Router Configuration Mode

Examples

iS5comm(config)# router ospf

is5comm(config-router)# ASBR Router

23.4. bfd

To enable Bidirectional Forwarding Detection (BFD) monitoring on all or specific OSPF interfaces, use the command **bfd** in OSPF Router Configuration Mode. The no form of the command disables BFD monitoring on all or specific OSPF interfaces. The BFD protocol is a simple hello mechanism that detects failures in a network. BFD works with a wide variety of network environments and topologies. A pair of routing devices exchange BFD packets, and hello packets are sent at a specified regular interval.

bfd

```
bfd {all-interface | <interface-type> <interface-id> | vlan <vlan-id
(1-4094)> [switch <switch-name>]}
```

no bfd

```
no bfd {all-interface | <interface-type> <interface-id> | vlan <vlan-id
(1-4094)> [switch <switch-name>]}
```

Parameters

Parameter	Type	Description
all-interface		Enter to enable BFD monitoring on all OSPF interfaces.
<interface-type>		Enter an interface type on which BFD monitoring to be enabled.
<interface-id>		Enter an interface identifier on which BFD monitoring to be enabled. The interface identifier is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents a slot number of 0 and port number of 1.
vlan		Enter to enable BFD monitoring on the specified VLAN ID
<vlan-id (1-4094)>	Integer	Enter a VLAN ID on which BFD monitoring is to be enabled. This value ranges from 1 to 4094.
switch		Enter to configure a switch name.
<switch-name>		Enter default for switch name.

Mode

OSPF Router Configuration Mode

Default

BFD is disabled for all interfaces.

Prerequisites

This command can be configured only if bfd is enabled and OSPF is started on the interface.

Examples

iS5comm(config)# router ospf

iS5comm(config-router)# bfd all-interface

is5comm (config-router)# bfd vlan 1 switch default

23.5. capability opaque

To enable the capability of storing opaque LSAs (link state advertisements), use the command **capability opaque** in OSPF Router Configuration Mode. The no form of this command disables the opaque capability. The Opaque LSAs are new class of link state advertisements (LSAs) that provide a generalized mechanism to allow for the future extensibility of OSPF. Opaque LSAs are types 9, 10, and 11 link state advertisements. The link-state ID of the Opaque LSA is divided into an Opaque type field (the first 8 bits) and a type-specific ID (the remaining 24bits). Refer to RFC 5250 for more details.

capability opaque

```
capability opaque
```

no capability opaque

```
no capability opaque
```

Mode

OSPF Router Configuration Mode

Default

Opaque capability is disabled

Examples

iS5comm(config)# router ospf

is5comm(config-router)# capability opaque

23.6. compatible rfc1583

To set OSPF compatibility list compatible with RFC 1583 and control the preference rules when choosing among multiple AS external LSAs advertising the same destination, use the command **compatible rfc1583** in OSPF Router Configuration Mode. The no form of this command disables RFC 1583 compatibility. When such compatibility is enabled, the preference rules remain those specified by RFC 1583. When the compatibility is set to disabled, the preference rules are those stated in RFC 2178.

compatible rfc1583

```
compatible rfc1583
```

no compatible rfc1583

```
no compatible rfc1583
```

Mode

OSPF Router Configuration Mode

Default

OSPF is Compatible

Examples

iS5comm(config)# router ospf

is5comm(config-router)# compatible rfc1583

23.7. debug ip ospf

To set OSPF debug level, use the command **debug ip ospf** in Privileged EXEC Mode. The no form of the command removes OSPF related configuration.

debug ip ospf

```
debug ip arp {pkt {hp | ddp | lrq | lsu | lsa} | module {adj_formation | ism
| nsm | config | interface | restarting-router | helper | redundancy}
```

no debug ip ospf

```
no debug ip ospf [pkt {hp | ddp | lrq | lsu | lsa] [module {adj_formation |
ism | nsm | config | interface | restarting-router | helper | redundancy]
[all]
```

Parameters

Parameter	Type	Description
pkt		Enter to generate debug statements for Packet High Level Dump traces.
hp		Enter to generate debug statements for DDP (Datagram Delivery Protocol) packet traces.
lrq		Enter to generate debug statements for Link State Request Packet traces.
lsu		Enter to generate debug statements for Link State Update Packet traces.
lsa		Enter to generate debug statements for Link State Acknowledge Packet traces
module		Enter to generate debug statements for RTM Module traces.
adj_formation		Enter to generate debug statements for Adjacency formation traces.
ism		Enter to generate debug statements for Interface State Machine traces.
nsm		Enter to generate debug statements for Neighbor State Machine traces.
config		Enter to generate debug statements for Configuration traces.
interface		Enter to generate debug statements for Interface.
helper		Enter to generate debug statements for messages related to router in Helper Mode.
redundancy		Enter to generate debug statements for redundancy messages.
all		Enter to generate debug statements for all messages.

Mode

Privileged EXEC Mode

Examples

iS5comm# debug ip ospf pkt hp

23.8. disable bfd

To disable Bidirectional Forwarding Detection (BFD) feature in OSPF, use the command **disable bfd** in OSPF Router Configuration Mode. If it is disabled, OSPF will not register with BFD for neighbor IP path monitoring.

disable bfd

```
disable bfd
```

Mode

OSPF Router Configuration Mode

Default

BFD feature is disabled.

Examples

iS5comm(config)# router ospf

is5comm(config-router)# disable bfd

23.9. default-information

To enable generation of a default external route into an OSPF routing domain and configure other parameters related to that area, use the command **default-information** in OSPF Router Configuration Mode. The no form of the command disables generation of a default external route into an OSPF routing domain.

default-information

```
default-information originate always [metric <metric-value (0-16777215)>]
[metric-type <type (1-2)>]
```

no default-information

```
no default-information originate always [metric <metric-value (0-16777215)>]
[metric-type <type (1-2)>]
```

Parameters

Parameter	Type	Description
originate		Enter to enable generation of a default external route into an OSPF routing domain.
always		Enter to configure advertising of the default route always regardless of whether the software has a default route.
metric		Enter to configure to set the Metric value applied to the route before it is advertised into the OSPF Domain Metric used for generating the default route.
<metric-value (0-16777215)>	Integer	Enter a metric value to be applied to the route before it is advertised into the OSPF Domain Metric used for generating the default route. If you omit a value and do not specify a value using the default-metric router configuration command, the default metric value is 1. The value used is specific to the protocol. This value ranges from 0 to 16777215.
metric-type		Enter to configure a metric type to be applied to the route before it is advertised into the OSPF Domain External link type associated with the default route advertised into the OSPF routing domain.
<type (1-2)>]	Integer	Enter a metric type to be applied to the route before it is advertised into the OSPF Domain External link type associated with the default route advertised into the OSPF routing domain. It can be one of the following values: • 1—Sets Type 1 external route • 2—Sets Type 2 external route

Mode

OSPF Router Configuration Mode

Default

- metric - 10
- metric-type - 2

Examples

iS5comm(config)# router ospf

iS5comm(config-router)# default-information originate always metric 1 metric-type 1

23.10. distance

To update the routes filtered via route-map at IP routing layer, use the command **distance** in OSPF Router Configuration Mode. The no form of this command disables the administrative distance (route preference).

distance

```
distance <1-255> [route-map <name(1-20)>]
```

no distance

```
no distance
```

Parameters

Parameter	Type	Description
<1-255>		Enter a value for the administrative distance. The distance value (i.e. the preference value) ranges between 1 and 255. The administrative distance (route preference value) can be updated for routes filtered via only one route map. The distance (route preference) should be disassociated for the already associated route map if distance needs to be associated for another route map.
route-map		Enter to configure the name of the Route Map for which the distance value should be enabled and set
<name(1-20)>		Enter a name for the Route Map for which the distance value should be enabled and set. This value is a string with maximum string of 20.

Mode

OSPF Router Configuration Mode

Default

0 (Represents directly connected route)

Prerequisites

This command executes only if OSPF router is enabled

Examples

iS5comm(config)# router ospf

is5comm(config-router)# distance 10 route-map rmap-test

23.11. distribute-list

To enable inbound filtering for routes and define the conditions for distributing the routes from one routing protocol to another, use the command **distribute-list** in OSPF Router Configuration Mode. The no form of the command disables inbound filtering for the routes.

distribute-list

```
distribute-list route-map <name (1-20)> in
```

no distribute-list

```
no distribute-list route-map <name (1-20)> in
```

Parameters

Parameter	Type	Description
route-map		Enter to configure the name of the Route Map for which filtering should be enabled. Only one route map can be set for inbound routes. Another route map can be assigned, only if the already associated route map is disassociate
<name(1-20)>	Integer	Enter a name for a route map. This is a string with maximum size of 20.
in		Enter to configure inbound filtering configuration

Mode

OSPF Router Configuration Mode

Examples

iS5comm(config)# router ospf

iS5comm(config-router)# distribute-list route-map rmap-test in

NOTE: The **clear ip ospf** command will have to be executed for this to take effect.

23.12. enable bfd

To enable Bidirectional Forwarding Detection (BFD) feature in OSPF, use the command **enable bfd** in OSPF Router Configuration Mode. The BFD protocol is a simple hello mechanism that detects failures in a network. BFD works with a wide variety of network environments and topologies. A pair of routing

devices exchange BFD packets, and hello packets are sent at a specified regular interval. This command registers OSPF with BFD for neighbor IP path monitoring.

enable bfd

```
enable bfd
```

Mode

OSPF Router Configuration Mode

Default

BFD feature is disabled.

Examples

iS5comm(config)# router ospf

is5comm(config-router)# enable bfd

23.13. ip ospf

To OSPF related configuration, use the command **ip ospf** in OSPF Router Configuration Mode. The no form of this command deletes the OSPF related configuration or sets all configured values to default.

ip ospf

```
ip ospf
 {authentication {simple | message-digest | sha-1 | sha-224 | sha-256 |
sha384 | sha-512 | null | simple}
 | authentication-key <key (8)>
 | bfd [disable]
 | cost <cost (1-65535)> [tos <value(0-30)>]
 | dead-interval <seconds (1-65535)>
 | demand-circuit
 | hello-interval <seconds (1 - 65535)>
 | key <Key-ID (0-255)> {start-accept <DD-MON-YEAR,HH:MM> | start-generate
<DD-MON-YEAR,HH:MM> | stop-accept <DD-MON-YEAR,HH:MM> | stop-generate
<DD-MON-YEAR,HH:MM>}
 | message-digest-key <Key-id (0-255)> {md5 | sha-1 | sha-224 | sha-256 |
sha-384 | sha-512} <key(16)>}
```

```
 | network {broadcast | non-broadcast | point-to-multipoint |
point-to-point}
 | priority <value (0 - 255)>
 | retransmit-interval <value (1-3600)>
 | transmit-delay <value (1-3600)>}
 }
```

no ip ospf

```
no ip ospf
 {authentication
 | authentication-key
 | cost [tos <value(0-30)>]
 | dead-interval
 | demand-circuit
 | hello-interval
 | message-digest-key <Key-id (0-255)>
 | network
 | priority
 | retransmit-interval
 | transmit-delay }
```

Parameters

Parameter	Type	Description
`authentication`		Enter to configure the authentication type as simple password authentication mechanism. Note that this command executes only if Message digest Key is configured.
`simple`		Enter to set the authentication type as message digest authentication mechanism.
`message-digest`		Enter to set the authentication type as message digest authentication mechanism.
`sha-1`		Enter to set the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes.
`sha-224`		Enter to set the authentication type as Secure Hash Algorithm 224 (SHA224) authentication. SHA224 generates Authentication digest of length 28 bytes.
`sha-256`		Enter to set the authentication type as Secure Hash Algorithm 256 (SHA256) authentication. SHA256 generates Authentication digest of length 32 bytes.
`sha-384`		Enter to set the authentication type as Secure Hash Algorithm 384 (SHA384) authentication. SHA384 generates Authentication digest of length 48 bytes.
`sha-512`		Enter to set the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. SHA512 generates Authentication digest of length 64 bytes.
`null`		Enter to set the no password authentication. This is the default authentication method. This is the default option.
`authentication-key`		Enter to configure a password to be used by neighboring routers that are using the OSPF simple password authentication. The password created by this command is used as a key that is inserted directly into the OSPF header when the routing protocol packets are originated. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information.
`<key (8)>`	Integer	Enter to set the simple password authentication mechanism. The size of the password is 8 bytes. The password string can contain from 1 to 8 uppercase and lowercase alphanumeric characters.

Parameter	Type	Description
bfd		Enter to enables or disables BFD support on the interface. If this is enabled, OSPF will register with BFD for monitoring the neighbor IP path for the neighbors associated with this OSPF interface. **NOTE:** BFD disabled for a specific interface using this command will be internally enabled on the execution of bfd all-interface command. **NOTE:** This command can be configured only if BFD is enabled and OSPF is started on the interface. By using this command, any BFD disabled for a specific interface will be enabled.
disable		Enter to disable BFD support on the interface. When disabled, it will de-register from BFD for the all neighbors associated with this interface and no longer allows registration with BFD for the neighbors associated with this interface.
cost		Enter to specify the cost of sending a packet on an interface. The link-state metric is advertised as the link cost in the router link advertisement. the path cost is calculated using the following formula: 108 / bandwidth For example when using this formula, the default path costs are calculated: • 56-kbps serial link-Default cost is 1785 • Ethernet-Default cost is 10
<cost>	Integer	Enter a value for the Type 1 external metrics which is expressed in the same units as OSPF interface cost, that is in terms of the OSPF link state metric. This value ranges from 1 to 65535.
tos		Enter to configure the Type of Service of the route being configured. It can be configured only if the code is compiled with TOS Support.
<tos value(0-30)>	Integer	Enter a value for Type of Service of the route being configured. This value ranges from 0 to 30. The default value for TOS is 0.
dead-interval		Enter to set the interval (in seconds) at which hello packets must not be seen before neighbors declare the router down. The interval is advertised in router hello packets
<seconds (1-65535)>	Integer	Enter a value for the interval (in seconds) at which hello packets must not be seen before neighbors declare the router down. This value ranges from 1 to 65535. The default is 40.

Parameter	Type	Description
demand-circuit		Enter to configure OSPF to treat the interface as an OSPF demand circuit. On point-to-point interfaces, only one end of the demand circuit must be configured. This command allows the underlying data link layer to be closed when the topology is stable. It indicates whether Demand OSPF procedures (hello suppression to FULL neighbors and setting the DoNotAge flag on imported LSAs must be performed on this interface. On point-to-point interfaces, only one end of the demand circuit must be configured with this command. Periodic hello messages are suppressed and periodic refreshes of link-state advertisements (LSAs) do not flood the demand circuit. This command executes only if OSPF routing process is enabled.
hello-interval		Enter to configure the interval (in seconds) between hello packets sent on the interface. This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes will be detected.
<seconds (1 - 65535)>	Integer	Enter a value to configure the interval (in seconds) between hello packets sent on the interface. This value ranges from 1 to 65535. This value must be the same for all routers attached to a common network.
key		Enter to configure the time the router starts accepting packets that is created with the configured key id.
<Key-ID (0-255)>	Integer	Enter a value for the secret key used to create the message digest appended to the OSPF packet. This value ranges from 0 to 255.
start-accept		Enter to configure the time when the router will start accepting packets that have been created with the configured key-id. **NOTE:** This command executes only if, • Authentication key for Simple Password Authentication is removed • OSPF Message Digest authentication is enabled and authentication type is specified for the interface
<DD-MON-YEAR,HH:MM>		Enter a value for the time when the router will start accepting packets that have been created with the configured key-id. This value is the sum of configured time and the system time at which the start-accept value is configured and is configured in 24 hours format. **NOTE:** For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30

Parameter	Type	Description
start-generate		Enter to configure the time when the router will start generating OSPF packets with the configured key id. **NOTE:** This command executes only if, • Authentication key for Simple Password Authentication is removed • OSPF Message Digest authentication is enabled and authentication type is specified for the interface
<DD-MON-YEAR,HH:MM>		Enter a value for the time when the router will start generating OSPF packets with the configured key id. This value is the sum of the configured time and the system time at which the start-generate value is configured. Start Generate Time value is configured in 24 hours format. Default value is set as current system time. **NOTE:** For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30
stop-generate		Enter to configure the time when the router will stop generating OSPF packets with the configured key id. **NOTE:** This command executes only if, • Authentication key for Simple Password Authentication is removed • OSPF Message Digest authentication is enabled and authentication type is specified for the interface
<DD-MON-YEAR,HH:MM>		Enter a value for the time when the router will stop generating OSPF packets with the configured key id. Stop Generate value is configured in 24 hours format. Default value is set to the current system time. **NOTE:** For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30
stop-accept		Enter to configure the time when the router will stop accepting OSPF packets with specified key id. **NOTE:** This command executes only if, • Authentication key for Simple Password Authentication is removed. • OSPF Message Digest authentication is enabled and authentication type is specified for the interface .

Parameter	Type	Description
<DD-MON-YEAR,HH:MM>		Enter a value for the time when the router will stop accepting OSPF packets with specified key id. Stop accept value is configured in 24 hours format. **NOTE:** For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30
message-digest-key		Enter to enable OSPF MD5 authentication. One key per interface is used to generate authentication information when sending packets and to authenticate incoming packets. Message Digest authentication is a cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the OSPF packet, the key, and the key-id to generate a "message digest" that gets appended to the packet Usually, one key per interface is used to generate authentication information when sending packets and to authenticate incoming packets. The same key identifier on the neighbor router must have the same key value. **NOTE:** The authentication type should be the same as set in the ip ospf authentication command.
<Key-id (0-255)>	Integer	Enter to set the simple password authentication mechanism.
md5		Enter to set the authentication type as message digest authentication mechanism.
sha-1		Enter to set the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes.
sha-224		Enter to set the authentication type as Secure Hash Algorithm 224 (SHA224) authentication. SHA224 generates Authentication digest of length 28 bytes
sha-256		Enter to set the authentication type as Secure Hash Algorithm 256 (SHA256) authentication. SHA256 generates Authentication digest of length 32 bytes.
sha-384		Enter to set the authentication type as Secure Hash Algorithm 384 (SHA384) authentication. SHA384 generates Authentication digest of length 48 bytes
sha-512		Enter to set the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. SHA512 generates Authentication digest of length 64 bytes.

Parameter	Type	Description
<key(16)>	Integer	Enter a value to configure the cryptographic key value which is used to create the message digest appended to the OSPF packet. All neighboring routers on the same network must have the same key identifier and key to route OSPF traffic. This is a string with maximum 16 characters.
network		Enter to configure the OSPF network type to a type other than the default for a given media and configures broadcast networks as NBMA networks. Each pair of routers on a broadcast network is assumed to be able to communicate directly. An Ethernet is an example of a broadcast network. A 56Kb serial line is an example of a point-to-point network.
broadcast		Enter to configure the broadcast networks supporting many (more than two) attached routers, together with the capability to address a single physical message to all of the attached routers (broadcast). This is the default option.
non-broadcast		Enter to configure the non broadcast networks supporting many (more than two) routers, but having no broadcast capability Sets the network type to nonbroadcast multi-access (NBMA).
point-to-multipoint		Enter to set the network type to point-to-multipoint and treats the non-broadcast network as a collection of point-to-point links.
point-to-point		Enter to set the network type to point-to-point that joins a single pair of routers
priority		Enter to set the router priority which helps determine the designated router for this network. When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. . When two routers attached to a network attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence.
<value (0 - 255)>	Integer	Enter a value to specify the priority of the router The number value ranges from 0 to 255. The default value is 1.
retransmit-interval		Enter to configure the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPF virtual link interface.

Parameter	Type	Description
<value (1-3600)>	Integer	Enter a value for the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPF virtual link interface. This value ranges from 1 to 3600 in seconds with a default of 5. This value is also used while retransmitting database description and link-state request packets.
transmit-delay		Enter to set the estimated time (in seconds) it is required to transmit a link state update packet on the interface. Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the seconds argument before transmission.
<value (1-3600)>	Integer	Enter a value for the time in which the router will stop using this key for packets generation. This value ranges from 1 to 3600 in seconds with a default of 1 second.

Mode

OSPF Router Configuration Mode

Prerequisites

This command executes only if the OSPF routing process is enabled.

Examples

iS5comm(config)# router ospf

is5comm(config-if)# ip ospf authentication message-digest

is5comm(config-if)# ip ospf authentication-key asdf123

iS5comm(config-router)# enable bfd

iS5comm(config-router)# exit

iS5comm(config)# int vlan 55

is5comm(config-if)# ip ospf bfd disable

is5comm(config-if)# ip ospf cost 10

is5comm(config-if)# ip ospf dead-interval 1000

is5comm(config-if)# ip ospf demand-circuit

is5comm(config-if)# ip ospf hello-interval 75

is5comm(config-if)# ip ospf key 20 start-accept 13-May-2014,19:18

is5comm(config-if)# ip ospf key 20 start-generate 13-May-2014,19:18

is5comm(config-if)# ip ospf key 20 stop-generate 13-May-2014,19:18

is5comm(config-if)# ip ospf key 20 stop-accept 13-May-2014,19:18

is5comm(config-if)# ip ospf network broadcast

is5comm(config-if)# ip ospf priority 25

is5comm(config-if)# ip ospf retransmit-interval 300

is5comm(config-if)# ip ospf transmit-delay 50

23.14. neighbor

To specifies a neighbor router and its priority, use the command **neighbor** in OSPF Router Configuration Mode. The no form of the command removes the neighbor and resets the neighbor priority to its default value. This command configures the Router ID of OSPF routers interconnecting to nonbroadcast networks.

neighbor

```
neighbor <neighbor-id>
 [priority <priority value (0-255)>]
 [poll-interval <poll-interval (1-2147483647)>]
 [cost <cost number 0-255)>]
 [database-filter all]
```

no neighbor

```
no neighbor <neighbor-id> [poll-interval seconds] [priority] [poll-interval
seconds] [cost number] [database-filter all]
```

Parameters

Parameter	Type	Description
<neighbor-id>		Enter to configure the neighbor router ID based on which the priority of the neighbor is defined.
priority		Enter to configure the router priority and the priority of the nonbroadcast neighbor router associated with the specified IP address. The router with the highest priority becomes the designated router.
<priority value (0-255)>	Integer	Enter a number value that specifies the router priority and the priority of the nonbroadcast neighbor router associated with the specified IP address. This value ranges from 0 to 255 with the value 0 signifying that the neighbor is not eligible to become the designated router on this particular network,
poll-interval		Enter to configure the poll interval between the Hello packets sent to an inactive non-broadcast multi-access neighbor.
<poll-interval (1-2147483647)	Integer	Enter a poll interval value. This value ranges from 1 to 2147483647 seconds.
cost		Enter to configure route path cost value.
<cost number 0-255)>	Integer	Enter a value for route path cost. It ranges from 0 to 255.
database-filter		Enter to configure the database filter.
all		Enter to set database filter as all.

Mode

OSPF Router Configuration Mode

Default

priority - 1

Examples

iS5comm(config)# router ospf

iS5comm(config-router)# neighbor 12.0.0.8 priority 25

23.15. network

To defines the interfaces on which OSPF runs and the area ID for those interfaces, use the command **network** in OSPF Router Configuration Mode. The no form of the command OSPF routing for interfaces defined and to remove the area ID of that interface. When a more specific OSPF network range is removed, interfaces belonging to that network range will be retained and remain active if and only if a less specific network range exists. There is no limit to the number of network commands that can be used on the router. The IP address for the entry should be same as that of the configured interface.

network

```
network <Network number>
 {area <area-id> [unnum {vlan <vlan-id/vfi-id>
 | <interface-type> <interface-num>
 | <IP-interface-type> <IP-interface-number>}]
 | <wildcard-mask> area <area-id>
 [unnum vlan <PortNumber>]}
```

no network

```
no network <Network number> {area <area-id> [unnum {vlan <vlan-id/vfi-id>
[switch <switch-name>] | <interface-type> <interface-num> | <IP-inter-
face-type> <IP-interface-number>}]
```

Parameters

Parameter	Type	Description
<Network number>		Enter to configure the network type for the interfaces (e.g. of the format is 0.0)
area		Enter to configure the area associated with the OSPF address range and the identifier of the area about which routes are to be summarized.
<area-id>		Enter a value (either a decimal value or as an IP address) to configure the area associated with the OSPF address range and the identifier of the area about which routes are to be summarized.
unnum		Enter to configure the network type for the specified unnumbered interface configuration.
vlan		Enter to configure network type for the specified VLAN / VFI ID.
<vlan-id/vfi-id>		Enter a value for the VLAN ID or VFI-ID for which the network type will be configured. This value ranges from 1 to 65535. The options are as follow: • <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535. **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries. **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

Parameter	Type	Description
<interface-type>		Enter interface type to configure the Network type. The interface types are: • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links
<interface-num>		Enter a value interface number to configure the network type. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example, 0/1 represents that the slot number is 0 and port number is 1.
<IP-interface-type>		Enter to configure the network type for the specified L3 Pseudo wire interface in the system.
<IP interface-num>		Enter a value to configure the network type for the specified L3 Pseudo wire interface in the system. Network type for the specified L3 Pseudo wire interface identifier. This is a unique value that represents the specific interface. This value ranges from 1 to 65535 for Pseudowire interface. **NOTE:** Maximum number of PseudoWire interfaces supported in the system is 100.
<wildcard-mask>		Enter to configure the wild card mask for the network IP address.
area		Enter to configure the area associated with the OSPF address range and the identifier of the area about which routes are to be summarized.
<area-id>		Enter a value (either a decimal value or as an IP address) to configure the area associated with the OSPF address range and the identifier of the area about which routes are to be summarized.
unnum		Enter to configure unnumbered VLAN for the area.
Vlan		Enter to configure unnumbered VLAN for the area
<Vlan id (1-4094)>		Enter a value for VLAN ID. This is a unique value that represents the specific VLAN and ranges from 1 to 4094.

Mode

OSPF Router Configuration Mode

Prerequisites

- This command can be configured only if, router ospf is enabled.
- IP address must be configured for the interface which is to be added as the unnumbered interface

Examples

iS5comm(config)# router ospf

iS5comm(config-router)# network 0.0 area 0.0 unnum gi 0/2

is5comm (config-router)# network 1.1.1.1 0.0.0.0 area 0.0.0.0 unnum Vlan 55

is5comm(config-router)# network 1.1.1.1 area 0.0.0.0

23.16. nsf ietf

To configure the Non Stop Forwarding (nsf) features such as strict LSA check option in helper mode, grace period, helper support, graceful restart support, the reason for graceful support, OSPF graceful restart timeout interval, and the maximum number of retransmissions for unacknowledged grace LSA, use the command **nsf ietf** in OSPF Router Configuration Mode. The no form of the command disables all above mentioned configured features.

nsf ietf

```
nsf ietf {helper {[gracetimelimit <gracelimit period(0-1800)>] [softwareRe-
start] [strict-lsa-checking] [swReloadUpgrade] [switchToRedundant]
[unknown]}
 | helper-support {[softwareRestart] [swReloadUpgrade] [switchToRedundant]
[unknown]}
 | grace lsa ack required
 | grlsa retrans count <grlsacout (0-180)>
 | restart-interval <grace period(1-1800)>
 | restart-reason {[softwareRestart] [swReloadUpgrade] [switchToRedundant]
[unknown]}
 | restart-support plannedOnly}
```

no nsf ietf

```
no nsf ietf {helper [strict-lsa-checking]
```

```
 | helper-support {[softwareRestart] [swReloadUpgrade] [switchToRedundant]
[unknown]}
 | grace lsa ack required
 | restart-interval
 | restart-support
```

Parameters

Parameter	Type	Description
`helper`		Enter to enable the helper mode. When a router Y receives a grace-LSA from router X, it enters helper mode for X on the associated network segment. **NOTE:** This command executes only if • OSPF router is enabled • Helper Mode is enabled
`gracetimelimit`		Enter to configure the grace period till which the OSPF router acts as Helper. *The router attempting a graceful restart originates link-local Opaque-LSAs, herein called Grace-LSAs, announcing its intention to perform a graceful restart within a specified amount of time or "grace period".* During this period, the router advertises that the restarting router is active and is in FULL state. The value is provided as an intimation of the restart period to the neighbors that do not support graceful restart or that are connected using multipoint interfaces.
`<gracelimit period(0-1800)>`	Integer	Enter a value for the grace period till which the OSPF router acts as Helper. This value ranges from 0 to 1800 seconds. The default is 0.
`softwareRestart`		Enter to configure the helper support for restarting of system due to restart of software.
`strict-lsa-checking`		Enter to enable the strict LSA check option in helper. The strict LSA check option allows the helper to terminate the graceful restart, once a changed LSA that causes flooding during the restart process is detected. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent. By default, Strict LSA check option is disabled in helper. **NOTE:** This command executes only if • OSPF router is enabled • Helper Mode is enabled
`swReloadUpgrade`		Enter to configure helper support for restarting of system due to reload or upgrade of software.
`switchToRedundant`		Enter to configure helper support for restarting of system due to switchover to a redundant support processor.
`unknown`		Enter to configure helper support for restarting of system due to unplanned events (such as restarting after a crash).

Parameter	Type	Description
helper-support		Enter to configure helper support. The helper support is enabled for all options if the command is executed without selecting any of the additional options. The helper support can be enabled for more than one option, one after the other. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent. By default, Helper support is enabled. **NOTE:** This command executes only if • OSPF router is enabled
softwareRestart		Enter to configure the helper support for restarting of system due to restart of software.
swReloadUpgrade		Enter to configure helper support for restarting of system due to reload or upgrade of software.
switchToRedundant		Enter to configure helper support for restarting of system due to switchover to a redundant support processor.
unknown		Enter to configure helper support for restarting of system due to unplanned events (such as restarting after a crash).
grace		Enter to configure graceful restart mode. The grace link-state advertisements (LSAs) sent by the router are expected to be acknowledged by peers, if the graceful restart mode Grace Ack Required state is enabled. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent. By default, graceful restart mode Grace Ack Required state is enabled in restarter. **NOTE:** This command executes only if • OSPF router is enabled
lsa		Enter to set the LSA related configuration.
ack		Enter to set acknowledgment related configuration.
required		Enter to enable acknowledgment related state configuration.
grlsa		Enter to configure the maximum number of retransmissions for unacknowledged grace LSA.
retrans		Enter for retransmission related configuration.
count		Enter to perform counting operation. **NOTE:** This command executes only if • OSPF router is enabled

Parameter	Type	Description
<grlsacout (0-180)>	Integer	Enter a value for number of retransmission of unacknowledgedGrace LSAs. This value ranges from 0 to 180. The default is 2.
restart-interval		Enter to configure the maximum number of retransmissions for unacknowledged grace LSA. This value ranges from 0 to 1800. The default is 120.
<grace period(1-1800)>	Integer	Enter a value for maximum number of retransmissions for unacknowledged grace LSA.
restart-reason		Enter to configures the reason for graceful restart in the OSPF router. The reason for restart can be software upgrade, scheduled restart or switch to redundant router. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent. **NOTE:** This command executes only if • OSPF router is enabled
softwareRestart		Enter to configure restarting of system due to restart of software.
swReloadUpgrade		Enter to configure restarting of system due to reload or upgrade of software.
switchToRedundant		Enter to configure restarting of system due to switchover to a redundant support processor.
unknown		Enter to configure helper restarting of system due to unplanned events (such as restarting after a crash). This is default
restart-support		Enter to enable the graceful restart support in OSPF router. Graceful restart support is provided for both unplanned and planned restart, if the command is executed without any option. The graceful restart mechanism allows forwarding of data packets to continue along known routes, while the routing protocol information is being restored following a processor switch over. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent. By default, Graceful restart support is disabled. **NOTE:** This command executes only if • OSPF router is enabled • Helper Mode is enabled

Parameter	Type	Description
plannedOnly		Enter to configure support of only planned restarts (suchas restarting a control plane after a planned downtime).

Mode

OSPF Router Configuration Mode

Default

Unknown

Prerequisites

This command executes only if OSPF router is enabled.

Examples

iS5comm(config)# router ospf

iS5comm(config-router)# nsf ietf helper gracetimelimit 100

S5comm(config-router)# nsf ietf helper strict-lsa-checking

is5comm(config-router)# nsf ietf helper-support switchToRedundant

is5comm(config-router)# nsf ietf grace lsa ack required

is5comm(config-router)# nsf ietf grlsa retrans count 100

is5comm(config-router)# nsf ietf restart-interval 200

is5comm(config-router)# nsf ietf restart-reason softwareRestart

is5comm(config-router)# nsf ietf restart-support

23.17. passive-interface

To suppress routing updates on an interface and make the interface passive, use the command **passive-interface** in OSPF Router Configuration Mode. The no form of the command enables routing updates on an interface. OSPF routing information is neither sent nor received through the specified router interface.

passive-interface

```
passive-interface {vlan <vlan-id/vfi-id> [switch <switch-name>] | <inter-
face-type> <interface-id> | <IP-interface-type> <IP-interface-number> |
default}
```

no passive-interface

```
no passive-interface {vlan <vlan-id/vfi-id> [switch <switch-name>] | <inter-
face-type> <interface-id> | <IP-interface-type> <IP-interface-number> |
default}
```

Parameters

Parameter	Type	Description
vlan		Enter to configure specified VLAN / VFI ID as passive interface.
<vlan-id/vfi-id>		Enter a value for the VLAN ID or VFI-ID for which the passive interface will be configured. This value ranges from 1 to 65535. The options are as follow: • <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535. **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries. **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
switch		Enter to configure a switch context.
<switch-name>		Enter default for switch name.
<interface-type>		Enter interface type to configure the passive interface. The interface types are: • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links
<interface-id>		Enter a value interface number to configure the network type. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example, 0/1 represents that the slot number is 0 and port number is 1.

Parameter	Type	Description
<IP-interface-type>		Enter to configure the network type for the specified L3 Pseudo wire interface in the system.
<IP interface-num>		Enter a value to configure the network type for the specified L3 Pseudo wire interface in the system. Network type for the specified L3 Pseudo wire interface identifier. This is a unique value that represents the specific interface. This value ranges from 1 to 65535 for Pseudowire interface. **NOTE:** Maximum number of PseudoWire interfaces supported in the system is 100.
default		Enter to configure the passive interface to be default i.e. all OSPF interfaces created after the execution of this command will be passive. This is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

Mode

OSPF Router Configuration Mode

Prerequisites

- This command can be configured only if, router ospf is enabled.

Examples

iS5comm(config)# router ospf

iS5comm(config-router)# passive-interface gigabitethernet 0/2

is5comm(config-router)# passive-interface default

23.18. redist-config

To configure the information to be applied to routes learnt from RTM (Route Table Manager), use the command **redist-config** in OSPF Router Configuration Mode. The no form of the command deletes the information applied to routes learnt from RTM.

redist-config

```
redist-config <Network> <Mask>
 [metric <metric-value (0-16777215)>]
```

```
[metric-type {asExttype1 | asExttype2}]
[tag <tag-value>]
```

no redist-config

```
no redist-config <Network> <Mask>
```

Parameters

Parameter	Type	Description
<Network>		Enter an IP address to configure the IP address of the network indicated by the range.
<Mask>		Enter the subnet mask that pertains to the range. The mask indicates the range of addresses being described by the particular route. For example, a summary-LSA for the destination 128.185.0.0 with a mask of 0xffff0000 actually is describing a single route to the collection of destinations 128.185.0.0 - 128.185.255.255.
metric		Enter to configure the metric values for the routes to be redistributed into OSPF.
<metric-value (0-16777215)>	Integer	Enter a metric value for the routes to be redistributed into OSPF. This value ranges from 0 to 16777215.
metric-type		Enter to configure the metric type applied to the routes to be redistributed.
asExttype1		Enter to set the metric type as external Type 1.
asExttype2		Enter to set the metric type as external Type 2.
tag		Enter to configure the tag type and describe whether tags will be automatically generated or will be manually configured. . This is not used by OSPF protocol itself. It may be used to communicate information between AS boundary routers. The precise nature of this information is outside the scope of OSPF. If tags are manually configured, the futospfRRDRouteTag MIB has to be set with the Tag value needed. **NOTE:** To execute this command with the tag option, the router must to set as ASBR
<tag-value>	Integer	Enter a tag value. This value ranges from 0 to 4294967295

Mode

OSPF Router Configuration Mode

Default

- metric - 10
- metric-type - asExttype2
- tag - manual

Prerequisites

This command executes only if the router is set as ASBR

Examples

iS5comm(config)# router ospf

iS5comm(config-router)# redist-config 10.0.0.0 255.0.0.0 metric-value 100 metric-type asExttype1

23.19. redistribute

To configure the protocol from which the routes have to be redistributed into OSPF and advertise the routes learned by other protocols, use the command **redistribute** in OSPF Router Configuration Mode. The no form of the command disables redistribution of routes from the given protocol.

redistribute

```
redistribute {static | connected | rip | bgp | isis [{level-1 | level-2 |
level-1-2}] | all}
 [route-map <name (1-20)>]
 [metric <metric-value (0-16777215)>]
 [metric-type <type (1-2)>]
```

no redistribute

```
no redistribute {static | connected | rip | bgp | all} [route-map <name
(1-20)>] [metric]
```

Parameters

Parameter	Type	Description
`static`		Enter to configure redistribution of routes configured statically in the OSPF routing process.
`connected`		Enter to configure redistribution of directly connected networks routes into OSPF routing process.
`rip`		Enter to enable redistribution of routes that are learnt by the RIP process into OSPF routing process.
`bgp`		Enter to configure redistribution of routes that are learnt by the BGP process into OSPF routing process.
`isis`		Enter to enable redistribution of routes learnt by ISIS in the OSPF routing process.
`level-1`		Enter to import routes learnt by ISIS level-1 in the OSPF routing process.
`level-2`		Enter to import routes learnt by ISIS level-2 in the OSPF routing process.
`level-1-2`		Enter to import routes learnt by ISIS in the OSPF routing process.
`all`		Enter to import routes learnt in the OSPF routing process.
`route-map`		Enter to identify the specified route-map in the list of route-maps. **NOTE:** Redistribution can be configured for only one route map. Another route map can be assigned, only if the already assigned route map is disabled.
`<name(1-20)>`	Integer	Enter a name for a route map. This is a string with maximum size of 20.
`metric`		Enter to configure the metric values for the routes to be redistributed into OSPF.
`<metric-value (0-16777215)>`	Integer	Enter a metric value for the routes to be redistributed into OSPF. This value ranges from 0 to 16777215.
`metric-type`		Enter to configure the metric type applied to the routes to be redistributed.
`<type (1-2)>]`	Integer	Enter a metric type to be applied to the routes to be redistributed. It can be one of the following values: • 1—Sets Type 1 external route • 2—Sets Type 2 external route

Mode

OSPF Router Configuration Mode

Default

- metric - 10
- metric-type - 2

Examples

iS5comm(config)# router ospf

iS5comm(config-router)# redistribute static

23.20. route-calculation

To enable OSPF route calculation staggering feature and configure the staggering interval, use the command **route-calculation** in OSPF Router Configuration Mode. The no form of this command disables OSPF route calculation staggering and changes the staggering interval to default.

route-calculation

```
route-calculation {staggering | staggering-interval <milli-seconds
(1000-2147483647)>}
```

no route-calculation

```
no route-calculation staggering
```

Parameters

Parameter	Type	Description
staggering		Enter to configure staggering of the OSPF route calculation at regular intervals for processing neighbor keep alive and other OSPF operations.
staggering-interval		Enter to configure the OSPF route calculation staggering interval.
<milli-seconds (1000-2147483647)>	Integer	Enter a value for the OSPF route calculation staggering interval (in milliseconds). This value represents the time after which the route calculation is suspended for doing other OSPF operations and ranges from 1000 to 2147483647 milliseconds. The default is 10000 milliseconds.

Mode

OSPF Router Configuration Mode

Default

10000 milliseconds (OSPF route calculation staggering interval is equal to Hello interval)

Prerequisites

This command executes only if OSPF router is enabled.

Examples

iS5comm(config)# router ospf

is5comm(config-router)# route-calculation staggering-interval 2000

23.21. router ospf

To enable OSPF routing process, enter into the OSPF Router Configuration Mode, and enable OSPF in cyber security context, use the command **router ospf** in Global Configuration Mode. The no form of this command disables the OSPF Router Admin Status to terminate the OSPF process or deletes the Cyber security context of OSPF.

router

```
router ospf [cybsec]
```

no router

```
no router ospf [cybsec]
```

Parameters

Parameter	Type	Description
ospf		Enter to enable OSPF routing process and enter into the OSPF Router Configuration Mode.
cybsec		Enter to enable OSPF in cyber security space. The switch runs two instances of OSPF: one in iBiome and another one in cyber security space. This command turns on the dynamic routing capability using OSPF protocol in the cyber security space.

Mode

Global Configuration Mode

Examples

iS5comm(config)# router ospf cybsec

is5comm(config-router)# exit

iS5comm(config)# no router ospf cybsec

23.22. router-id

To set the router identification for the OSPF process, use the command **router-id** in OSPF Router Configuration Mode. The no form of this command resets the configured router ID and dynamically selects least interface IP as router ID for OSPF process.

router-id

```
router-id <router ip address>
```

no router-id

```
no router-id <router ip address>
```

Parameters

Parameter	Type	Description
<router ip address>		Enter to set the router ID for the OSPF process. The router ID is set to an IP address of a loopback interface if it is configured. An arbitrary value for the IP address for each router can be configured; however, each router ID must be unique. To ensure uniqueness, the router ID must match one of the router's IP interface addresses.

Mode

OSPF Router Configuration Mode

Examples

iS5comm(config)# router ospf

is5comm(config-router)# router-id 12.0.0.1

23.23. set nssa asbr-default-route

To enable or disable the setting of P bit in the default Type-7 LSA generated by NSSA internal ASBR, use the command **set nssa asbr-default-route** in OSPF Router Configuration Mode.

set nssa

```
set nssa sbr-default-route translator {disable | enable}
```

Parameters

Parameter	Type	Description
sbr-default-route		Enter to configure the setting of P bit in the default Type-7 LSA generated by NSSA internal ASBR.
translator		Enter to configure P-Bit related configuration.
disable		Enter to clear P-Bit in the generated default LAS, when NSSA ASBR is set to disabled.
enable		Enter to set P-Bit in the generated Type-7 default LSA, when NSSA ASBR is set to enabled.

Mode

OSPF Router Configuration Mode

Default

disable

Examples

iS5comm(config)# router ospf

iS5comm(config-router)# set nssa asbr-default-route translator enable

23.24. show ip ospf

To display the OSPF Related information, use the **show ip ospf** command in Privileged EXEC Mode.

show ip ospf

```
show ip ospf
 [area-id]
 [{database {asbr-summary | external | network | nssa-external | opaque-area
| opaque-as | opaque-link | router | summary} [link-state-id] [{adv-router
<ip-address> | self-originate}] | {database-summary | self-originate |
adv-router <ip-address>}}] [cybsec]
 [border-routers]
```

```
 [interface [{vlan <vlan-id/vfi-id> [switch <switch-name>] | {Gigabiteth-
ernet <interface-id> | Extreme-ethernet <interface-id> | <IP-interface-type>
<IP-interface-number> | ppp <1-128>}]

 [neighbor [{vlan <vlan-id/vfi-id> [switch <switch-name>] | {Gigabitethernet
<interface-id> | Extreme-ethernet <interface-id> | <IP-interface-type>
<IP-interface-number>] [Neighbor ID] [detail] [cybsec]

 [request-list [<neighbor-id>] [{vlan <vlan-id/vfi-id> [switch
<switch-name>] | {Gigabitethernet <interface-id> | Extreme-ethernet <inter-
face-id> | <IP-interface-type> <IP-interface-number>]

 [retransmission-list [<neighbor-id>] [{vlan <vlan-id/vfi-id> [switch
<switch-name>] | {Gigabitethernet <interface-id> | Extreme-ethernet <inter-
face-id> | <IP-interface-type> <IP-interface-number>]

 [route] [cybsec]

 [virtual-links]

 [{area-range | summary-address}

 [redundancy]
```

Parameters

Parameter	Type	Description
area-id		Enter to configure the area associated with the OSPF address range to be displayed. It will be specified as an IP address
database		Enter to display OSPF Database summary for the LSA type.
asbr-summary		Enter to display information only about the Autonomous System Boundary Router (ASBR) summary LSAs.
external		Enter to display information only about the external LSAs.
network		Enter to display information only about the network LSAs.
nssa-external		Enter to display information only about the external LSAs.
opaque-area		Enter to display information only about the network LSAs.
opaque-as		Enter to display information only about the external LSAs.
opaque-as		Enter to display information only about the network LSAs.
router		Enter to display information only about the router LSAs.
summary		Enter to display information only about the summary LSAs.
link-state-id		Enter to display the portion of the Internet environment that is being described by the advertisement. The value entered depends on the type of the LSA. The value must be entered in the form of an IP address.
adv-router		Enter to display all specified router link-state advertisements (LSAs). If no IP address is included, the information is about the local router itself.
<ip-address>		Enter to display only information only about this Ip Address.
cybsec		Enter to display the OSPF neighborship or database from the cyber security space, or the route learnt by the OSPF which runs in the cyber security space.
database-summary		Enter to display the total number of each type of LSA for each area there are in the database, and the total number of LSA type.
self-originate		Enter to display only self-originated LSAs (from the local router).
adv-router		Enter to display all specified router link-state advertisements (LSAs). If no IP address is included, the information is about the local router itself.
<ip-address>		Enter to display only information only about this Ip Address.

Parameter	Type	Description
border-routers		Enter to display the internal OSPF routing table entries to an Area Border Router and Autonomous System Boundary Router.
interface		Enter the general information of OSPF routing processes for the specified interface.
<vlan-id/vfi-id>		Enter to specify the range of the specified VLAN ID to be displayed. This is a unique value that represents the specific VLAN created and activated. The range (1-4094) is for VLAN ID and the range (4096 - 65535) is for VFI. Note that if router ports are used then correspondingly the last set of vlans will not be available. For example, if router ports is 24, then max VLAN number will be 4070 only.
switch		Enter to configure name of the switch to be displayed.
<switch-name>		Enter a name for the switch to be displayed.
Gigabitethernet <interface-id>		Enter to select Gigabit Ethernet interface to be displayed. Gigabit Ethernet interface is a version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. Specify the interface ID with a format <0>/<1-28>—slot number/port number.
Extreme-Ethernet <interface-id>		Enter to select Extreme Ethernet interface to be displayed. Extreme Ethernet interface is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. Specify the interface ID with a format <0>/<1-28>—slot number/port number.
<IP-interface-type>		Enter to display the IP ARP information for the specified L3 Pseudo wire interface in the system.
<IP-interface-number>		Enter to display the IP ARP information for the specified L3 Pseudo wire interface identifier. This is a unique value that represents the specific interface. This value ranges from 1 to 65535 for Pseudowire interface. **NOTE:** Maximum number of Pseudowire interfaces supported in the system is 100.
ppp		Enter to display the PPP related information.
<1-128>		Enter to display the PPP interface ID.
neighbor		Enter to display the OSPF neighbor information list and the neighbor data structure.

Parameter	Type	Description
<vlan-id/vfi-id>		Enter to specify the range of the specified VLAN ID to be displayed. This is a unique value that represents the specific VLAN created and activated. The range (1-4094) is for VLAN ID and the range (4096 - 65535) is for VFI. Note that if router ports are used then correspondingly the last set of vlans will not be available. For example, if router ports is 24, then max VLAN number will be 4070 only.
switch		Enter to configure name of the switch to be displayed.
<switch-name>		Enter a name for the switch to be displayed.
Gigabitethernet <interface-id>		Enter to select Gigabit Ethernet interface to be displayed. Gigabit Ethernet interface is a version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. Specify the interface ID with a format <0>/<1-28>—slot number/port number.
Extreme-Ethernet <interface-id>		Enter to select Extreme Ethernet interface to be displayed. Extreme Ethernet interface is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. Specify the interface ID with a format <0>/<1-28>—slot number/port number.
<IP-interface-type>		Enter to display the IP ARP information for the specified L3 Pseudo wire interface in the system.
<IP-interface-number>		Enter to display the IP ARP information for the specified L3 Pseudo wire interface identifier. This is a unique value that represents the specific interface. This value ranges from 1 to 65535 for Pseudowire interface. **NOTE:** Maximum number of Pseudowire interfaces supported in the system is 100.
Neighbor ID		Enter to display OSPF request LSAs for the specified neighbor router ID.
detail		Enter to display the OSPF Link state request list advertisements (LSAs) requested by a router and debugging OSPF routing operations.
request-list		Enter to display the OSPF Link state request list advertisements (LSAs) requested by a router and debugging OSPF routing operations.
<neighbor-id>		Enter to display OSPF request LSAs for the specified neighbor router ID.

Parameter	Type	Description
<vlan-id/vfi-id>		Enter to specify the range of the specified VLAN ID to be displayed. This is a unique value that represents the specific VLAN created and activated. The range (1-4094) is for VLAN ID and the range (4096 - 65535) is for VFI. Note that if router ports are used then correspondingly the last set of vlans will not be available. For example, if router ports is 24, then max VLAN number will be 4070 only
switch		Enter to configure name of the switch to be displayed.
<switch-name>		Enter a name for the switch to be displayed.
Gigabitethernet <interface-id>		Enter to select Gigabit Ethernet interface to be displayed. Gigabit Ethernet interface is a version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. Specify the interface ID with a format <0>/<1-28>—slot number/port number.
Extreme-Ethernet <interface-id>		Enter to select Extreme Ethernet interface to be displayed. Extreme Ethernet interface is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. Specify the interface ID with a format <0>/<1-28>—slot number/port number.
<IP-interface-type>		Enter to display the IP ARP information for the specified L3 Pseudo wire interface in the system.
<IP-interface-number>		Enter to display the IP ARP information for the specified L3 Pseudo wire interface identifier. This is a unique value that represents the specific interface. This value ranges from 1 to 65535 for Pseudowire interface. **NOTE:** Maximum number of Pseudowire interfaces supported in the system is 100.
retransmission-list		Enter to display list of all OSPF Link state retransmission list information waiting to be resent. This value is also used while retransmitting database description and link-state request packets.
Neighbor ID		Enter to display OSPF request LSAs for the specified neighbor router ID.

Parameter	Type	Description
<vlan-id/vfi-id>		Enter to specify the range of the specified VLAN ID to be displayed. This is a unique value that represents the specific VLAN created and activated. The range (1-4094) is for VLAN ID and the range (4096 - 65535) is for VFI. Note that if router ports are used then correspondingly the last set of vlans will not be available. For example, if router ports is 24, then max VLAN number will be 4070 only.
switch		Enter to configure name of the switch to be displayed.
<switch-name>		Enter a name for the switch to be displayed.
Gigabitethernet <interface-id>		Enter to select Gigabit Ethernet interface to be displayed. Gigabit Ethernet interface is a version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. Specify the interface ID with a format <0>/<1-28>—slot number/port number.
Extreme-Ethernet <interface-id>		Enter to select Extreme Ethernet interface to be displayed. Extreme Ethernet interface is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. Specify the interface ID with a format <0>/<1-28>—slot number/port number.
<IP-interface-type>		Enter to display the IP ARP information for the specified L3 Pseudo wire interface in the system.
<IP-interface-number>		Enter to display the IP ARP information for the specified L3 Pseudo wire interface identifier. This is a unique value that represents the specific interface. This value ranges from 1 to 65535 for Pseudowire interface. **NOTE:** Maximum number of Pseudowire interfaces supported in the system is 100.
route		Enter to display the routes learnt by OSPF process.
virtual-links		Enter to display the parameters and the current state of OSPF virtual links.
summary		Enter to display OSPF summary-address redistribution information configured under an OSPF process.
area-range		Enter to display the area associated with the OSPF address range.
summary-address		Enter to display the aggregate addresses for OSPF.

Mode

Privileged EXEC Mode

Examples

iS5comm # show ip ospf

```
OSPF Router with ID (0.0.0.0)
Supports only single TOS(TOS0) route  O
paque LSA Support : Disabled
ABR Type supported is Standard ABR
Autonomous System Boundary Router : Disabled
P-Bit setting for the default Type-7 LSA that needs to be generated by
the ASBR(which is not ABR) is disabled
Non-Stop Forwarding disabled
Restart-interval limit: 120
Grace LSA Retransmission Count: 2
Helper Grace LSA ACK :Required
Restart Reason is:
         Unknown
Helper is Giving Support for:
         Unknown
         Software Restart
         Software Reload/Upgrade
         Switch To Redundant
  Helper Grace Time Limit: 0
  Strict LSA checking State Is: Disabled
  Route calculation staggering is enabled
  Route calculation staggering interval is  -1718520588 milliseconds
Redistributing External Routes is disabled
Default passive-interface  Disabled
  Rfc1583 compatibility is enabled
  Administrative Distance is 110
  Number of Areas in this router is 0
  Default information originate is disabled
 BFD is disabled
```

show ip ospf database external

```
OSPF Router with ID (10.0.0.1)
      Summary Link States (Area 33.0.0.12)
--------------------------------------
LS age             : 300
```

```
    Options            : (No ToS Capability, DC)
    LS Type            : Summary Links(Network)
    Link State ID      : 10.0.0.0
    Advertising Router : 10.0.0.1
    LS Seq Number      : 0x80000002
    Checksum           : 0xae77
    Length             : 28
```

is5comm# show ip ospf database database-summary

```
    OSPF Router with ID (12.0.0.1)
    Router Link States (Area 0.0.0.0)
    ------------------------------------
    Link ID    ADV Router    Age   Seq#     Checksum  Link count-------
    ----------    ---     ----    --------  -----
    12.0.0.1   12.0.0.1      48    0x80000002   0xd129    112.0.0.2
    12.0.0.2      50    0x80000002   0xcf28    1              Network Link
    States (Area 0.0.0.0)
    ------------------------------------
    Link ID       ADV Router    Age     Seq#          Checksum
    -------       ----------    ---     ----          ------12.0.0.2
    12.0.0.2      49      0x80000001    0x629f
    OSPF Router with ID (14.0.0.1)
```

is5comm# show ip ospf border-routers

```
    OSPF Process Border Router Information
    Destination  TOS  Type  Next Hop      Cost   Rt. Type    Area
    -----------  ---  ----  -------      ----       -------  ----
    12.0.0.2     0    ASBR  12.0.0.2     1     intra Area  0.0.0.0
```

is5comm# show ip ospf interface vlan 1

```
    Vlan1 is line protocol is up
      Internet Address 13.0.0.1, Mask 255.0.0.0, Area 0.0.0.0
      AS 1, Router ID 12.0.0.2, Network Type BROADCAST, Cost 1
      demand circuit is disabled
      Transmit Delay is 1 sec, State 4, Priority 1
      Designated Router ID 12.0.0.2, Interface address 13.0.0.1
      No backup designated router on this network
      Timer intervals configured, Hello 10, Dead 40, Wait 40,  Retransmit 5
      Hello due in 1 sec
      Neighbor Count is 0, Adjacent neighbor count is 0
    sha-1  authentication enabled
    sha-1 authentication key is configured
     Youngest key id is 1
          Key Start Accept Time  is 26-Jun-2013,02:50
```

```
        Key Start Generate Time  is 26-Jun-2013,02:50
        Key Stop Generate Time  is 06-Feb-2136,06:28
        Key Stop Accept Time  is 06-Feb-2136,06:28
     Simple Authentication  Key is not Configured
     Bfd Enable
```

is5comm# show ip ospf neighbor

```
    Neighbor-ID  Pri   State        DeadTime   Address
    Interface Helper      HelperAge    HelperER   Bfd
    -----------  ---   -----        --------   -------
     --------- ---------   ------------ ---------  -----
    12.0.0.1     1     FULL/BACKUP  30         20.0.0.1
    vlan2     Not Helping 0             None       Enabled
```

is5comm# show ip ospf request-list vlan 1

```
    OSPF Router with ID (20.0.0.2)
    Neighbor 10.0.0.1, interface vlan1 address 40.0.0.1
    Type LS-ID     ADV-RTR     Seq No      Age    Checksum
     ---- ----     -------     -----      ---    --------
    Neighbor 20.0.0.2, interface vlan1 address 40.0.0.2
    Type LS-ID   ADV-RTR      Seq No       Age    Checksum
     ---- ----   -------      -----       ---    --------
```

is5comm# show ip ospf retransmission-list vlan 1

```
    OSPF Router with ID (20.0.0.2)
    Neighbor 10.0.0.1, interface vlan1 address 10.0.0.2
    Queue length 3
    Type  LS-ID   ADV-RTR   Seq No   Age  Checksum
    1     20.0.0.2 20.0.0.2  0x80000006 0 0x522f
```

is5comm# show ip ospf route

```
    OSPF Routing Table
    Dest/Mask      TOS Next Hop/Interface Cost Rt. Type   Area
    ---------        --- -------/--------- ---- -------
    12.0.0.0/255.0.0.0  0  0.0.0.0/vlan1    1   Intra Area 0.0.0.0
    20.0.0.0/255.0.0.0   0  12.0.0.2/vlan1  10  Type2Ext  0.0.0.0
```

is5comm# show ip ospf virtual-links

```
    Virtual Link to router 10.0.0.1, Interface State is DOWN
      Transit Area 33.0.0.12
      Transmit Delay is 1 sec, Neighbor State DOWN
      Timer intervals configured, Hello 10, Dead 60, Retransmit 5
```

is5comm# show ip ospf redundancy

```
Redundancy Summary ------------------  Hot standby admin status :
Enabled  Hot standby state : Active and Standby Up  Hot standby bulk
update status : Completed  Number of hello PDUs synced : 0  Number of
LSAs synced : 0
```

is5comm# show ip ospf area-range

```
Display of Summary addresses for Type3 and Translated Type5
Summary Address
-----------------------------------------------
Network  Mask       LSA Type Area       Effect        Tag
  -------  -------      ----               ------       ---
10.0.0.0  255.0.0.0 Summary 33.0.0.12 Advertise 1074636208
```

is5comm# show ip ospf neighbor cybsec

```
Neighbor-ID  Pri   State        DeadTime   Address Interface Helper
HelperAge    HelperER   Bfd
-----------  ---   -----        --------   ------- --------- ---------
-------------------  -----
```

is5comm# show ip ospf database cybsec

```
 OSPF Router with ID (11.11.11.11)

Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
1.1.1.1         1.1.1.1          562 0x8000000b 0xae39 1
11.11.11.11     11.11.11.11      561 0x80000003 0x565f 1

Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
192.168.50.1    1.1.1.1          562 0x80000001 0xd88f

ospfd#
```

is5comm# show ip ospf route cybsec

```
EXEC commands :

show ip ospf [vrf <name>] route [cybsec]

Raptor-1# show ip ospf route cybsec

Dest/Mask                       NextHop/Interface           Cost Area
---------                       -------/---------           ---- ----
```

```
    192.168.50.0/24                 0.0.0.0/vlan50              10
    0.0.0.0
```

23.25. summary-address

To creates aggregate addresses for OSPF and help in reducing the size of the routing table, use the command **summary-address** in OSPF Router Configuration Mode. The no form of the command deletes the External Summary Address.

summary-address

```
summary-address <Network> <Mask> <AreaId>
 [{allowAll | denyAll | advertise | not-advertise}]
 [Translation {disable | enable}]
 [tag <tag-value>]
```

no summary-address

```
no summary-address <Network> <Mask> <AreaId> [not-advertise] [tag
<tag-value>]
```

Parameters

Parameter	Type	Description
<Network>		Enter an IP address to configure the IP address of the network indicated by the range.
<Mask>		Enter the subnet mask that pertains to the range. The mask indicates the range of addresses being described by the particular route. For example, a summary-LSA for the destination 128.185.0.0 with a mask of 0xffff0000 actually is describing a single route to the collection of destinations 128.185.0.0 - 128.185.255.255.
<AreaId>		Enter to configure the area associated with the OSPF address range and the identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IP address. **NOTE:** The Area Id should be of backbone area or NSSA area.
allowAll		Enter to configure allowAll option and set associated area ID as 0.0.0.0 which generates the aggregated Type-5 for the specified range. In addition aggregated Type-7 are generated in all attached NSSA, for the specified range This parameter is valid only for area ID 0.0.0.0.
denyAll		Enter to configure denyAll in which neither Type-5 nor Type-7 will be generated for the specified range. This parameter is valid only for area ID 0.0.0.0.
advertise		Enter to set the address range status to advertise and generate a Type 3 summary link-state advertisement (LSA). When associated area Id is 0.0.0.0, aggregated Type-5 are generated. For associated other than 0.0.0.0, aggregated Type-7 is generated in NSSA x.x.x.x.
not-advertise		Enter to set the address range status to Not Advertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks When associated area Id is 0.0.0.0, Type-5 is not generated for the specified range, while aggregated Type-7 are generated in all attached NSSA. For associated area Id x.x.x.x which is other than 0.0.0.0, Type-7 are not generated in NSSA x.x.x.x for the specified range.
Translation		Enter to configure how an NSSA Border router is performing NSSA translation of Type-7 to Type-5 LSAs.
disable		Enter to clear P-Bit in the generated default LAS, when NSSA ASBR is set to disabled.

Parameter	Type	Description
enable		Enter to set P-Bit in the generated Type-7 default LSA, when NSSA ASBR is set to enabled.
tag		Enter to configure the tag option for OSPF.
<tag-value>	Integer	Enter a tag value.

Mode

OSPF Router Configuration Mode

Default

- summary-address - advertise
- translation - enabled

Examples

iS5comm(config)# router ospf

iS5comm(config-router)# summary-address 10.0.0.6 255.0.0.0 10.0.0.0 Translation enabled

23.26. timers spf

To configure delay time and hold time between two consecutive SPF calculations, use the command **timers spf** in OSPF Router Configuration Mode. The no form of the command resets the spf-delay and spf-holdtime to their default values.

timers spf

```
timers spf <spf-delay(0-65535)> <spf-holdtime(0-65535)>
```

no timers spf

```
no timers spf
```

Parameters

Parameter	Type	Description
<spf-delay(0-65535)>	Integer	Enter a value to configure the interval by which SPF calculation is delayed after a topology change reception. This value ranges from 0 to 65535 seconds. The default is 5.
<spf-holdtime(0-65535)>	Integer	Enter a value to configure the minimum time between two consecutive SPF calculations. This value ranges from 0 to 65535 seconds. The default is 10.

Mode

OSPF Router Configuration Mode

Default

- spf-delay - 5 seconds
- spf-holdtime - 10 seconds

Examples

iS5comm(config)# router ospf

iS5comm(config-router)# timers spf 10 20

DHCP

24. DHCP

DHCP (Dynamic Host Configuration Protocol) is used in a wide variety of devices, such as ISDN routers, firewalls, etc., for assigning IP addresses to workstations. Besides obtaining IP address, other configuration parameters for a workstation can also be configured for a DHCP server. DHCP clients can retrieve these parameters along with the IP address.

DHCP is based on client-server architecture. DHCP servers are configured with an IP address and several other configuration parameters. DHCP clients, typically workstations, obtain this IP address at start-up. The client obtains the address for a time period termed as the “lease” period. DHCP clients renew the address by sending a request for the IP address before the lease expires.

DHCP uses UDP (User Datagram Protocol) as its transport protocol and an UDP port for communication. DHCP relay agents connect servers present on a LAN with a client present on another.

24.1. DHCP Client

This section describes the DHCP Client on the switch.

DHCP (Dynamic Host Configuration Protocol) Client is an Internet host using DHCP to obtain configuration parameters such as an IP address.The figure below shows the basic steps that occur when a DHCP client requests an IP address from a DHCP server. The client, Host A, sends a DHCP DISCOVER broadcast message to locate a DHCP server. A DHCP server offers configuration parameters (such as an IP address, a MAC address, a domain name, and a lease for the IP address) to the client in a DHCP OFFER unicast message.

The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given Internet layer address, typically an IPv4 address. The ARP uses a simple message format containing one address resolution request or response. The size of the ARP message depends on the link layer and network layer address sizes. The message header specifies the types of network in use at each layer as well as the size of addresses of each. The message header is completed with the operation code for request (1) and reply (2). The payload of the packet consists of four addresses, the hardware and protocol address of the sender and receiver hosts.

24.2. DHCP Relay

This section describes the DHCP Relay agent on the switch.

DHCP relay agent is a host or an IP router that allows the DHCP client and DHCP server in different subnets to communicate with each other, so that the DHCP client can obtain its configuration information while booting. The relay agent receives packets from the client, inserts information such as network details, and forwards the modified packets to the server. The server identifies the client's network from the received packets, allocates the IP address accordingly, and sends reply to the relay. The relay strips the information inserted by the server and broadcasts the packets to the client's network.

Relay Agent Information Option

Automatic DHCP address allocation is typically based on an IP address, whether it be the gateway IP address (giaddr field of the DHCP packet) or the incoming interface IP address. In some networks, it is necessary to use additional information to further determine which IP addresses to allocate. By using the relay agent information option, the DHCP relay agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server.

When using the relay agent information option, the DHCP relay agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to assign IP addresses, perform access control, and set quality of service (QoS) and security policies (or other parameter-assignment policies) for each subscriber of a service provider network.

The relay agent information option is inserted into the DHCP packet as follows:

1) The DHCP client generates a DHCP request and broadcasts it on the network.
2) The DHCP relay agent intercepts the broadcast DHCP request packet and inserts the relay agent information option (option 82) in the packet. The relay agent information option contains the related suboptions.The DHCP relay agent unicasts the DHCP packet to the DHCP server.The DHCP server receives the packet and uses the suboptions to assign IP addresses and other configuration parameters and forwards them back to the client.
3) The suboption fields are stripped off of the packet by the relay agent while forwarding to the client.

24.3. DHCP Server

This section describes the DHCP Server on the switch.

DHCP server is used for dynamically assigning unique IP address and other configuration parameters, such as gateway, to interfaces of a DHCP client. The IP address is leased to the interface only for a particular time period as mentioned in the DHCP lease. The interface should be renewed the DHCP lease once it expires.

The DHCP server assigns IP addresses from specified address pools on a router and manages them. Then, the subnet network number and mask of the DHCP address pool, the domain name for the client, the IP address of a DNS server that is available to a DHCP client, and the IP address of the default router for a DHCP client are specified.

As defined in RFC 3261, a Session Initiation Protocol (SIP) server must be an outbound proxy server. In the context of this document, a SIP server refers to the host the SIP server is running on. SIP is an application-layer control protocol that can establish, modify, and terminate multimedia sessions or established by Voice-over-IP telephony calls.

24.4. bootfile config-file

To define the name of the boot image file that the DHCP client should download during auto install process, use the command **bootfile config-file** in Global Configuration Mode. The no form of the command deletes the specified boot file name and assigns the value of boot file name as None (that is, no file is set as boot image file). The DHCP server passes this file name to the DHCP client. This command is a complete standardized implementation of the existing command and operates similar to that of the command ip dhcp bootfile.

bootfile config-file

```
bootfile config-file <bootfile (63)>
```

no bootfile config-file

```
no bootfile config-file
```

Parameters

Parameter	Type	Description
<bootfile (63)>		Enter a name for the boot image file. This is a string with maximum size of 63.

Mode

Global Configuration Mode

Default

None (Null terminated string)

Examples

iS5comm (config)# bootfile config-file boot.img

24.5. clear ip dhcp client statistics

To clear the DHCP client statistics for all ports or for the specified interface created in the system, use the command **clear ip dhcp client statistics** in Privileged EXEC Mode / Global Configuration Mode.

clear ip dhcp client statistics

```
clear ip dhcp client statistics
 [interface {vlan <vlan-id (1-4094)> | <interface-type> <interface-id>}]
```

Parameters

Parameter	Type	Description
`interface`		Enter to specify a interface to have DHCP client statistics cleared.
`vlan`		Enter to clear the DHCP client statistics for a specified VLAN.
`<vlan-id (1-4094)>`	Integer	Enter a VLAN ID for the DHCP client statistics to be cleared. This is a unique value that represents the specific VLAN created. This value ranges from 1 to 4094.
`<interface-type>`		Enter to specify the type of interface for the DHCP client statistics to be cleared. The interface can be: • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
`<interface-id>`		Enter an interface ID for the DHCP client statistics to be cleared. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example, 0/1 represents that the slot number is 0 and port number is 1.

Mode

Privileged EXEC Mode / Global Configuration Mode

Examples

iS5comm# clear ip dhcp client statistics

iS5comm (config)# clear ip dhcp client statistics

24.6. clear ip dhcp relay statistics

To clears the DHCP relay statistics, use the command **clear ip dhcp relay statistics** in Privileged EXEC Mode / Global Configuration Mode.

clear ip dhcp relay statistics

```
clear ip dhcp relay statistics
```

Mode

Privileged EXEC Mode / Global Configuration Mode.

Examples

iS5comm (config)# clear ip dhcp relay statistics

24.7. clear ip dhcp server statistics

To clear the DHCP client statistics for all ports or for the specified interface created in the system, use the command **clear ip dhcp server statistics** in Privileged EXEC Mode / Global Configuration Mode.

clear ip dhcp server statistics

```
clear ip dhcp server statistics
```

Mode

Privileged EXEC Mode / Global Configuration Mode

Examples

iS5comm# clear ip dhcp server statistics

iS5comm (config)# clear ip dhcp server statistics

24.8. debug ip dhcp

To enable the tracking of the DHCP operations as per the configured debug level, use the command **debug ip dhcp** in Privileged EXEC Mode. The no form of the command disables the tracking of the DHCP client operations. This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

debug ip dhcp

```
debug ip dhcp
 {client {all | event | packets | errors | bind}
 | relay {all | errors}
 | server {all | events | packets | errors | bind | linkage}
 | snooping {[entry] [exit] [debug] [fail] | all}}
```

no debug ip dhcp

```
no debug ip dhcp
 {client {all | event | packets | errors | bind}
 | relay {all | errors}
 | server {all | events | packets | errors | bind | linkage}
 | snooping
```

Parameters

Parameter	Type	Description
client		Enter to enable the tracking of the DHCP client operations as per the configured debug levels. The debug statements are generated for the specified trace levels.
all		Enter to generate debug statements for all kind of failure traces.
event		Enter to generate debug statements for DHCP client events that provide DHCP client service status. The DHCP client events are generated when any of packets are sent successfully or when an ACK is received
packets		Enter to generate debug statements for packets related messages. These messages are generated for all events generated during processing of packets.
errors		Enter to generate debug statements for Link State Acknowledge Packet traces
bind		Enter to generate debug statements for trace bind messages. These messages are generated when a DHCP ACK is received.
relay		Enter to enable the tracking of the DHCP relay operations as per the configured debug levels. The debug statements are generated for the specified trace levels.
all		Enter to generate debug statements for all kind of failure traces.
errors		Enter to generate debug statements for trace error code debug messages. These messages are generated for all error events generated.
server		Enter too enable the tracking of the DHCP relay operations as per the configured debug levels. The debug statements are generated for the specified trace levels.
all		Enter to generate debug statements for all kind of failure traces.
event		Enter to generate debug statements for DHCP server events that provide DHCP server service status. The DHCP client events are generated when any of packets are sent successfully or when an ACK is received
packets		Enter to generate debug statements for packets related messages. These messages are generated for all events generated during processing of packets.
errors		Enter to generate debug statements for trace error code debug messages. These messages are generated for all error events generated.
bind		Enter to generate debug statements for trace bind messages. These messages are generated when a DHCP ACK is received.

Parameter	Type	Description
linkage		Enter to generate debug statements for database linkage messages.
snooping		Enter to enable the tracing of the DHCP snooping module as per the configured debug level. The trace statements are generated for the configured trace levels.
entry		Enter to generate debug statements for function entry traces. The names of the functions entered are displayed in the log.
exit		Enter to generate debug statements for function exit traces. The names of the functions exited are displayed in the log.
debug		Enter to generate debug statements for debug traces. This is used for debugging the packet flow of DHCP snooping functionality.
fail		Enter to generate debug statements for all failure traces. These traces are used for all valid and invalid failures. The valid failures represent the expected error. The invalid failures represent the unexpected error
all		Enter to generate debug statements for all types of traces.

Mode

Privileged EXEC Mode

Default

Tracking of all DHCP modules operation is disabled

Examples

iS5comm# debug ip dhcp client all

iS5comm# debug ip dhcp relay all

iS5comm# debug ip dhcp server all

iS5comm# debug ip dhcp snooping entry

24.9. default-router

To configure the IP address for the corresponding DHCP server address pool and of a default router to which a DHCP client should send packets after booting, use the command **default-router** in DHCP Pool Configuration Mode. The no form of the command deletes the default router IP address configuration for the DHCP server address pool. The default router IP address configuration is deleted, if the no form of the network command is executed successfully.

default-router

```
default-router <ip address>
```

no default-router

```
no default-router
```

Parameters

Parameter	Type	Description
<ip address>		Enter a value to configure the IP address of a default router to which a DHCP client should send packets after booting.

Mode

DHCP Pool Configuration Mode

Prerequisites

- The configured IP address of the default router should be on the same subnet of the DHCP client.
- The default router IP address configuration takes effect only after creating a subnet pool for a DHCP server address pool

Examples

iS5comm(config)# ip dhcp pool 1 pool1

iiS5comm(dhcp-config)# default-router 10.23.2.99

24.10. dns-server

To configure the IP address of a DNS server for the corresponding DHCP server address pool, use the command **dns-server** in DHCP Pool Configuration Mode. The no form of the command deletes the DNS server IP address option configuration for the DHCP server address pool.

dns-server

```
dns-server <ip address> [<ip address>]
```

no dns-server

```
no dns-server
```

Parameters

Parameter	Type	Description
<ip address> [<ip address>]		Enter a value to configure the unicast IP address to be set for the corresponding DNS server that accepts IP address. The client correlates the DNS IP address with the host name. The DNS server is used to translate domain names and host names into corresponding IP addresses.

Mode

DHCP Pool Configuration Mode

Prerequisites

This command is executed successfully only if a subnet pool is already created for the DHCP address pool.

Examples

iS5comm(config)# ip dhcp pool 1 pool1

iiS5comm(dhcp-config)# dns-server 12.0.0.1

24.11. domain-name

To configure the domain name option for the corresponding DHCP server address pool, use the command **domain-name** in DHCP Pool Configuration Mode. The no form of the command deletes the domain name option configuration for the DHCP server address pool. The domain name option configuration is deleted if the no form of the network command is executed successfully.

domain-name

```
domain-name <domain (63)>
```

no domain-name

```
no domain-name <domain (63)>
```

Parameters

Parameter	Type	Description
<domain (63)>	Integer	Enter a value for the domain name option or the corresponding DHCP server address pool. A DHCP client uses this domain name while resolving host names through a domain name system. The DHCP option code is 15. This value is a string of maximum size 63.

Mode

DHCP Pool Configuration Mode

Prerequisites

This command is executed successfully only if a subnet pool is already created for the DHCP address pool.

Examples

iS5comm(config)# ip dhcp pool 1 pool1

iS5comm(dhcp-config)# domain-name 12

24.12. excluded-address

To create an excluded pool that defines a range of IP addresses that needs to be excluded from the created subnet pool, use the command **excluded-address** in DHCP Pool Configuration Mode. The no form of the command deletes the created excluded pool. The same start IP address and end IP address of the already created excluded pool should be provided while executing the no form of the command.

excluded-address

```
excluded-address <low-address> <high-address>
```

no excluded-address

```
no excluded-address <low-address> <high-address>
```

Parameters

Parameter	Type	Description
<low-address>	Integer	Enter to set the start IP address for an excluded pool. This address denotes the first IP address of a range of IP addresses which needs to be excluded from the created subnet pool. This IP address should be: • lower than the end IP address, and • in the same network of the subnet pool's start IP address.
<high-address>		Enter to set the end IP address for an excluded pool. This address denotes the last IP address of a range of IP addresses which needs to be excluded from the created subnet pool. This IP address should be: • high than the start IP address, and within or equal to the subnet pool's end IP address

Mode

DHCP Pool Configuration Mode

Prerequisites

This command is executed successfully only if a subnet pool is already created for the DHCP address pool.

Examples

iS5comm(config)# ip dhcp pool 1 pool1

iS5comm(dhcp-config)# excluded-address 20.0.0.1 20.0.0.30

24.13. host hardware-type

To configure host hardware type and its DHCP option with specific values, and set the NTP server, DNS server, and SIP server with the host specific DHCP server configuration parameters, use the command **host hardware-type** in DHCP Pool Configuration Mode. The no form of the command deletes the hardware type and its DHCP option and all servers from the host specific DHCP server configuration parameters.

host hardware-type

```
host hardware-type <integer (1-255)> client-identifier
 {<mac-address> {ip <ip address> | option <code (1-2147483647)> {ascii
<string> | hex <hex_str> | ip <ip address>}}}
 | {<ucast_mac>
```

```
 {ntp-server <ip address> [<ip address>]
 | dns-server <ip address> [<ip address>]
 | sip-server {{domain <string> [<string>]} | {ip <ip address> [<ip
address>]}}
```

no host hardware-type

```
no host hardware-type <host-hardware-type (1-255)> client-identifier
 {<client-mac-address> {ip | option <code (1-255)>}]
 | {<ucast_mac>
 {ntp-server
 | dns-server
 | sip-server}}
```

Parameters

Parameter	Type	Description
<integer (1-255)>	Integer	Enter a value to configure the host hardware type for which the host address and the DHCP options needs to be configured. This value ranges from 1 to 255. Only the value 1 is supported, which represents that the hardware type is Ethernet.
client-identifier		Enter to configure the DHCP client identifier in a host declaration so that a host record can be found using this client identifier. The client identifier represents the physical address (MAC address) of a network card.
<mac-address>		Enter a MAC address for the IPv4 address for the DHCP host.
ip		Enter to configure the IPv4 address for the DHCP host.
<ip address>		Enter the IPv4 address for the DHCP host.
option		Enter to configure the unique DHCP option code that represents a specific DHCP option used in a DHCP OFFER message on response to a DHCP DISCOVER message
<code (1-2147483647)>	Integer	Enter a value for the unique DHCP option code that represents a specific DHCP option used in a DHCP OFFER message in response to a DHCP DISCOVER message. This value ranges from 1 to 2147483647.
ascii		Enter to configure the ASCII value to be set for the corresponding option code that accepts ASCII string.
<string>		Enter an ASCII value to be set for the corresponding option code that accepts ASCII string. This value is a character string that should contain only characters from NVT ASCII character set.
hex		Enter to configure the hexadecimal value to be set for the corresponding option code that accepts hexadecimal string.
<string>		Enter a hexadecimal value for the corresponding option code.
ip		Enter to configure the unicast IP address to be set for the corresponding option code that accepts IP addres
<ip address>		Enter to configure the unicast IP address to be set for the corresponding option code that accepts IP address.
<ucast_mac>		Enter to configure the client identifier with the host MAC address.
ntp-server		Enter to set NTP servers in the host specific DHCP server configuration parameters.

Parameter	Type	Description
<ip address>		Enter an unicast IP address for the corresponding NTP servers in the host specific DHCP server configuration.
dns-server		Enter to set DNS servers in the host specific DHCP server configuration parameters.
<ip address>		Enter an unicast IP address for the corresponding DNS servers in the host specific DHCP server configuration.
sip-server		Enter to set SIP servers in the host specific DHCP server configuration parameters. SIP stands for Session Initiation Protocol and refers to a TCP/IP-based network protocol which is often used in Voice-over-IP telephony to establish connection for telephone calls.
domain		Enter to configure the domain names for the server.
string		Enter a domain name for the server. The domain name should be specified as ASCII string
ip		Enter to set SIP servers in the host specific DHCP server configuration parameters.
<ip address>		Enter to an unicast IP address for the corresponding SIP servers in the host specific DHCP server configuration.

Mode

DHCP Pool Configuration Mode

Examples

iS5comm(config)# ip dhcp pool 1 pool1

iS5comm(dhcp-config) # host hardware-type 1 client-identifier 00:01:02:03:04:01 option 67 ascii abcd

iS5comm(dhcp-config) # host hardware-type 1 client-identifier 00:11:22:33:44:55 dns-server 12.0.0.1 13.0.0.0

iS5comm(dhcp-config) # host hardware-type 1 client-identifier 00:11:22:33:44:55 ntp-server 12.0.0.1 13.0.0.0

iS5comm (dhcp-config)# host hardware-type 1 client-identifier 00:11:22:33:44:55 sip-server domain sipsrv sipsrv1

24.14. ip dhcp bootfile

To configure the name for the initial boot file to be loaded in a DHCP client, use the command **ip dhcp bootfile** in Global Configuration Mode. The no form of the command deletes the boot file name (that is, no file is specified as the initial boot file).

ip dhcp bootfile

```
ip dhcp bootfile <bootfile (63)>
```

no ip dhcp bootfile

```
no ip dhcp bootfile
```

Parameters

Parameter	Type	Description
<bootfile (63)>		Enter a name for the initial boot file to be loaded in a DHCP client. The file name is a string whose maximum size is 63. The boot file contains the boot image that is used as the operating system for the DHCP client.

Mode

Global Configuration Mode

Examples

iS5comm (config)# ip dhcp bootfile boot1

24.15. ip dhcp client

To set the DHCP option type for requests to the server and set an unique identifier for the DHCP client identifier, use the command **ip dhcp client** in Interface Configuration Mode (VLAN / Router). The no form of the command resets the DHCP option type for requests to the server and the DHCP client identifier.

ip dhcp client

```
ip dhcp client
 {client-id {<interface-type> <interface-id> | vlan <vlan-id (1-4094)> |
port-channel <port-channel-id (1-65535)> | tunnel <tunnel-id (0-128)> |
loopback <interface-id (0-100)> | ascii <string> | hex <string>}
 | request {tftp-server-name | boot-file-name | sip-server-info | option240}
 | vendor-specific <vendor-info>}
```

no ip dhcp client

```
no ip dhcp client
 {client-id
 | request {tftp-server-name | boot-file-name | sip-server-info | option240}
 | vendor-specific}
```

Parameters

Parameter	Type	Description
client-id		Enter to set the unique identifier for the DHCP client identifier. This command advertises the client-id in the DHCP control packet.
<interface-type>		Enter to specify the interface type for the DHCP client-id. The interface can be: • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan – Internal LAN created on a bridge per IEEE 802.1ap.
<interface-id>		Enter to configure an interface id for the DHCP client-id for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.
vlan		Enter to configure DHCP client-id for a specified VLAN.
<vlan-id (1-4094)>	Integer	Enter a VLAN ID for the DHCP client ID.This is a unique value that represents the specific VLAN created. This value ranges from 1 to 4094.
port-channel		Enter to configure the port to be used by the host to configure the router. The port channel identifier can be created or port channel related configuration can done, only if the LA feature is enabled in the switch.
<port-channel-id (1-65535)>	Integer	Enter a value for port ID for the port to be used by the host to configure the router. This value ranges from 1 to 65535
tunnel		Enter to configure the tunnel identifier.
<tunnel-id (0-128)>	Integer	Enter a value for the tunnel identifier. This value ranges from 0 to 128.
loopback		Enter to configure the loopback identifier.

Parameter	Type	Description
<interface-id (0-100)>	Integer	Enter a a value for the loopback identifier. This value ranges from 0 to 100.
ascii		Enter to configure the DHCP client ID in ascii format.
<string>		Enter a value for client ID in ascii format. The client-id is given as a string.
hex		Enter to configure the DHCP client ID in hex format
<string>		Enter a value for client ID in ascii format. The client-id is given as a string.
request		Enter to set the DHCP option type for requests to the server. This is required to send DHCP request to get the tftp server name, Boot file name, sip server name and option240.
tftp-server-name		Enter to configure to send the DHCP requests for getting the TFTP server's domain name
boot-file-name		Enter to configure to send the DHCP requests for getting he boot File Name
sip-server-info		Enter to configure to send the DHCP requests for getting the sip server details
option240		Enter to configure to send the DHCP requests for getting the the option 240 information.
vendor-specific		Enter to configure vendor specific information for the DHCP client.
<vendor-info (string)>		Enter a vendor name. The vendor name is given as a string.

Mode

Interface Configuration Mode (VLAN / Router)

Prerequisites

This command executes successfully only if the VLAN interfaces and router ports are in BOUND state (that is, IP address is dynamically acquired from DHCP server and an active lease is bound to the interface). The port should have been configured as router port for dynamically acquiring an IP address from DHCP server.

Examples

iS5comm (config-if)# ip dhcp client client-id gigabitethernet 0/1

iS5comm (config-if)# ip dhcp client request option240

24.16. ip dhcp client

To enable DHCP fast access Mode and configure the ARP, discovery and idle DHCP timers, use the command **ip dhcp client** in Privileged EXEC Mode. The no form of the command resets all DHCP Client timers to their defaults and disables DHCP Client fast access mode.

ip dhcp client

```
ip dhcp client
 {arp-check timer <integer (1-20)>
 | discovery timer <integer (1-300)>
 | fast-access
 | idle timer <integer (1-300)>}
```

no ip dhcp client

```
no ip dhcp client
 {arp-check timer | discovery timer | fast-access | idle timer}
```

Parameters

Parameter	Type	Description
`arp-check time`		Enter to configure DHCP client retransmission timeout between ARP messages. For devices to be able to communicate with each other when they are not part of the same network, the 48-bit MAC address must be mapped to an IP address. One of the Layer 3 protocols used to perform the mapping is Address Resolution Protocol (ARP).
`<integer (1-20)>`	Integer	Enter a value for the DHCP client retransmission timeout between ARP messages. This value ranges from 1 to 20.
`discovery timer`		Enter to configure DHCP Client Discovery timer, which denotes the time to wait between discovery messages sent by the DHCP client. **NOTE:** This command executes only ifip dhcp client fast-access is enabled
`<integer (1-300)>`	Integer	Enter a value for the time to wait between discovery messages sent by the DHCP client. This value ranges from 1 to 300
`fast-access`		Enter to enable DHCP fast access mode. If fast access mode is enabled, time to wait between discovery messages i.e. discovery timeout and time to wait after four unsuccessful discovery will be user configurable and the default value for discovery timeout is 5 seconds and for the null state timeout is 1 second.
`idle timer`		Enter to configure DHCP Client Discovery timer, DHCP Client idle timer which specifies the time to wait after four unsuccessful DHCP client discovery messages. **NOTE:** This command executes only ifip dhcp client fast-access is enabled.
`<integer (1-300)>`	Integer	Enter a value for the time to wait after four unsuccessful DHCP client discovery messages. This value ranges from 1 to 300.

Mode

Privileged EXEC Mode

Default

- If dhcp fast mode is enabled, the default DHCP Client arp-check timer is 1, DHCP Client Discovery timer is 5, and the default DHCP Client Idle timer is 1.
- If dhcp fast mode is disabled, the default DHCP Client arp-check timer is 3, the default DHCP Client Discovery timer is 15, and the default DHCP Client Idle timer is 18.

Examples

iS5comm# ip dhcp client arp-check timer 8

iS5comm# ip dhcp client fast-access

iS5comm# ip dhcp client discovery timer 8

iS5comm# ip dhcp client idle timer 8

24.17. ip dhcp dns-server

To set the DNS server in the host specific DHCP server configuration parameters, use the command **ip dhcp dns-server** in Global Configuration Mode. The no form of the command deletes the DNS servers from the host specific DHCP server configuration parameters.

ip dhcp dns-server

```
ip dhcp dns-server <ip address> [<ip address>]
```

no ip dhcp dns-server

```
no ip dhcp dns-server
```

Parameters

Parameter	Type	Description
`dns-server`		Enter to set DNS servers in the host specific DHCP server configuration parameters.
`ip`		Enter to set DNS servers in the host specific DHCP server configuration parameters.
`<ip address>`		Enter to an unicast IP address for the corresponding DNS servers in the host specific DHCP server configuration.

Mode

Global Configuration Mode

Examples

iS5comm(config)# ip dhcp dns-server 12.0.0.1 13.0.0.0

24.18. ip dhcp excluded-address

To create an excluded pool and to prevent DHCP server from assigning certain addresses to DHCP clients, use the command **ip dhcp excluded-address** in Global Configuration Mode. The no form of the command deletes the created excluded pool. This command is a complete standardized implementation of the existing command and operates similar to that of the command excluded-address. This command is used to exclude a single IP address or a range of IP addresses.

ip dhcp excluded-address

```
ip dhcp excluded-address <low-address> <high-address>
```

ip dhcp excluded-address

```
no ip dhcp excluded-address <low-address> <high-address>
```

Parameters

Parameter	Type	Description
<low-address>	Integer	Enter to set the start IP address for an excluded pool. This address denotes the first IP address of a range of IP addresses which needs to be excluded from the created subnet pool. This IP address should be: • lower than the end IP address, and • in the same network of the subnet pool's start IP address.
<high-address>		Enter to set the end IP address for an excluded pool. This address denotes the last IP address of a range of IP addresses which needs to be excluded from the created subnet pool. This IP address should be: • high than the start IP address, and within or equal to the subnet pool's end IP address

Mode

Global Configuration Mode

Prerequisites

- Subnet pool should have been created before creating an excluded pool. This excluded pool should be within the range of the created subnet pool.
- For example, the excluded pool 20.0.0.20 – 20.0.0.30 created using this command is within the already created subnet pool 20.0.0.0 – 20.0.0.100.

Examples

iS5comm(config)# ip dhcp excluded-address 20.0.0.20 20.0.0.30

24.19. ip dhcp next-server

To set the IP address of the boot server (that is, TFTP server) from which the initial boot file is to be loaded in a DHCP client, use the command **ip dhcp next-server** in Global Configuration Mode. The no form of the command deletes the boot server details and resets to its default value.

ip dhcp next-server

```
ip dhcp next-server <ip address>
```

no ip dhcp next-server

```
no ip dhcp next-server
```

Parameters

Parameter	Type	Description
<ip address>		Enter a valid address for the IP address of the boot server (that is, TFTP server) from which the initial boot file is to be loaded in a DHCP client. This boot server acts as a secondary server.

Mode

Global Configuration Mode

Default

0.0.0.0; No boot server is defined. DHCP server is used as the boot server.

Examples

iS5comm (config)# ip dhcp next-server 12.0.0.1

24.20. ip dhcp ntp-server

To set the NTP server in the host specific DHCP server configuration parameters, use the command **ip dhcp ntp-server** in Global Configuration Mode. The no form of the command deletes the NTP servers from the host specific DHCP server configuration parameters.

ip dhcp ntp-server

```
ip dhcp ntp-server <ip address> [<ip address>]
```

no ip dhcp ntp-server

```
no ip dhcp ntp-server
```

Parameters

Parameter	Type	Description
ntp-server		Enter to set NTP servers in the host specific DHCP server configuration parameters.
ip		Enter to set NTP servers in the host specific DHCP server configuration parameters.
<ip address>		Enter to an unicast IP address for the corresponding NTP servers in the host specific DHCP server configuration.

Mode

Global Configuration Mode

Examples

iS5comm(config)# ip dhcp ntp-server 12.0.0.1 14.0.0.1

24.21. ip dhcp option

To set the DHCP Server options, use the command **ip dhcp server** in Global Configuration Mode. The no form of the command deletes the existing DHCP server option. This command globally configures the various available DHCP server options with the corresponding specific values. These values can be an ASCII string, hexadecimal string or IP address. These global options are applicable for all DHCP server address pools.

ip dhcp option

```
ip dhcp option <code (1-2147483647)> {ascii <string> | hex <string> | <ip address>}
```

no ip dhcp option

```
no ip dhcp option <code (1-2147483647)>
```

Parameters

Parameter	Type	Description
<code (1-2147483647)>	Integer	Enter a value for the unique DHCP option code that represents a specific DHCP option used in a DHCP OFFER message in response to a DHCP DISCOVER message. This value ranges from 1 to 2147483647.
ascii		Enter to configure the ASCII value to be set for the corresponding option code that accepts ASCII string.
<string>		Enter an ASCII value to be set for the corresponding option code that accepts ASCII string. This value is a character string that should contain only characters from NVT ASCII character set.
hex		Enter to configure the hexadecimal value to be set for the corresponding option code that accepts hexadecimal string.
<string>		Enter a hexadecimal value for the corresponding option code.
<ip address>		Enter to configure the unicast IP address to be set for the corresponding option code that accepts IP address.

Mode

Global Configuration Mode

Examples

iS5comm(config)# ip dhcp option 19 hex d

iS5comm# show ip dhcp server pools

```
    Global Options
    --------------
    Code       :    19, Value      : 0
```

24.22. ip dhcp pool

To create a DHCP server address pool and enters DHCP pool configuration mode in which the pool is customized, use the command **ip dhcp pool** in Global Configuration Mode. The address pool has a range of IP addresses that can be assigned to the DHCP client and also information about client configuration parameters such as domain name. The no form of the command deletes the existing DHCP server address pool.

ip dhcp pool

```
ip dhcp pool <index (1-2147483647)> [<Pool Name>]
```

no ip dhcp pool

```
no ip dhcp pool <index (1-2147483647)>
```

Parameters

Parameter	Type	Description
<index (1-2147483647)>		Enter to a value for a unique ID for the specified DHCP server address pool. This value ranges from 1 to 2147483647.
<Pool Name>		Enter a name for the poll; the format is a string.

Mode

Global Configuration Mode

Examples

iS5comm (config)# ip dhcp pool 1 PoolZD

iS5comm(dhcp-config)

24.23. ip dhcp relay

To define the type of information to be present in circuit ID sub-option that is used in the DHCP relay agent information option or enable support for the DHCP relay agent information option, use the command **ip dhcp relay** in Global Configuration Mode. The no form of the command disables the processing related to DHCP relay agent information option.

ip dhcp relay

```
ip dhcp relay {circuit-id option {router-index | vlanid | recv-port} |
information option}
```

no ip dhcp relay

```
no ip dhcp relay information option
```

Parameters

Parameter	Type	Description
circuit-id		Enter to define the type of information to be present in circuit ID sub-option that is used in the DHCP relay agent information option. **NOTE:** The type of information to be present in the circuit ID sub-option can be configured, only if the DHCP relay agent is enabled to perform processing related to DHCP relay agent information option.
option		Enter to configure the option related configuration.
router-index		Enter to add information related to router interface indexes in the circuit ID sub-option. This is the default option.
vlanid		Enter to enable the Default Circuit Id information in the relay agent information (RAI) option. The recv-port can be a physical interface index or lag port.
recv-port		Enter to add information related to physical interfaces or LAG ports in the circuit ID sub-option.
information		Enter to enable the DHCP relay agent information (RAI) option. By using the RAI option, the DHCP relay agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server. By default, processing related to DHCP relay agent information option is disabled. **NOTE:** If RAI is enabled, the circuit-id needs to be configured explicitly by users.
option		Enter to enable the DHCP relay agent information option. By using the relay agent information option, the DHCP relay agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to assign IP addresses, perform access control, and set quality of service (QoS) and security policies (or other parameter-assignment policies) for each subscriber of a service provider network. **NOTE:** Since ip dhcp relay information command is configured in Global Configuration Mode but not in Interface Configuration mode, the global configuration is applied to all interfaces.

Mode

Global Configuration Mode

Examples

iS5comm(config)# ip dhcp relay circuit-id option vlanid

iS5comm(config)# ip dhcp relay information option

24.24. ip dhcp server

To add the configured IP address to the IP address list created for the DHCP server, use the command **ip dhcp server** in Global Configuration Mode. The no form of the command deletes the mentioned IP address from the IP address list.

ip dhcp server

```
ip dhcp server {<ip address> | {offer-reuse <timeout (1-120)>}
```

no ip dhcp server

```
no ip dhcp server {<ip address> | offer-reuse}
```

Parameters

Parameter	Type	Description
<ip address>		Enter to configure the Configure the IP address. The switches or systems having these IP addresses represent the DHCP servers to which the DHCP relay agent can forward the packets that are received from DHCP clients.The DHCP relay agent broadcasts the received packets to entire network except the network from which the packets are received, if the DHCP server list is empty (that is IP address is configured as 0.0.0.0).
offer-reuse		Enter to configure the amount of time the DHCP Server entity would wait for the DHCP REQUEST from the client before reusing the offer.
<timeout (1-120)>		Enter a value for the amount of time the DHCP Server entity would wait for the DHCP REQUEST from the client before reusing the offer.

Mode

Global Configuration Mode

Default

DHCP server list

Prerequisites

The IP address list can contain only 5 IP addresses (that is, only a maximum of 5 DHCP servers can be listed).

Examples

iS5comm(config)# ip dhcp server 12.0.0.1

24.25. ip dhcp sip-server

To set the SIP server in the host specific DHCP server configuration parameters, use the command **ip dhcp sip-server** in Global Configuration Mode. The no form of the command deletes the SIP servers from the host specific DHCP server configuration parameters.

ip dhcp sip-server

```
ip dhcp sip-server {{domain <string> [<string>]} | {ip <ip address> [<ip address>]}}
```

no ip dhcp sip-server

```
no ip dhcp sip-server
```

Parameters

Parameter	Type	Description
`sip-server`		Enter to set SIP servers in the host specific DHCP server configuration parameters. SIP stands for Session Initiation Protocol and refers to a TCP/IP-based network protocol which is often used in Voice-over-IP telephony to establish connection for telephone calls.
`domain`		Enter to configure the domain names for the server.
`string`		Enter a domain name for the server. The domain name should be specified as ASCII string
`ip`		Enter to set SIP servers in the host specific DHCP server configuration parameters.
`<ip address>`		Enter to an unicast IP address for the corresponding SIP servers in the host specific DHCP server configuration.

Mode

Global Configuration Mode

Examples

iS5comm(config)# ip dhcp sip-server domain str str1

24.26. ip dhcp snooping

To enable Layer 2 DHCP snooping in the specific VLAN, use the command **ip dhcp snooping** in VLAN Configuration Mode. The no form of the command globally disables Layer 2 DHCP snooping in the specific VLAN. DHCP snooping feature filters the untrusted DHCP messages to provide security for DHCP servers.

ip dhcp snooping

```
ip dhcp snooping
```

Mode

VLAN Configuration Mode

Default

L2 DHCP snooping is disabled on VLANs.

Examples

iS5comm(config)# int vlan 1

iS5comm (config-vlan)# ip dhcp snooping

24.27. ip dhcp snooping trust

To configure the port as a trusted port, use the command **ip dhcp snooping trust** in Interface Configuration Mode. The no form of the command configures the port as an untrusted port. The packets coming from the trusted port is considered as trusted packets and are not filtered by the DHCP snooping feature.

ip dhcp snooping trust

```
ip dhcp snooping trust
```

Mode

Interface Configuration Mode

Default

Ports are considered trusted.

Examples

iS5comm(config)# interface gi 0/2

iS5comm (config-if)# ip dhcp snooping trust

24.28. ip dhcp snooping

To enable the L2 DHCP snooping in the switch globally or in the specific VLAN or DHCP MAC verification in the switch, use the command **ip dhcp snooping** in Global Configuration Mode. The no form of the command globally disables Layer 2 DHCP snooping in the switch or disables DHCP snooping in the specific VLAN. The DHCP snooping module will stop the protocol operation when the snooping is globally disabled.

ip dhcp snooping

```
ip dhcp snooping [vlan <vlan-id (1-4094)> | verify mac-address]
```

no ip dhcp snooping

```
no ip dhcp snooping [vlan <vlan-id (1-4094)> | verify mac-address]
```

Parameters

Parameter	Type	Description
vlan		Enter to configure L2 DHCP snooping in the specific VLAN. The DHCP snooping module will start the protocol operation when the snooping is enabled globally.
<vlan-id (1-4094)>	Integer	Enter a VLAN ID for the L2 DHCP snooping to be configured. This is a unique value that represents the specific VLAN created. This value ranges from 1 to 4094.
verify		Enter to enable globally DHCP MAC verification in the switch.
mac-address		Enter to start MAC Address verification. If the MAC verification status is enabled, DHCP snooping module will verify whether the source Mac address and client hardware Mac address are same. If they are same, packet will be processed further; else, it is dropped.

Mode

Global Configuration Mode

Default

DHCP MAC address verification is enabled.

Examples

iS5comm (config)# ip dhcp snooping vlan 2

NOTE: The example used and the ip dhcp snooping command used in the config-vlan mode serve the same purpose.

iS5comm (config)# ip dhcp snooping verify mac-address

24.29. lease

To configure the DHCP lease period for an IP address (for the corresponding DHCP server address pool) that is assigned from a DHCP server to a DHCP client, use the command **lease** in DHCP Pool Configuration Mode. The no form of the command resets the DHCP lease period to its default value. The DHCP lease period configuration is deleted and reset if the no form of the network command is executed successfully.

lease

```
lease {<days (0-365)> [<hours (0-23)> [<minutes (1-59)>]] | infinite}
```

no lease

```
no lease
```

Parameters

Parameter	Type	Description
<days (0-365)>	Integer	Enter a value for the number of days that is used to calculate the DHCP lease period. The period also depends on the configured number of hours and minutes. This value ranges from 0 to 365. The value 0 is valid only if either number of hours or minutes is configured with any value other than 0.
<hours (0-23)>	Integer	Enter a value for the number of hours that is used to calculate the DHCP lease period. The period also depends on the configured number of days and minutes. This value ranges from 0 to 23. The value 0 is valid only if either number of days or minutes is configured with any value other than 0.
<minutes (1-59)>	Integer	Enter a value for the number of minutes that is used to calculate the DHCP lease period. The period also depends on the configured number of days and hours. This value ranges from 1 to 59.
infinite		Enter to configure the DHCP lease period as 2147483647 seconds.

Mode

DHCP Pool Configuration Mode

Default

3600 seconds (1 hour)

Prerequisites

The DHCP lease period configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Examples

iS5comm(config)# ip dhcp pool 1 pool1

iS5comm(dhcp-config) # lease 1

24.30. netbios-name

To configure the IP address of a NetBIOS (Network Basic Input / Output System) and WINS (Windows Internet Naming Service) name servers that are available to Microsoft DHCP clients for the corresponding DHCP server address pool, use the command **netbios-name** in DHCP Pool Configuration Mode. The no form of the command deletes the NetBIOS and WINS name servers IP address configuration for the DHCP server address pool. The NetBIOS WINS name server option configuration is deleted, if the no form of the network command is executed successfully.

netbios-name

```
netbios-name <ip address>
```

no netbios-name

```
no netbios-name
```

Parameters

Parameter	Type	Description
<ip address>		Enter a value to configure the NetBIOS and WINS name servers IP address configuration for the DHCP server address pool. The NetBIOS name server provides the following three distinct services: • Name service for name registration and resolution • Session service for connection oriented communication • Datagram distribution service for connectionless communication

Mode

DHCP Pool Configuration Mode

Prerequisites

The NetBIOS WINS name server configuration takes effect only if a subnet pool is already created for the DHCP server address pool.

Examples

iS5comm(config)# ip dhcp pool 1 pool1

iiS5comm(dhcp-config)# netbios-name-server 20.0.0.3

24.31. netbios-node

To configure the NetBIOS node type for Microsoft DHCP clients for the corresponding DHCP server address pool, use the command **netbios-node** in DHCP Pool Configuration Mode. The node type denotes the method used to register and resolve NetBIOS names to IP addresses. The no form of the command deletes thee NetBIOS node type option configuration for the DHCP server address pool.

netbios-node

```
netbios-node {<0-FF> | b-node | h-node | m-node | p-node}
```

no netbios-node

```
no netbios-node
```

Parameters

Parameter	Type	Description
<0-FF>		Enter a value to allow NetBIOS over TCP/IP clients. The value ranges from 0 to 255.
b-mode		Enter to configure the DHCP server address pool to broadcast IP messages for registering and resolving NetBIOS names to IP addresses. The node type value is set as 1.
h-mode		Enter to configure the DHCP server address pool to initially query name server and subsequently broadcast IP messages for registering and resolving NetBIOS names to IP addresses. The node type value is set as 8. This node type is the best option for all conditions.
m-mode		Enter to configure the DHCP server address pool to initially broadcast IP message and then query name server for registering and resolving NetBIOS names to IP addresses. The node type value is set as 4.
p-mode		Enter to configure the DHCP server address pool to have point-to-point communication with a NetBIOS name server for registering and resolving NetBIOS names to IP addresses. The node type value is set as 2.

Mode

DHCP Pool Configuration Mode

Prerequisites

The NetBIOS node type configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Examples

iS5comm(config)# ip dhcp pool 1 pool1

iS5comm (dhcp-config)# netbios-node h-node

24.32. netbios-node-type

To configure the NetBIOS node type for Microsoft DHCP clients for the corresponding DHCP server address pool, use the command **netbios-node-type** in DHCP Pool Configuration Mode. The node type denotes the method used to register and resolve NetBIOS names to IP addresses. The no form of the command deletes the NetBIOS node type option configuration for the DHCP server address pool.

netbios-node-type

```
netbios-node-type {<0-FF> | b-node | h-node | m-node | p-node}
```

no netbios-node-type

```
no netbios-node-type
```

Parameters

Parameter	Type	Description
<0-FF>		Enter a value to allow NetBIOS over TCP/IP clients. It ranges from 0 to 255.
b-mode		Enter to configure the DHCP server address pool to broadcast IP messages for registering and resolving NetBIOS names to IP addresses. The node type value is set as 1.
h-mode		Enter to configure the DHCP server address pool to initially query name server and subsequently broadcast IP messages for registering and resolving NetBIOS names to IP addresses. The node type value is set as 8. This node type is the best option for all conditions.
m-mode		Enter to configure the DHCP server address pool to initially broadcast IP message and then query name server for registering and resolving NetBIOS names to IP addresses. The node type value is set as 4.
p-mode		Enter to configure the DHCP server address pool to have point-to-point communication with a NetBIOS name server for registering and resolving NetBIOS names to IP addresses. The node type value is set as 2.

Mode

DHCP Pool Configuration Mode

Prerequisites

The NetBIOS node type configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Examples

iS5comm(config)# ip dhcp pool 1 pool1

iS5comm (dhcp-config)# netbios-node-type h-node

24.33. network

To create a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client, use the command **network** in DHCP Pool Configuration Mode. The no form of the command deletes the created subnet pool.

network

```
network <start- IP> [<mask> | / <prefix-length (1-31)>] [<end ip>]
```

no network

```
no network
```

Parameters

Parameter	Type	Description
<start-IP>		Enter a value for the IP subnet address for the DHCP pool. The addresses within the specified network subnet are assigned to the DHCP client, if no restriction is applied. For example, the value is configured as 20.0.0.0, then any one of the address within the range from 20.0.0.1 to 20.255.255.254 can be assigned to the DHCP client if no other limitations such as end IP address are set. This value should be unique (that is, one subnet address can be assigned only for one DHCP address pool).
<mask>		Enter a value for the subnet mask for the network IP address. This is a 32-bit number which is used to divide the IP address into network address and host address. This value is used to automatically calculate the end IP address for the pool. For example: The value 254.0.0.0 represents that the end IP address is 21.255.255.254, if the network subnet is set as 20.0.0.0
<prefix-length (1-31)>		Enter a number of high-order bits in the IP address. These bits are common among all hosts within a network. This value should be preceded by a slash (/) with space before and after the slash. This value is used to automatically calculate the end IP address for the pool and set the mask for the subnet. For example: value 20.0.0.0 / 6 represents that the end IP address is 23.255.255.254 and the mask is 252.0.0.0.
<end ip>		Enter a value for the end IP address for the network IP subnet set for the DHCP address pool. This value restricts the IP addresses that can be assigned to the DHCP client. This value is used to manually set the end IP address. This value overrides the end IP address calculated automatically using the mask or prefix-length.

Mode

DHCP Pool Configuration Mode

Default

- mask - 255.0.0.0
- end ip - Represents the last possible subnet address. For example: If network subnet address is mentioned as 20.0.0.0, then end IP address would be 20.255.255.254.

Examples

iS5comm(config)# ip dhcp pool 1 pool1

iS5comm(dhcp-config)# network 20.0.0.0 255.0.0.0 20.0.0.50

24.34. ntp-server

To set the NTP server in the host specific DHCP server configuration parameters, use the command **ntp-server** in DHCP Pool Configuration Mode. The no form of the command deletes the NTP servers from the host specific DHCP server configuration parameters.

ntp-server

```
ntp-server <ip address> [<ip address>]
```

no ntp-server

```
no ntp-server
```

Parameters

Parameter	Type	Description
ntp-server		Enter to set NTP servers in the host specific DHCP server configuration parameters.
ip		Enter to set NTP servers in the host specific DHCP server configuration parameters.
<ip address>		Enter to an unicast IP address for the corresponding NTP servers in the host specific DHCP server configuration.

Mode

DHCP Pool Configuration Mode

Examples

iS5comm(config)# ip dhcp pool 1 pool1

iS5comm (dhcp-config)# ntp-server 12.0.0.1 13.0.0.

24.35. option

To configure the various available DHCP server options with the corresponding specific values for the corresponding DHCP server address pool, use the command **option** in DHCP Pool Configuration Mode. These values can be an ASCII string, hexadecimal string or IP address. The no form of the command deletes he DHCP server option for the DHCP server address pool. The DHCP server option configuration is deleted if the no form of the network command is executed successfully.

option

```
option <code (1-2147483647)> {ascii <string> | hex <hex_str> | <ip address>}
```

no option

```
no option <code (1-2147483647)>
```

Parameters

Parameter	Type	Description
<code (1-2147483647)>	Integer	Enter a value for the unique DHCP option code that represents a specific DHCP option used in a DHCP OFFER message in response to a DHCP DISCOVER message. This value ranges from 1 to 2147483647.
ascii		Enter to configure the ASCII value to be set for the corresponding option code that accepts ASCII string.
<string>		Enter an ASCII value to be set for the corresponding option code that accepts ASCII string. This value is a character string that should contain only characters from NVT ASCII character set.
hex		Enter to configure the hexadecimal value to be set for the corresponding option code that accepts hexadecimal string.
<string>		Enter a hexadecimal value for the corresponding option code.
<ip address>		Enter to configure the unicast IP address to be set for the corresponding option code that accepts IP address.

Mode

DHCP Pool Configuration Mode

Default

Option code - 1

Prerequisites

The DHCP server options configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Examples

iS5comm(config)# ip dhcp pool 1 pool1

iS5comm(dhcp-config) # option 19 hex f

24.36. release dhcp

To immediately release the DHCP lease obtained for an IP address from a DHCP server and assigned to the specified interface, use the command **release dhcp** in Privileged EXEC Mode. The current lease assigned to that interface is terminated manually. The lease is terminated to reset the DHCP client which faces connectivity problem. The DHCP lease provided by the DHCP server represents the time interval till which the DHCP client can use the assigned IP address.

release dhcp

```
release dhcp
 {cpu0 | vlan <vlan-id (1-4094)> | <interface-type> <interface-id>}
```

Parameters

Parameter	Type	Description
`cpu0`		Enter to release the DHCP lease for the management interface.
`vlan`		Enter to configure release of the DHCP lease for a specified VLAN.
`<vlan-id (1-4094)>`	Integer	Enter a VLAN ID for the DHCP lease to be released. This is a unique value that represents the specific VLAN created. This value ranges from 1 to 4094.
`<interface-type>`		Enter to specify the type of interface for the DHCP lease to be released. The interface can be: • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
`<interface-id>`		Enter to configure release of the DHCP lease for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1

Mode

Privileged EXEC Mode

Prerequisites

This command executes successfully only if the VLAN interfaces and router ports are in BOUND state (that is, IP address is dynamically acquired from DHCP server and an active lease is bound to the interface). The port should have been configured as router port for dynamically acquiring an IP address from DHCP server.

Examples

iS5comm# release dhcp vlan 1

24.37. renew dhcp

To immediately renew the DHCP lease for the interface specified, use the command **renew dhcp** in Privileged EXEC Mode. The current lease acquired by the specified interface is manually renewed or else,

when a new DHCP lease is acquired for an interface with a terminated lease. The DHCP lease is automatically renewed, once the lease expires.

renew dhcp

```
renew dhcp
 {cpu0 | vlan <vlan-id (1-4094)> | <interface-type> <interface-id>}
```

Parameters

Parameter	Type	Description
cpu0		Enter to renew the DHCP lease for the management interface.
vlan		Enter to configure renewal of DHCP lease for a specified VLAN.
<vlan-id (1-4094)>	Integer	Enter a VLAN ID for the DHCP lease to be renewed. This is a unique value that represents the specific VLAN created. This value ranges from 1 to 4094.
<interface-type>		Enter to specify the type of interface for the DHCP lease to be renewed. The interface can be: • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
<interface-id>		Enter an interface ID to have configured renewal of the DHCP lease. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.

Mode

Privileged EXEC Mode

Prerequisites

This command executes successfully only if the VLAN interfaces and router ports are in BOUND state (that is, IP address is dynamically acquired from DHCP server and an active lease is bound to the interface). The port should have been configured as router port for dynamically acquiring an IP address from DHCP server.

Examples

iS5comm# renew dhcp vlan 1

24.38. service dhcp

To enable the DHCP server in the switch and relay agent features on router that assigns unique IP addresses and other configuration parameters to interfaces of a DHCP client, use the command **service dhcp** in Global Configuration Mode.The no form of this command disables the DHCP Server. This command is a complete standardized implementation of the existing command and operates similar to that of the command service dhcp-server.

service dhcp

```
service dhcp
```

no service dhcp

```
no service dhcp
```

Mode

Global Configuration Mode

Default

DHCP server is disabled

Prerequisites

The DHCP server can be enabled in the switch, only if the DHCP relay agent is disabled in the switch.

Examples

iS5comm(config)# service dhcp

24.39. service dhcp-relay

To enable the DHCP relay agent in the switch, use the command **service dhcp-relay** in Global Configuration Mode. DHCP relay agent relays DHCP messages between DHCP client and DHCP server located in different subnets. The no form of the command disables the DHCP relay agent.

service dhcp-relay

```
service dhcp-relay
```

no service dhcp-relay

```
no service dhcp-relay
```

Mode

Global Configuration Mode

Default

DHCP relay agent is disabled (that is, the switch acts as a DHCP client)

Prerequisites

The DHCP relay agent can be enabled in the switch, only if the DHCP server is disabled in the switch.

Examples

iS5comm(config)# service dhcp-relay

24.40. service dhcp-server

To enable the DHCP server in the switch (that is, to enable the switch to act as a DHCP server), use the command **service dhcp-server** in Global Configuration Mode. The DHCP server assigns unique IP address and other configuration parameters such as gateway to interfaces of a DHCP client. This is the first step in enabling the DHCP server on the router. The no form of the command disables the DHCP server in the switch.

service dhcp-server

```
service dhcp-server
```

no service dhcp-server

```
no service dhcp-server
```

Mode

Global Configuration Mode

Default

DHCP server is disabled (that is, the switch acts as a DHCP client)

Prerequisites

The DHCP server can be enabled in the switch, only if the DHCP relay agent is disabled in the switch.

Examples

iS5comm(config)# service dhcp-server

24.41. set dhcp-client enable / disable

To enable DHCP services the **set dhcp-client enable/disable** command is used to open the necessary UDP ports and permit access to the service.

set dhcp-client enable/disable

```
set dhcp-client
 {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enables the DHCP client module status
disable		Disables the DHCP client module status

Mode

Global Configuration Mode

Examples

iS5comm# configure terminal

iS5comm(config)# set dhcp-client enable

24.42. show dhcp server

To display the DHCP servers' IP addresses, use the command **show dhcp server** in Privileged EXEC Mode. These addresses denote the PCs or switches that can act as a DHCP server.

show dhcp server

```
show dhcp server
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show dhcp server

```
    Context Name : default
    ------------
    DHCP server                 : 0.0.0.0
```

24.43. show ip dhcp client

To display the unique identifier for the DHCP client, DHCP fast access information, DHCP client options, and DHCP client statistics information, use the command **show ip dhcp client** in Privileged EXEC Mode.

show ip dhcp client

```
show ip dhcp client
 {client-id | fast-access | option | stats}
```

Parameters

Parameter	Type	Description
client-id		Enter to display the unique identifier for the DHCP client.
fast-access		Enter to display DHCP fast access information such as Fast Access Mode status, Dhcp Client Fast Access DiscoverTimeOut, Dhcp Client Fast Access NullStateTimeOut, Dhcp Client Fast Access Arp Check TimeOut values.
option		Enter to display DHCP client options set by a server which provides the details like interface, interface type, length, and value.
stats		Enter to display the DHCP client statistics information for interfaces that are configured to acquire IP address dynamically from the DHCP server. The statistics information contains interface name, IP address assigned by DHCP server, DHCP lease details, details regarding number of DHCPDISCOVER, DHCPREQUEST, DHCPDECLINE, DHCPRELEASE and DHCPINFORM packets received and number of DHCPOFFER packets sent from the DHCP client.

Mode

Privileged EXEC Mode

Examples

iS5comm# show ip dhcp client client-id

iS5comm# show ip dhcp client fast-access

```
DHCP Client Timer Settings
---- ------ ----- -------
Fast Access Mode                        : Enable
DHCP Client Fast Access DiscoverTimeOut : 5
DHCP Client Fast Access NullStateTimeOut : 1
DHCP Client Fast Access Arp Check TimeOut : 1
```

iS5comm# show ip dhcp client option

```
DHCP Client Options

Interface   Type   Len   Value
---------   ----   ---   ------


vlan1  43
vlan1  60  6 vendor
vlan1  66
vlan1  67
vlan1  120
vlan1      240
```

iS5comm# show ip dhcp client stats

```
DHCP Client Statistics
--------------------------I
nterface                     : vlan1
Client IP Address             : 12.0.0.21
Client Lease Time             : 3600
Client Remain Lease Time      : 3569
Message Statistics
------------------
DHCP DISCOVER                 : 1
DHCP REQUEST                  : 1
DHCP DECLINE                  : 0
DHCP RELEASE                  : 0
DHCP INFORM                   : 0
DHCP OFFER                    : 1
```

24.44. show ip dhcp relay

To display the DHCP relay agent configuration information for a VLAN interface or all interfaces for which relay agent details are configured, use the command **show ip dhcp relay** in Privileged EXEC Mode. The information contains status of the DHCP relay, DHCP server IP addresses, status of relay information

option, configured debug level and statistics details regarding number of packets affected by relay information option, circuit ID sub option, remote ID sub option, and subnet mask sub option.

show ip dhcp relay

```
show ip dhcp relay information [vlan <vlan-id (1-4094)>] [<iftype> <ifnum>]
```

Parameters

Parameter	Type	Description
information		Enter to display the DHCP relay agent configuration information.
vlan		Enter to display the DHCP relay agent configuration information for a specified VLAN.
<vlan-id (1-4094)>	Integer	Enter a VLAN ID for the DHCP relay agent configuration information to be displayed. This is a unique value that represents the specific VLAN created. This value ranges from 1 to 4094.
<iftype>		Enter to specify the type of interface for the DHCP relay agent configuration information to be displayed. The interface can be: • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
<ifnum>		Enter a number for interface identifier for the DHCP relay agent configuration information to be displayed. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1

Mode

Privileged EXEC Mode

Examples

iS5comm# show ip dhcp relay information

```
Context Name: default
------------
DHCP Relay : Disabled
DHCP Relay Servers only : Enabled
```

```
DHCP server : 0.0.0.0

DHCP Relay RAI option : Disabled
Default Circuit Id information : router-index
Debug Level : 0x0

No of Packets inserted RAI option : 0
No of Packets inserted circuit ID sub option : 0
No of Packets inserted remote ID sub option : 0
No of Packets inserted subnet mask sub option : 0
No of Packets dropped : 0
No of Packets which did not inserted RAI option : 0
```

24.45. show ip dhcp server

To display the DHCP server binding, configuration, information, global DHCP option configuration for all DHCP server address pools and various DHCP server statistics-related, use the command **show ip dhcp server** in Privileged EXEC Mode.

show ip dhcp server

```
show ip dhcp server
 {binding | information | pools | statistics}
```

Parameters

Parameter	Type	Description
binding		Enter to display the DHCP server binding information. A DHCP binding is created when a DHCP server assigns an IP address to a DHCP client. The information contains the allocated IP address, host hardware type, host hardware address, binding state and expiry time of the allocated DHCP lease
information		Enter to display the DHCP server configuration information. The information contains status of DHCP server, ICMP echo mechanism, debug level, boot server IP address, boot file name and server offer reuse time.
pool		Enter to display the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.
statistics		Enter to display the various DHCP server statistics-related information such as number of DHCPDECLINE messages received, DHCPOFFER messages sent and so on.

Mode

Privileged EXEC Mode

Prerequisites

The DHCP server binding information is displayed, only if the DHCP server is enabled and the DHCP binding is created.

Examples

iS5comm# show ip dhcp server binding

```
Ip       Hw                      Binding  Expire
Address  Type     Address           State    Time
-------  ----     -------           ------   ------
12.0.0.2 Ethernet 00:02:02:03:04:01 Assigned May 12 13:22:41 2009
```

iS5comm# show ip dhcp server information

```
DHCP server status                : Enable
Send Ping Packets                 : Enable
Debug level                       : All
Server Address Reuse Timeout      : 10 secs
```

```
    Next Server Address                : 12.0.0.1
    Boot file name                     : boot1.img
```

iS5comm# show ip dhcp server pools

```
    Global Options
    --------------

    Code       :    19, Value      : 0

    Pool Id                         : 1
    ----------------------------------------
    Pool Name                       : pool1
    Subnet                          : 20.0.0.0
    Subnet Mask                     : 255.0.0.0
    Lease time                      : 2147483647 secs
    Utilization threshold           : 76%
    Start Ip                        : 20.0.0.1
    End Ip                          : 20.0.0.50
    Exclude Address Start IP        : 20.0.0.1
    Exclude Address End IP          : 20.0.0.30
    Exclude Address Start IP        : 20.0.0.20
    Exclude Address End IP          : 20.0.0.30

    Subnet Options
    --------------
    Code       :     1, Value      : 255.0.0.0
    Code       :     3, Value      : 10.23.2.99
    Code       :     6, Value      : 12.0.0.1
    Code       :    15, Value      : 12
    Code       :    19, Value      : 0
    Code       :    43, Value      : ven
    Code       :    46, Value      : 8

    Host Options
    ------------
    Client Identifier               Hardware type        Code       Value
    00:01:02:03:04:01               1                    67         abcd
```

iS5comm# show ip dhcp server statistics

```
    Address pools : 1

    Message                Received
```

```
-------                 --------
DHCPDISCOVER            0
DHCPREQUEST             0
DHCPDECLINE             0
DHCPRELEASE             0
DHCPINFORM              0
Message                 Sent
-------                 ----
DHCPOFFER               0
DHCPACK                 0
DHCPNAK                 0
```

24.46. show ip dhcp snooping

To display global configuration of DHCP snooping and the DHCP snooping configuration and statistics of all VLANs in which the DHCP snooping feature is enabled, use the command **show ip dhcp snooping** in Privileged EXEC Mode.

show ip dhcp snooping

```
show ip dhcp snooping
 [globals] [vlan <vlan-id (1-4094)>]
```

Parameters

Parameter	Type	Description
globals		Enter to display the global configuration of DHCP snooping. The global status of Layer 2 DHCP snooping and MAC verification are displayed.
vlan		Enter to display L2 DHCP snooping in the specific VLAN. The DHCP snooping module will start the protocol operation when the snooping is enabled globally.
<vlan-id (1-4094)>	Integer	Enter a VLAN ID for the L2 DHCP snooping to be configured. This is a unique value that represents the specific VLAN created. This value ranges from 1 to 4094.

Mode

Privileged EXEC Mode

Prerequisites

The DHCP server binding information is displayed, only if the DHCP server is enabled and the DHCP binding is created.

Examples

iS5comm# show ip dhcp snooping globals

```
DHCP Snooping Global information
--------------------------------

Switch : default
-------  -------
Layer 2 DHCP Snooping is globally disabled
MAC Address verification is enabled
```

iS5comm# show ip dhcp snooping vlan 2

```
DHCP Snooping Vlan information
------------------------------
VLAN                           : 2
Snooping status                : Enabled
Number of Incoming Discovers   : 0
Number of Incoming Requests    : 0
Number of Incoming Releases    : 0
Number of Incoming Declines    : 0
Number of Incoming Informs     : 0
Number of Transmitted Offers   : 0
Number of Transmitted Acks     : 0
Number of Transmitted Naks     : 0
Total Number Of Discards       : 0
Number of MAC Discards         : 0
Number of Server Discards      : 0
Number of Option Discards      : 0
```

24.47. show dhcp-client module status

The **show dhcp-client module status** command shows the DHCP module status. It indicates to the user if the module is enabled or disabled. It also shows the UDP port which is in use.

show dhcp-client module status

```
show dhcp-client module status
```

Mode

Privileged Execution Mode

Examples

iS5comm# show dhcp-client module status

24.48. sip-server

To set the Session Initiation Protocol (SIP) server in the host specific DHCP server configuration parameters, use the command **sip-server** in Global Configuration Mode. The no form of the command deletes the SIP server from the host specific DHCP server configuration parameters.

sip-server

```
sip-server {{domain <string> [<string>]} | {ip <ip address> [<ip address>]}}
```

no sip-server

```
no sip-server
```

Parameters

Parameter	Type	Description
sip-server		Enter to set SIP servers in the host specific DHCP server configuration parameters. SIP stands for Session Initiation Protocol and refers to a TCP/IP-based network protocol which is often used in Voice-over-IP telephony to establish connection for telephone calls.
domain		Enter to configure the domain names for the server.
string		Enter a domain name for the server. The domain name should be specified as ASCII string
ip		Enter to set SIP servers in the host specific DHCP server configuration parameters.
<ip address>		Enter to an unicast IP address for the corresponding SIP servers in the host specific DHCP server configuration.

Mode

Global Configuration Mode

Examples

iS5comm(config)# ip dhcp pool 1 pool1

iS5comm (dhcp-config)# sip-server domain str str1

iS5comm (dhcp-config)# sip-server ip 12.0.0.1 13.0.0.0

24.49. utilization threshold

To configure the pool utilization threshold value (as percentage) for the corresponding DHCP server address pool, use the command **utilization threshold** in DHCP Pool Configuration Mode. The no form of the command resets the pool utilization threshold value to its default value for the DHCP server address pool.

utilization threshold

```
utilization threshold <integer (0-100)>
```

no utilization threshold

```
no utilization threshold
```

Parameters

Parameter	Type	Description
<integer (0-100)>	Integer	Enter a value for the pool utilization threshold value (as percentage) for the corresponding DHCP server address pool.

Mode

DHCP Pool Configuration Mode

Default

75 percent

Prerequisites

The pool utilization threshold configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Examples

iS5comm(config)# ip dhcp pool 1 pool1

iS5comm(dhcp-config) # utilization threshold 76

24.50. vendor-specific

To set the vendor specific information in the pool specific DHCP server configuration parameters, use the command **vendor-specific** in DHCP Pool Configuration Mode. The no form of the command deletes vendor-specific information from the pool specific DHCP server configuration parameters.

vendor-specific

```
vendor-specific <vendor-specific-string> [<vendor-specific-string>]
```

no vendor-specific

```
no vendor-specific
```

Parameters

Parameter	Type	Description
<vendor-specific-string>		Enter to configure vendor-specific details for the DHCP server.

Mode

DHCP Pool Configuration Mode

Examples

iS5comm(config)# ip dhcp pool 1 pool1

iS5comm (dhcp-config)# vendor-specific ven

RIP

25. RIP

RIP (Routing Information Protocol) is a widely used protocol for managing router information within a self-contained network such as a corporate local area network or an interconnected group of such LANs. RIP is classified by the IETF (Internet Engineering Task Force) as one of several internal gateway protocols.

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers about the change. These updates are sent independently of the regularly scheduled updates that RIP routers send. RIP uses a hop count to determine network distance. Each host with a router in the network uses the routing table information to determine the next host to route a packet for a specified destination.

25.1. auto-summary

To enable auto summarization feature in RIP, enable or disable the auto summarization of routes in RIP, and restore the default behavior of automatic summarization of subnet routes into network-level routes, use the command **auto-summary** in RIP Router Configuration Mode.

auto-summary

```
auto-summary [enable] [disable]
```

Parameters

Parameter	Type	Description
enable		Enter to enable auto summarization feature in RIP, so that the summary routes are sent in regular updates for RIP. This is the default.
disable		Enter to disable auto summarization feature in RIP, so that either individual subnet route is sent or subnet routes are sent based on the specific aggregation configured over the interface.

Mode

RIP Router Configuration Mode

Prerequisites

Auto-summarization feature must be disabled to configure interface specific aggregation with RIP version 2.

Examples

iS5comm(config)# router rip

is5comm(config-router)# auto-summary disable

25.2. debug ip rip

To set the debug level for RIP module, use the command **debug ip rip** in Privileged EXEC Mode. The no form of the command resets the debug level for RIP module. This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

debug ip rip

```
debug ip rip [{all | buffer | control | data | database | dump  | events |
failure | init | mgmt | os | triggers}
```

debug ip rip

```
debug ip rip [{all | buffer | control | data | database | dump  | events |
failure | init | mgmt | os | triggers}
```

Parameters

Parameter	Type	Description
`all`		Enter to generate debug statements for all traces.
`buffer`		Enter to generate debug statements for Buffer traces.
`control`		Enter to generate debug statements for Control Plane traces.
`data`		Enter to generate debug statements for Data path traces. This trace is generated during failure in packet processing.
`database`		Enter to generate debug statements for database related traces
`dump`		Enter to generate debug statements for Packet Dump traces.
`events`		Enter to generate debug statements for Events related traces.
`failure`		Enter to generate debug statements for All failure messages including Packet Validation.
`init`		Enter to generate debug statements for Initialization and Shutdown traces. This trace is generated on failed initialization of RIP related entries. This is default.
`mgmt`		Enter to generate debug statements for Management traces. This trace is generated during failure in configuration of any of the RIP features.
`os`		Enter to generate debug statements for OS Resource traces. This trace is generated during failure in message queues.
`triggers`		Enter to generate debug statements for Triggers related traces.

Mode

Privileged EXEC Mode

Prerequisites

This command executes only if RIP is enabled.

Examples

iS5comm# debug ip rip all

25.3. default-information

To set the metric to be used for default route propagated over the interface, use the command **default-information** in Interface Configuration Mode. The no form of the command disables the origination of default route over the interface. The administrative distance can be enabled for one route map only. If distance needs to be enabled for a route map, then distance should be disabled for an already assigned route map. This command is a standardized implementation of the existing command: ip rip default route originate. It operates similar to the existing command.

default-information

```
default-information originate <metric (1-15)> [route-map <string(32)>]
```

no default-information

```
no default-information originate
```

Parameters

Parameter	Type	Description
originate		Enter to enable default route propagated over the interface. This distance value will not be used for distributing list.
<metric(1-15)>	Integer	Enter a metric value to be used for default route. This value ranges from 1 to 15.
route-map		Enter to configure the name of the existing route map for which the metric value should be enabled and set.
<string(32)>	Integer	Enter a name of the existing route map for which the metric value should be enabled and set. This value is a string with the maximum size of 32.

Mode

Interface Configuration Mode

Examples

iS5comm(config-if)# default-information originate 10

25.4. default-metric

To set the default metric values to be used for redistributed routes for RIP, use the command **default-metric** in RIP Router Configuration Mode. The command is used in conjunction with the redis-

tribute router command to cause the current routing protocol to use the same metric value for all redistributed routes. The no form of the command sets the metric used with redistributed routes to its default value. The metric value given in the no form of the command will be ignored during the execution of the command.

default-metric

```
default-metric [<value (1-16)>]
```

no default-metric

```
no default-metric [<short (1-16)>]
```

Parameters

Parameter	Type	Description
<value>		Enter a route-map value. A default metric helps in solving the problem of redistributing routes with incompatible metrics. The default metric provides a reasonable substitute and enables the redistribution to proceed further. The metric value ranges between 1 and 16.

Mode

RIP Router Configuration Mode

Default

3

Examples

iS5comm(config)# router rip

iS5comm(config-router)# default-metric 1

25.5. distance

To enable the administrative distance (that is, the metric to reach destination) of the routing protocol and set the administrative distance value, use the command **distance** in RIP Router Configuration Mode. The no form of this command disables the administrative distance.

distance

```
distance <1-255> [route-map <name(1-20)>]
```

no distance

```
no distance [route-map <name(1-20)>]
```

Parameters

Parameter	Type	Description
<1-255>	Integer	Enter a value for the administrative distance. The distance value (i.e. the preference value) ranges between 1 and 255. The default is 121. This distance value will not be used for distribute list. The administrative distance can be enabled for only one route map. The distance should be disabled for the already assigned route map, if distance needs to be enabled for another route map.
route-map		Enter to configure the name of the Route Map for which the distance value should be enabled and set
<name(1-20)>		Enter a name for the Route Map for which the distance value should be enabled and set. This value is a string with maximum string of 20.

Mode

RIP Router Configuration Mode

Default

121

Examples

iS5comm(config)# router rip

is5comm(config-router)# distance 10 route-map rmap-test

25.6. distribute-list

To enable route map filtering for inbound or outbound routes and define the conditions for distributing the routes from one routing protocol to another, use the command **distribute-list** in RIP Router Configuration Mode. The no form of the command disables route map filtering for inbound or outbound routes.

distribute-list

```
distribute-list route-map <name (1-20)> {in | out}
```

no distribute-list

```
no distribute-list route-map <name (1-20)> {in | out}
```

Parameters

Parameter	Type	Description
route-map		Enter to configure a route map filtering for inbound or outbound routes and defines the conditions for distributing the routes from one routing protocol to another.
<name(1-20)>	Integer	Enter a name for a route map. This is a string with maximum size of 20.
in		Enter to set route map filtering for inbound routes.
out		Enter to set route map filtering for outbound routes.

Mode

RIP Router Configuration Mode

Prerequisites

Only one route map can be set for inbound or outbound routes. Another route map can be assigned, only if the already assigned route map is disabled.

Examples

iS5comm(config)# router rip

iS5comm(config-router)# distribute-list route-map rmap-test in

25.7. ip rip

For RIP- related configuration, use the command **ip rip** in VLAN Interface Configuration Mode. The no form of this command deletes the RIP related configuration or sets all configured values to default.

ip rip

```
ip rip
 {auth-type {md5 | sha-1 | sha-256 | sha-512}
 | authentication {key-chain <key-chain-name (16)>
 | key-id <integer (0-255)> key <key string(16)>
 | mode {md5 [key <key string(16)>] | text [key <key string(16)>]}
```

```
 | default route {install | originate <metric(1-15)>}
 | key-id <key-id (0-255)> {start-accept <key> | start-generate <key> |
stop-accept <key> | stop-generate <key>}
 | receive version {1 [2] |2 [1] | none}
 | send [demand] {version {1 [2] |2 [1] | none}
 | summary-address <ip-address> <mask>
 }
```

no ip rip

```
no ip rip
 {authentication {key-chain <key-chain-name (16)> | key-id <integer (0-255)>
| mode}
 | default route {install | originate}
 | receive version | send version | summary-address <ip-address> <mask>
 }
```

Parameters

Parameter	Type	Description
auth-type		Enter to configure the authentication type.
md5		Enter to set the authentication type as keyed message digest 5 (MD5) authentication mechanism. This is the default option.
sha-1		Enter to set the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes.
sha-256		Enter to set the authentication type as Secure Hash Algorithm 256 (SHA256) authentication. SHA256 generates Authentication digest of length 32 bytes.
sha-512		Enter to set the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. SHA512 generates Authentication digest with length of 64 bytes.
authentication		Enter to configure the authentication mode and key to be used in RIP packets for VLAN interface / router port. **NOTE:** • This command executes only if RIP is enabled in the switch. • Only the configurations that are done after associating the IP address of the VLAN interface / router port with the RIP routing process, are applied to the RIP
key-chain		Enter to configure the interface RIP version 2 authentication string.
<key-chain string(16)>		Enter a value for the interface RIP version 2 authentication string.- a string of size 16.
key-id		Enter to configure the authentication key ID and the authentication key as part of crypto key configuration.
<integer (0-255)>	Integer	Enter a value to configure the active authentication key ID to be used in the interface for sending RIP updates. This value ranges from 0 to 255.
key		Enter to configure the authentication key.
<key string(16)>		Enter a value for the authentication key - a string of size 16. If a string shorter than 16 octets is supplied, it will be left- justified and padded to 16 octets, on the right, with nulls (0x00).This command is a standardized implementation of the existing command “ip rip authentication mode - key-chain”. It operates similar to the existing command.

Parameter	Type	Description
mode	Integer	Enter to configure the authentication mode for RIP version 2. The default is None (No authentication is set)
md5		Enter to set the authentication type as keyed MD5.
key		Enter to configure the authentication key as keyed MD5.
<key string(16)>		Enter a value for the authentication key - a string of size 16. If a string shorter than 16 octets is supplied, it will be left- justified and padded to 16 octets, on the right, with nulls (0x00).This command is a standardized implementation of the existing command “ip rip authentication mode - key-chain”. It operates similar to the existing command.
text		Enter to set the authentication type as keyed message digest 5 (MD5) authentication mechanism.
key		Enter to configure the authentication key as simple text.
<key string(16)>		Enter a value for the authentication key - a string of size 16. If a string shorter than 16 octets is supplied, it will be left- justified and padded to 16 octets, on the right, with nulls (0x00).This command is a standardized implementation of the existing command “ip rip authentication mode - key-chain”. It operates similar to the existing command.
default		Enter to install the default route received in updates to the RIP database. By default, the default route origination is disabled. Only the configurations that are done after associating the IP address of the VLAN interface / router port with the RIP routing process are applied to the RIP.
route		Enter to install the default route received in updates to the RIP database.
install		Enter to install the default route received in updates to the RIP database.
originate		Enter to set the metric to be used for default route propagated over the VLAN interface / router port in a RIP update message and generate a default route into RIP.
<metric(1-15)>	Integer	Enter a value for the metric to be used for default route propagated over the VLAN interface / router port in a RIP update message. The metric value ranges between 1 and 15.

Parameter	Type	Description
key-id		Enter to configure the time as created with the configured key idwhen the router starts managing the packets. **NOTE:** This command executes only if, • RIP authentication mode is configured.
<Key-ID (0-255)>	Integer	Enter a value to configure the active authentication Key ID in the interface. This value ranges from 0 to 255.
start-accept		Enter to configure the time when the router will start accepting packets that have been created with the configured key-id.
<key>		Enter a value for the time when the router will start accepting packets that have been created with the configured key-id. If the value is not set then the current time (time at which authentication key-id is configured) will be considered as start-accept time. **NOTE:** For example, Tuesday May 26, 1992 at 1:30:15 PM should be entered as, 1992-5-26,13:30:15 (YYYY-MM-DD,hh:mm:ss format).
start-generate		Enter to configure the time when the router will start using this key for packet generation.
<key>		Enter a value for the time when the router will start using this key for packet generation. If the value is not set then the current time (time at which authentication key-id is configured) will be considered as start-accept time. **NOTE:** For example, Tuesday May 26, 1992 at 1:30:15 PM should be entered as, 1992-5-26,13:30:15 (YYYY-MM-DD,hh:mm:ss format).
stop-generate		Enter to configure the time when the router will stop using the key for packet generation.
<key>		Enter a value for the time when the router will top using the key for packet generation. If the value is not set then the current time (time at which authentication key-id is configured) will be considered as start-accept time. **NOTE:** For example, Tuesday May 26, 1992 at 1:30:15 PM should be entered as, 1992-5-26,13:30:15 (YYYY-MM-DD,hh:mm:ss format).
stop-accept		Enter to configure the time when the router will stop using the key for packet generation.
<key>		Enter a value for the time when the router will stop accepting OSPF packets with specified key id. Stop accept value is configured in 24 hours format. **NOTE:** For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30

Parameter	Type	Description
receive		Enter to set IP RIP version number for receiving advertisements (that is, version of RIP updates to be received on a VLAN interface / Router port). Only the configurations that are done after associating the IP address of the VLAN interface / router port with the RIP routing process, are applied to the RIP.
version		Enter to set IP RIP version number for receiving advertisements (that is, version of RIP updates to be received on a VLAN interface / Router port).
1		Enter to set the global version of RIP as 1. This implies that RIP updates are sent/ received in compliance with RFC 1058.
2		Enter to set the global version of RIP as 2. This implies that only multicasting RIP updates are sent/received.
none		Enter to configure that no RIP update is to be received.
send		Enter to set IP RIP version number for transmitting advertisements (that is, version of RIP updates to be sent on a VLAN interface / Router port). Only the configurations that are done after associating the IP address of the VLAN interface / router port with the RIP routing process, are applied to the RIP
demand		Enter to configure the RIP version number for demand trigger updates.
version		Enter to configure version number version of RIP updates to be sent.
1		Enter to configure sending only RIP updates compliant with RFC 1058, on the interface.
2		Enter to configure sending only multicasting RIP updates on the interface.
none		Enter to configure that no RIP update is to be sent.

Parameter	Type	Description
summary-address		Enter to set route aggregation over a VLAN interface/router port for all subnet routes that fall under the specified IP address and mask. **NOTE:** • Only the configurations that are done after associating the IP address of the VLAN interface / router port with the RIP routing process, are applied to the RIP. • This command should not be used with RIPv1 send version. • Auto-summarization overrides interface specific aggregation. Therefore, auto-summarization should be disabled for interface specific route aggregation.
<ip-address>		Enter a value for the IP address that is to be combined with the subnet mask to set route aggregation for all subnet routes that fall under the specified IP address and mask of the interface specific aggregation.
<mask>		Enter a value for the subnet mask that is to be combined with the IP address to set route aggregation for all subnet routes that fall under the specified mask and IP address of the interface specific aggregation

Mode

VLAN Interface Configuration Mode

Prerequisites

This command executes only if RIP is enabled in the switch.

Examples

iS5comm(config)# int vlan 2

iS5comm(config-if)# ip rip auth-type md5

iS5comm(config-if)# ip rip authentication key-chain abc

iS5comm(config-if)# ip rip authentication key-id 0 key key1

iS5comm(config-if)# ip rip authentication mode text

iS5comm(config-if)# ip rip default route originate 10

iS5comm(config-if)# ip rip key-id 0 start-accept 2014-07-22,12:26:30

iS5comm(config-if)# ip rip key-id 0 stop-accept 2014-07-22,12:26:30

iS5comm(config-if)# ip rip key-id 0 start-generate 2014-07-22,12:26:30

iS5comm(config-if)# ip rip key-id 0 stop-generate 2014-07-22,12:26:30

iS5comm(config-if)# ip rip receive version 1

iS5comm(config-if)# ip rip send version 1

iS5comm(config-if)# ip rip summary-address 12.0.0.0 255.0.0.0

25.8. ip rip

To configure the security level of the RIP in the system to accept / ignore RIPv1 packets when authentication is in use and determine the retransmission timeout interval and number of retries to retransmit the update request packet or an unacknowledged update response packet, use the command **ip rip** in RIP Router Configuration Mode. The no form of the command resets the security level, retransmission timeout interval, or the number of retransmission retries to their default values.

ip rip

```
ip rip
 {retransmission {interval <timeout-value (5-10)> | retries <value (10-40)>}
 | security {minimum | maximum}
```

no ip rip

```
no ip rip {retransmit {interval | retries} | security}
```

Parameters

Parameter	Type	Description
retransmission / retransmit		Enter to configure the security level of the RIP in the system to accept / ignore RIPv1 packets when authentication is in use.
interval		Enter to configure the timeout interval to be used to retransmit the update request packet or an unacknowledged update response packet. The packets are transmitted at the specified interval till a response is received or the maximum retries.
<timeout-value (5-10)>	Integer	Enter a timeout interval value for retransmitting the update request packet or an unacknowledged update response packet. This value ranges from 5 to 10. The default value is 5.
retries		Enter to configure the maximum number of retransmissions of the update request and update response packets.
<value (10-40)>	Integer	Enter a value for the maximum number of retransmissions of the update request and update response packets. This value ranges from 10 to 40. The default value is 36.
security		Enter to configure the retransmission timeout interval and number of retries to retransmit the update request packet or an unacknowledged update response packet.
minimum		Enter to configure that RIP1 packets will be accepted even when authentication is in use.
maximum		Enter to configure that RIP1 packets will be ignored when authentication is in use. This is the default option.

Mode

RIP Router Configuration Mode

Examples

iS5comm(config)# router rip

iS5comm(config-router)# ip rip retransmission retries 30

iS5comm(config-router)# ip rip security minimum

25.9. ip split-horizon

To enable the split horizon updates for the RIP, which prevents the routing loops in distance routing protocol, by prohibiting the router from advertising a route back onto the interface, use the command **ip split-horizon** in VLAN Interface Configuration Mode.

ip split-horizon

```
ip split-horizon [poisson]
```

Parameters

Parameter	Type	Description
poisson		Enter to configure the split horizon with poison reverse enabled.

Mode

VLAN Interface Configuration Mode

Default

Split horizon with poison reverse is enabled.

Examples

iS5comm(config)# int vlan 2

iS5comm(config-if)# ip split-horizon

25.10. neighbor

To add a trusted neighbor router with which routing information can be exchanged and from which RIP packets can be accepted, use the command **neighbor** in RIP Router Configuration Mode. This command permits the point-to-point (nonbroadcast) exchange of routing information. When used in combination with the passive-interface vlan, router configuration command, routing information can be exchanged between a subset of routers an access servers. On a LAN, multiple neighbor commands can be used to specify additional neighbors or peers. The no form of the command deletes a trusted neighbor router.

neighbor

```
neighbor <ip-address>
```

Parameters

Parameter	Type	Description
<ip-address>		Enter an Unicast IP address for the trusted neighbor.

Mode

RIP Router Configuration

Examples

iS5comm(config)# router rip

iS5comm(config-router)# neighbor 10.0.0.5

25.11. network

To enable RIP on a primary IP network or a secondary IP network or an unnumbered VLAN interface / router port, use the command **network** in RIP Router Configuration Mode. It configures a list of networks for the RIP routing process. RIP routing updates will be sent and received only through the specified interfaces on this network. If an interface's network is not specified, then the network will not be advertised in any RIP update. This should be configurable for Primary and Secondary IP address. The no form of the command disables RIP on a primary IP network or a secondary IP network or an unnumbered VLAN interface / router port

network

```
network <ip-address> [unnum {vlan <vlan-id/vfi-id> [switch <switch name>]
 | <iftype> <ifnum>}]
```

no network

```
no network <ip-address> [unnum {vlan <vlan-id/vfi-id> [switch <switch name>]
| <iftype> <ifnum>}]
```

Parameters

Parameter	Type	Description
<ip-address>		Enter to configure the IP network address of the interface that is to be associated with RIP routing process. This can be either Primary or Secondary IP address. • The network IP address specified must not contain any subnet information. RIP routing updates will be sent and received only through interfaces on this network. • The Primary IP address should be same as that of the existing VLAN interface / router port. • The Secondary IP address should be same as that of the existing VLAN interface / router port
unnum		Enter for unnumbered interface to be used.
vlan		Enter to configure the unnumbered VLAN / VFI ID that is to be associated with RIP routing process.
<vlan-id/vfi-id>	Integer	Enter a VLAN ID for unnumbered VLAN / VFI ID that is to be associated with RIP routing process. This value ranges from 1 to 65535. • <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id> - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.
switch		Enter to configure the switch context for the unnumbered VLAN ID.
<switch-name>		Enter a switch name. Currently is default.

Parameter	Type	Description
<iftype>		Enter to configure the type of unnumbered router interface that is to be associated with RIP routing process. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
<ifnum>		Enter to configure the unnumbered router interface identifier. This is a unique value that represents the specific interface that is to be associated with RIP routing process. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan or port-channel ID.

Mode

RIP Router Configuration

Examples

iS5comm(config-router)# network 12.0.0.1

25.12. output-delay

To enable interpacket delay for RIP updates, where the delay is in milliseconds between packets in a multiple-packet RIP update, use the command **output-delay** in RIP Router Configuration Mode. This interpacket delay feature helps in preventing the routing table from losing information due to flow of RIP update from a high speed router to la ow speed router. The no form of the command disables interpacket delay for RIP updates.

output-delay

```
output-delay <milli-seconds (8-50)>
```

no output-delay

```
no output-delay
```

Parameters

Parameter	Type	Description
<milli-seconds (8-50)>		Enter a value for the interpacket delay. The delay between packets in a multiple-packet RIP update is in milliseconds and can range between 8 to 50 milliseconds.

Mode

RIP Router Configuration Mode

Default

Disabled (Interpacket delay feature is disabled).

Examples

iS5comm(config)# router rip

iS5comm (config-router)# output-delay 10

25.13. passive-interface

To suppress the RIP routing updates on a specified VLAN interface in a defined L2 switch context / default context or on a specified router port, use the command **passive-interface** in RIP Router Configuration Mode. It denotes that the RIP process runs in a passive VLAN interface / passive router port. If the sending of routing updates is disabled on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed. The no form of the command restricts suppressing of RIP routing updates from an interface

passive-interface

```
passive-interface {vlan <vlan-id/vfi-id> [switch <switch-name>] | <inter-
face-type> <interface-id>}
```

no passive-interface

```
no passive-interface {vlan <vlan-id/vfi-id> [switch <switch-name>] | <inter-
face-type> <interface-id>}
```

Parameters

Parameter	Type	Description
vlan		Enter to configure a specified VLAN/VFI interface as a passive interface on which RIP routing updates are suppressed.
<vlan-id/ vfi-id>	Integer	Enter a value for the VLAN ID or VFI-ID for which the passive interface will be configured. This value ranges from 1 to 65535. The options are as follow: • <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535. **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries. **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
switch		Enter to configure a switch context for the VLAN interface that is set as passive interface.
<switch-name>		Enter default for switch name.
<interface-type>		Enter interface type to configure the passive interface. The interface types are: • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links
<interface-id>		Enter a value interface number to configure the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example, 0/1 represents that the slot number is 0 and port number is 1.

Mode

RIP Router Configuration Mode

Prerequisites

This command executes only if RIP is enabled on an IP network.

Examples

iS5comm(config)# router rip

iS5comm(config-router)# passive-interface vlan 55

25.14. redistribute

To enable RIP to participate in route redistribution, use the command **redistribute** in RIP Router Configuration Mode. When enabled, RIP starts advertising the routes learned by other protocols. The no form of the command disables RIP to participate in route redistribution. When disabled, RIP will stop redistribution of routes but will continue to send updates to the RTM.

redistribute

```
redistribute {all | connected | ospf | static} [route-map <string (1-20)>]
```

no redistribute

```
no redistribute {all | connected | ospf} [route-map <string (1-20)>]
```

Parameters

Parameter	Type	Description
`all`		Enter to specify that all routes have to be imported from the RIP. It redistributes all routes that are learnt into RIP process.
`connected`		Enter to configure redistribution of directly connected networks routes into OSPF routing process.
`ospf`		Enter to import routes learnt in the OSPF routing process.
`static`		Enter to import static routes.
`route-map`		Enter to identify the specified route-map in the list of route-maps. **NOTE:** Redistribution can be configured for only one route map. Another route map can be assigned, only if the already assigned route map is disabled.
`<string(1-20)>`		Enter a name for a route map. This is a string with maximum size of 20.

Mode

RIP Router Configuration Mode

Default

By default, route redistribution is disabled.

Examples

Example 1

iS5comm(config)# router rip

iS5comm(config-router)# redistribute all

Example 2

iS5comm(config)# router rip

iS5comm(config-router)# redistribute ospf

iS5comm(config-router)# redistribute connected

NOTE: the **redistribute connected** command is required when we want to redistribute OSPF to RIP.

To redistribute OSPF to RIP, we need to redistribute the connected networks. To filter the connected networks to allow only the required ones, perform the following commands:

iS5comm(config)# router rip

iS5comm(config-router)# redistribute ospf

iS5comm(config-router)# redistribute connected route-map FILTER

Example 3: redistribute default route

SW1:

iS5comm(config)# ip route 0.0.0.0 0.0.0.0 192.168.10.100

iS5comm(config)# router rip

iS5comm(config-router)# redistribute static

iS5comm(config)# interface gigabitethernet 0/1

iS5comm(config-if)# ip rip default route install

iS5comm(config-if)# ip rip default route originate 1

SW2:

iS5comm(config)# interface gigabitethernet 0/1

iS5comm(config-if)# ip rip default route install

iS5comm(config-if)# ip rip default route originate 1

iS5comm# show ip route

```
Vrf Name:           default
---------
R 0.0.0.0/0  [121/2] via 192.168.10.100
```

25.15. rip

To set the flag to decide whether the last authentication key on expiry should have its lifetime as infinite or not, use the command **rip** in Global Configuration Mode.

rip

```
rip authentication last-key infinite lifetime {true | false}
```

Parameters

Parameter	Type	Description
`authentication`		Enter to configure if the last authentication key on expiry should have its lifetime to be infinite or not.
`last-key`		Enter to configure if the last authentication key,
`infinite`		Enter to configure the last authentication key lifetime to infinite.
`lifetime`		Enter to set the last authentication key lifetime not to be infinite.
`true`		Enter to set the lifetime of last key to be infinite. The last key on expiry resets its lifetime to be infinite and continues to be the key until a new authentication key id is configured.
`false`		Enter to set the lifetime of last key not to be infinite. After the last key expires, the received RIP updates will be dropped and the routes may tear down. No updates will be sent on that interface.

Mode

Global Configuration Mode

Default

true

Examples

iS5comm(config)# rip authentication last-key infinite lifetime true

25.16. router rip

To enable RIP and enter the Router Configuration mode, use the command **router rip** in Global Configuration Mode. The no form of the command disables RIP.

router rip

```
router rip
```

no router rip

```
no router rip
```

Mode

Global Configuration Mode

Default

Router rip is disabled.

Examples

iS5comm(config)# router rip

iS5comm (config-router)#

25.17. show ip rip

To display the IP RIP database, statistics, authentication, use the **show ip rip** command in Privileged EXEC Mode.

show ip rip

```
show ip rip {database [<ip-address> <ip-mask>] | statistics | authentica-
tion}
```

Parameters

Parameter	Type	Description
database		Enter for display the RIP protocol database details for all RIP interface entry or for entry with the specified IP address and IP mask.
<ip-address>		Enter to specify an IP address to be displayed.
<ip-mask>		Enter to specify an IP mask to be displayed.
statistics		Enter to display the RIP statistics on the router.
authentication		Enter to display the authentication related information configured for the RIP Interface entry. The authentication information includes the Authentication type, authentication key IDs configured & its associated lifetime values.

Mode

Privileged EXEC Mode

Examples

iS5comm # show ip rip database

```
12.0.0.0/8  [1]        auto-summary
12.0.0.0/8  [1]        directly connected, vlan1
15.0.0.0/8  [3]        auto-summary
15.0.0.0/8  [3]        directly connected, vlan2
20.0.0.0/8  [4]        auto-summary
20.0.0.0/8  [4]        via 12.0.0.2, vlan1
12.0.0.0/8  [1]        auto-summary
12.0.0.0/8  [1]        directly connected, vlan2
```

iS5comm # show ip rip statistics

```
RIP Global Statistics:
----------------------
 Total number of route changes is 1
 Total number of queries responded is 1
 Total number of dropped packets is 0
RIP Interface Statistics:
-------------------------
Interface Periodic  BadRoutes  Triggered  BadPackets Admin
IP Address Updates Sent Received Updates Sent Received Status
---------- ---------- -------- ------------ -------- -
12.0.0.1       19          1         2         0  Enabled
```

iS5comm# show ip rip authenticatio

```
RIP Interface Authentication Statistics:
----------------------------------------
Interface Name                   vlan1
Authentication Type              3
Authentication KeyId in use:     0
Authentication Last key status:  false
RIP Authentication Key Info:
----------------------------
Authentication KeyId        0
Start Accept Time           2013-06-03,17:00:00
Start Generate Time         2013-06-03,17:00:00
Stop Generate Time          2013-06-03,17:00:00
Stop Accept Time            2013-06-03,17:00:00

RIP Authentication Key Info:
----------------------------
```

```
Authentication KeyId        1
Start Accept Time           2013-06-03,16:35:00
Start Generate Time         2013-06-03,16:35:00
Stop Generate Time          2136-02-06,06:28:15
Stop Accept Time            2136-02-06,06:28:15
```

25.18. timers basic

To configures update, route age and garbage collection timers for the VLAN interface / router port, use the command **timers basic** in Interface Configuration Mode.

timers basic

```
timers basic <update-interval (10-3600)> <invalid(30-500)> <holddown
(10-3600)> <flush(120-180)> <sleep(10-3600)>
```

Parameters

Parameter	Type	Description
<update-interval(10-3600)>	Integer	Enter a value to configure the time interval (in seconds) at which the RIP updates should be sent. This is the fundamental timing parameter of the routing protocol. This value ranges from 10 to 3600 seconds.
<invalid(30-500)>	Integer	Enter a value to configure the time (in seconds) after which the route entry is put into garbage collect (that is, marked as invalid). This value ranges from 30 to 500 seconds.
<holddown (10-3600)>	Integer	Enter a value to configure the time (in seconds) during which the routing information regarding better paths is suppressed. This value ranges from 10 to 3600 seconds.
<flush(120-180)>	Integer	Enter a value to configure the time (in seconds) after which the route entry marked as invalid is deleted. The advertisements of this entry is set to INFINITY while sending to others. This value ranges from 120 to 180 seconds.
<sleep(10-3600)>	Integer	Enter a value to configure the time interval (in milliseconds) for postponing routing updates in the event of a flash update. This value ranges from 10 to 3600 milliseconds.

Mode

Interface Configuration Mode

Default

- update-value - 30
- invalid-value - 180
- flush-value - 120

Examples

iS5comm(config-if)# timers basic 360 300 130 3000 125 3000

25.19. version

To set the global version of RIP, use the command **version** in RIP Router Configuration Mode. The command is used in conjunction with the redistribute router command to cause the current routing protocol to use the same metric value for all redistributed routes. The no form of the command sets the RIP global version to its default value. This command is a complete standardized implementation of the existing commands and operates similarly to that of the commands ip rip send version and ip rip receive version.

version

```
version {1 [2] |2 [1] | none}
```

no version

```
no version
```

Parameters

Parameter	Type	Description
1		Enter to set the global version of RIP as 1. This implies that RIP updates are sent/ received in compliance with RFC 1058.
2		Enter to set the global version of RIP as 2. This implies that only multicasting RIP updates are sent/received.
none		Enter to configure that no RIP update is to be received.

Mode

RIP Router Configuration Mode

Default

1 and 2

Prerequisites

Only the configurations that are done after associating the IP address of the VLAN interface / router port with the RIP routing process are applied to the RIP.

Examples

iS5comm(config)# router rip

iS5comm(config-router)# version 1

BGP

26. BGP (Beta Version)

***BGP* (Border Gateway Protocol)** is used to build an *AS* connectivity graph that is used to prune routing loops and enforce policies at *AS* level.

The following sections outline all BGP-related CLI commands.

26.1. address-family

To facilitate entering of the router in the Address-family Router Configuration Mode and to enable configuration of the session that carries standard vpnv4 address prefixes and enters into VPN Address Family Configuration Mode, use the command **address-family** in *BGP* Router Configuration Mode. Routing information is advertised for IPv4 address family when a BGP session is configured, unless the default advertising is reset. The no form of the command deletes the peers belonging to the IPv4, IPv6 and VPNv4 address family.

address-family

```
address-family [ipv4 | ipv6 |l2vpn] | vpnv4
```

no address-family

```
no address-family [ipv4 | ipv6 |l2vpn] | vpnv4
```

Parameters

Parameter	Type	Description
ipv4		Enter to configure a session that carries standard IPv4 address prefixes.
ipv6		Enter to configure a session that carries standard IPv6 address prefixes.
l2vpn		Enter to configure a session that carries L2VPN VPLS address prefixes.
vpnv4		Enter to enable configuration of the session that carries standard vpnv4 address prefixes and enters into VPN Address Family Configuration Mode.

Mode

BGP Router Configuration Mode

Notes

BGP4 VPN allows the Service Providers to use their IP backbone to provide VPN services to their customers. BGP is used to distribute VPN routing information across the provider's backbone and MPLS is used to forward VPN traffic from one VPN site to another.

Examples

iS5comm (config-router)# address-family ipv4

iS5comm(config-router-af4)#

iS5comm (config-router)# address-family vpnv4

iS5comm(config-router-afvpnv4)#

26.2. aggregate-address

To create an aggregate entry in a *BGP* or multiprotocol *BGP* routing table if any more-specific *BGP* or multiprotocol *BGP* routes are available that fall in the specified range, use the command **aggregate-address** in *BGP* Router Configuration Mode. The entries in the table specifies the IP address based on which the routing information has to be aggregated. The aggregate route will be advertised as coming from autonomous system. The atomic aggregate attribute will be set only if some of the information in the AS PATH is missing in the aggregated route, else it will not be set.The no form of the command deletes the specified entry from the aggregate table.

aggregate-address

```
aggregate-address index <1-100> <ip-address> <prefixlen> [summary-only]
[as-set] [suppress-map map-name] [advertise-map map-name] [attribute-map
map-name]
```

no aggregate-address

```
no aggregate-address index <1-100>
```

Parameters

Parameter	Type	Description
index		Enter to configure the entry containing information about the IP address on which the aggregation has to be done..
<1-100>	Integer	Enter a value for the entry containing information about the IP address on which the aggregation has to be done
<ip-address>		Enter to configure the route prefix in the Network Layer Reachability Information on which aggregate policy needs to be applied.
<prefixlen>		Enter to configure the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges from 0 to 32 for IPv4 address and between 0 and 128 for IPv6 Address.
[summary-only]		Enter to specify that aggregated (summarized) route alone will be sent to the peers. If this is not specified , both the summary and the more-specific routes based on which the summary entry was generated are be advertised to the peers
[as-set]		Enter to generate autonomous system set path information.
[suppress-map map-name]		Enter to specify the name of the route map used to select the routes to be suppressed. The route map contains the rules for suppressing the more-specific routes in forming the aggregate route. When suppress-map configuration is used along with summary only option, summary-only configuration command doesn't have any effect. And the more-specific routes that the suppress-map suppresses are not advertised. Other routes are advertised in addition to the aggregated route. This value is a string with a maximum length of 20.
[advertise-map map-name]	Integer	Enter to specify the name of the route map used to select for forming aggregate routes. The route map contains the rules for selecting specific routes for aggregation Other routes are advertised. When advertise-map is used, only advertise-map influences the creation of aggregate entry. In absence of advertise-map, the aggregate route inherits the attributes of the more specific routes, both suppressed and unsuppressed.This value is a string with a maximum length of 20.

Parameter	Type	Description
[attribute-map map-name]		Enter to specify the name of the route map used to form the attribute of the aggregate route. The route map contains the rules for setting the attributes for the aggregated route. When attribute-map and advertise-map along with autonomous system set path information are enabled and other configurations, the attribute-map overrides the attribute that is formed with the routes selected by the advertise-map.. This value is a string with a maximum length of 200

Mode

BGP Router Configuration Mode

Notes

The IP address and the prefix length can be configured, only if the Aggregate admin status of the BGP is down.

Examples

iS5comm(config-router)# aggregate-address index 1 21.1.0.0 16 summary-only

26.3. bgp

For *BGP*-related configuration, use the command **bgp** in *BGP* Router Configuration Mode. For options, see the Parameters section below.

bgp

```
bgp
 {always-compare-med
 | asnotation dot
 | bestpath med dot
 | client-to-client reflection
 | cluster-id <cluster id value> <ip_addr(A.B.C.D)>
 | comm-filter <comm-value(4294967041-4294967043,65536-4294901759)> <permit
| deny> <in | out>
 | comm-policy <ip-address> <prefixlen> <set-add | set-none | modify>
```

```
 | comm-route {additive | delete} <ip-address> <prefixlen> comm-value
<4294967041-4294967043,65536-4294901759>

 | confederation {identifier <AS no> | peers <AS no>}

 | dampening <HalfLife-Time(600-2700)> <Reuse-Value(100-10800)>
<Suppress-Value(2000-3999)> <Max-Suppress-Time(1800-10800)>

 | default {ipv4-unicast | local-preference <Local Pref Value
(0-2147483647)>}

 | ecomm-filter <ecomm-value(xx:xx:xx:xx:xx:xx:xx:xx)> <permit | deny> <in |
out>

 | ecomm-policy <ip-address> <prefixlen> <set-add | set-none | modify>

 | ecomm-route {additive | delete} <ip-address> <prefixlen> ecomm-value
<value(xx:xx:xx:xx:xx:xx:xx:xx)>

 | graceful-restart [restart-time <(1-4096)<seconds>] [stalepath-time
<(90-3600)<seconds>]

 | local-preference <1-100> remote-as <AS no> <ip-address | ip6-address>
<prefixlen> [intermediate-as <AS-no list- AS1,AS2,...AS10>] value <value>
direction {in | out} [override]

 | med <1-100> remote-as <AS no> <ip-address> <prefixlen> [intermediate-as
<AS-no list- AS1,AS2,...AS10>] value <value> direction {in | out} [override]

 | nonbgproute-advt <external |both>

 | redistribute-internal

 | router-id A.B.C.D(<ucast_addr>)

 | trap <external |both>

 | update-delay <(60-1800)seconds>

 | update-filter <1-100> <permit | deny> remote-as <AS no> <ip-address>
<prefixlen> [intermediate-as <AS-no list- AS1,AS2,...AS10>] direction {in |
out}
```

no bgp

```
no bgp

 {always-compare-med

 | asnotation dot

 | client-to-client reflection | cluster-id <cluster id value>
<ip_addr(A.B.C.D)>

 | comm-filter <comm-value(4294967041-4294967043,65536-4294901759)> <permit
| deny> <in | out>

 | comm-policy <ip-address> <prefixlen>
```

```
 | comm-route {additive | delete} <ip-address> <prefixlen> comm-value
<4294967041-4294967043,65536-4294901759>

 | confederation {identifier | peers <AS no>}

 | dampening

 | default {ipv4-unicast | local-preference

 | ecomm-filter <ecomm-value(xx:xx:xx:xx:xx:xx:xx:xx)> <permit | deny> <in |
out>

 | ecomm-policy <ip-address> <prefixlen> | ecomm-route

 | graceful-restart [restart-time] [stalepath-time]

 | local-preference <1-100> | med <1-100> | nonbgproute-advt

 | redistribute-internal | router-id | update-delay

 | update-filter <1-100>
```

Parameters

Parameter	Type	Description
`always-compare-med`		Enter to enable the comparison of Multi Exit Discriminator (MED) for routes received from different AS. The MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED. The no form of the command disables the comparison of MED for routes received from different autonomous system. MED will be compared only for routes from same neighbor autonomous system
`asnotation dot`		Enter to change the output format of BGP ASNs (Autonomous System numbers) from asplain to asdot notation. The no form of the command resets the output format of BGP ASNs from asdot to asplain notation. By default, the output format of BGP ASNs is asplain. Note that BGP asnotation can be changed only if four-byte-ASN is enabled.
`bestpath med confed`		Enter to enable Multi Exit Discriminator (MED) comparison among paths learnt from confederation peers. The comparison between MEDs is only made if there are no external autonomous systems in the path. If there is an external autonomous system in the path, then the external MED is passed transparently through the confederation, and the comparison is not made. The no form of the command disables MED comparison among paths learnt from confed peers and prevent the software from considering the MED attribute in comparing paths. As default, in BGP route selection algorithm, MED attributes comparison between two routes originated within the local confederation is disabled.
`client-to-client reflection`		Enter to configure the Route Reflector to support route reflection to Client Peers. By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. If the clients are fully meshed, route reflection is not required. The no form of the command disables client-to-client reflection. If disabled, then Route Reflector will not advertise routes learnt from a client peer to other client peers. This occurs when all peers within a cluster are fully-meshed and the client peer itself is able to advertise routes to other clients of the route-reflector

Parameter	Type	Description
cluster-id		Enter to configure the Cluster ID for the Router Reflector of the BGP cluster which has more than one route reflector. Usually in a cluster of clients with single route reflector the cluster is identified by the router ID of the route reflector. In order to increase redundancy and avoid a single point of failure, a cluster might have more than one route reflector. In this case, all route reflectors in the cluster must be configured with the 4-byte cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster. The no form of the command resets the Cluster ID for the Route Reflector.
cluster id value		Enter a value for the Cluster ID. It ranges from 1 to 4294967295.
ip_address/integer		Enter a value for the Cluster ID.
comm-filter		Enter to allow/ filter the community attribute while receiving or advertising. The rules to filter out the updates are based on the AS from which it is received, NLRI and AS through which it had passed. The no form of the command removes the filter policy for the community attribute.
comm-value(4294967041-4294967043,65536-4294901759		Enter to configure the community attribute value.
deny		Enter to filter routes containing the community attribute value in received or advertised updates.
permit		Enter to allow a particular community attribute to be received or advertised in updates. This is the default option.
in		Enter to configure the direction of route-updates on which the community filter policy needs to be applied as in. This indicates that the community filter needs to be applied on received routes.
out		Enter to configure the direction of route-updates on which the community filter policy needs to be applied as out. This indicates that the community filter needs to be applied on routes advertised to peers.
comm-policy		Enter to configure the community attribute advertisement policy for specific destination. The no form of the command removes the community attribute advertisement policy for specific destination.
<ip-address>		Enter to configure the route prefix on which community policy needs to be applied.

Parameter	Type	Description
<prefixlen>		Enter to configure the IP prefix length for the destination. These bits are common among all hosts within a network. This value ranges from 1 to 32.
set-add		Enter to send only the configured additive communities with associated route.
set-none		Enter to send the associated route without any communities.
modify		Enter to remove the associated route with received delete communities and to add the configured additive communities.
comm-route		Enter to configure an entry in additive or delete community table for a given destination. The no form of the command removes the entry from additive or delete community table
additive		Enter to add an associated community value with the already existing communities in the route update.
delete		Enter to remove the community attribute from the route-prefix when it passes through the filter process.
<ip-address>		Enter to configure the Route prefix on which community policy needs to be applied.
<prefixlen>		Enter to configure the IP prefix length for the destination. These bits are common among all hosts within a network. This value ranges from 1 to 32.
comm-value <4294967041-4294967043,65536-4294901759>		Enter to configure the community attribute value. This value ranges from 4294967041 to 4294967043 or from 65536 to 4294901759.
confederation		Enter to configure the BGP confederation to which the AS belong to.

Parameter	Type	Description
`identifier <AS no>`		Enter to configure the BGP confederation identifier for the confederation to which the autonomous systems belong to. This value ranges from 1 to 4294967295 or 0.1 to 65535.65535. The no form of the command removes the configured BGP confederation identifier and resets the identifier to its default value. **NOTE:** If this value is already configured to a non-zero value, it must be reset to zero (using no form of the command) before reconfiguring. **NOTE:** When four-bit-asn is enabled, This value ranges from 1 to 4294967295or between 0.1 and 65535.65535. **NOTE:** When four-bit-asn is disabled, This value ranges from 1 to 65535. or between 0.1 and 0.65535 **NOTE:** When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.65535
`peers <AS no>`		Enter to configure the ASs that are visible internally to a confederation. Each autonomous system is fully meshed within itself. This value ranges from 1 to 4294967295 or 0.1 to 65535.65535. By default, no AS will be added to the confederation. The no form of the command removes the Autonomous Systems from the confederation. **NOTE:** When four-bit-asn is enabled, This value ranges from 1 to 4294967295or between 0.1 and 65535.65535. **NOTE:** When four-bit-asn is disabled, This value ranges from 1 to 65535. or between 0.1 and 0.65535 **NOTE:** When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.65535
`dampening`		Enter to enable the *BGP* dampening parameters. The no form of the command disables the *BGP* dampening feature but does not reset the other configured *RFD* parameters
`<HalfLife-Time (600-2700)>`		Enter to configure the time (in seconds) after which a penalty is decreased by half. Once a route has been assigned a penalty, the penalty is decreased for every 5 seconds. BGP's route flap damping algorithm calculates penalty for each routes. This penalty increases by a fixed value when a flap occurs, and decreases exponentially when the route is stable. This value ranges from 600 to 270.

Parameter	Type	Description
<Reuse Value (100-10800)>		Enter to configure the reuse value. If the penalty for a flapping route falls below this value, the route is re-used. The unsuppressing of routes occurs at 10-second increments. This value ranges from 100 to 10800. **NOTE:** Reuse value can be configured only if the HalfLife Time value is set.
<Suppress Value (2000-3999)>		Enter to configure the suppress value. The route is suppressed if the penalty associated with the route exceeds this value. This value ranges from 2000 to 3999. **NOTE:** Suppress value can be configured only if the HalfLife Time and Reuse value are set.
<Max-Suppress Time (1800-10800)		Enter to configure the maximum time (in seconds) a route can be suppressed. This value ranges from 1800 to 10800. **NOTE:** Max-Suppress Time can be configured only if the HalfLife Time, Reuse Value and Suppress Value are set.
default		Enter for BGP default information configuration.
ipv4-unicast		Enter for IPv4 unicast feature configuration for default routing.
local-preference		Enter to configure the default local preference value that is to be sent in updates to internal peers. The preference is sent to all routers and access servers in the local autonomous system. The no form of the command resets the default local preference to its default value.
<Local Pref Value>		Enter a default local preference value that is to be sent in updates to internal peers. This value ranges from 0 to 2147483647.
ecomm-filter		Enter to allow/ filter the extended community attribute while receiving or advertising. The no form of the command removes the filter policy for the extended community attribute.
<ecomm-value(xx:xx:xx:xx:xx:xx:xx:xx)>		Enter to configure the extended community value. This is an octet string value in the form xx:xx:xx:xx:xx:xx:xx:xx.
deny		Enter to deny the route-update with the associated extended community value to pass the filter test. This is the default option.
permit		Enter to allow the route -update with the associated extended community value to pass the filter test.
in		Enter to configure the incoming direction of applied filter.
out		Enter to configure the outgoing direction of applied filter.

Parameter	Type	Description
ecomm-policy		Enter to configure the Estendedcommunity attribute advertisement policy for specific destination. The no form of the command removes the community attribute advertisement policy for specific destination.
<ip-address>		Enter to configure the route prefix on which extended community policy needs to be applied.
<prefixlen>		Enter to configure the IP prefix length for the destination. These bits are common among all hosts within a network. This value ranges from 1 to 32.
set-add		Enter to send only the configured additive extended communities with associated route.
set-none		Enter to send the associated route without any extended communities.
modify		Enter to remove the associated route with received delete communities and to add the configured additive extended communities.
ecomm-route		Enter to configure an entry in additive or delete extended community table for a given destination. The no form of the command removes the entry from additive or delete community table.
additive		Enter to add an associated community value with the already existing communities in the route update.
delete		Enter to remove the community attribute from the route-prefix when it passes through the filter process.
<ip-address>		Enter to configure the Route prefix on which community policy needs to be applied.
<prefixlen>		Enter to configure the IP prefix length for the destination. These bits are common among all hosts within a network. This value ranges from 1 to 32.
comm-value <value(xx:xx:xx:xx:xx:xx:xx:xx)>		Enter to configure the community attribute value. This value ranges from 4294967041 to 4294967043 or from 65536 to 4294901759.

Parameter	Type	Description
graceful-restart		Enter to enable graceful restart capability in router which allows forwarding of data packets to continue along known routes, while the routing protocol information is being restored following a processor switch over. When graceful restart is enabled, peer networking devices are informed, through protocol extensions prior to the event. The no form of the command disables the graceful restart capability and resets the restart-time or stalepath-time to the default value
restart-time		Enter to configure the estimated time (in seconds) taken for re-establishing a BGP session after restart. The default value for this should be less than or equal to Hold Time carried in open message.
<(1-4096)<seconds>>		Enter a value for the restart time—it ranges from 1 to 4096 seconds.
stalepath-time		Enter to configure the time (in seconds) until which the router retains the stale routes.
<(90-3600)<seconds>>		Enter a value for the stalepath time—it ranges from 90 to 3600 seconds.
local-preference		Enter to configure an entry in the local preference table. This table contains the value that is to be assigned to the local preference attribute. The defaults are as follows: • remote-as - 0 • direction - in • value - 100 • ip-address - 0.0.0.0 • prefixlen - 0
<1-100>		Enter a value for the local preference index—it ranges from from 1 to 100.

Parameter	Type	Description
remote-as <AS no>		Enter to configure the remote Autonomous system number for which the local preference is associated. This value ranges from 1 to 4294967295 or 0.1 to 65535.65535. The no form of the command removes the configured BGP confederation identifier and resets the identifier to its default value. **NOTE:** When four-bit-asn is enabled, This value ranges from 1 to 4294967295or between 0.1 and 65535.65535. **NOTE:** When four-bit-asn is disabled, This value ranges from 1 to 65535. or between 0.1 and 0.65535 **NOTE:** When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.6553. A value of zero indicates that this entry is not valid and will not be matched for when the Local Pref value for an update is calculated
<ip-address>		Enter to configure the route prefix in the Network Layer Reachability Information on which local-preference policy needs to be applied. The input route ip address can be an ipv4 or an ipv6 address.
<prefixlen>		Enter to configure the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges from 0 to 32 for ipv4 address and 0 to 128 for ipv6 address.A value of zero indicates that the entry is not valid and will not be matched for when the Local Pref value for an update is calculated.
intermediate-as<AS-no list-AS1,AS2,...>		Enter to configure the sequence of intermediate AS numbers through which the route update is expected to travel or a Comma separated list of AS numbers that are to be checked against the AS_PATH attribute of the updates. This value is a list with the maximum size as 100.
value <value>		Enter to configure the local-preference value that needs to be associated with the route-update. This value ranges from 0 to 2147483647.
direction		Enter to specify the direction of the application of local-preference policy with which the entry is to be associated.
in		Enter to indicate a received route-update with other matching attributes such as as-number, intermediate-as numbers.
out		Enter to indicate a route-update that needs to be advertised to peer.
override		Enter to configure an entry in the local preference table. This table contains the value that is to be assigned to the local preference attribute.

Parameter	Type	Description
med		Enter to configure an entry in BGP4 MED Table and contains the MED values that are to be assigned to routes. The no form of the command deletes the entry from MED Table, BGP4 MED table. The entry will not be matched when the MED value for an update is calculated, if the prefix length is set as zero.The defaults are as follows: • remote-as - 0 • prefixlen - 0 • direction - in • value - 0
<1-100>		Enter a value for the entry containing information about the MED value—it ranges from1 to 100.
remote-as <AS no>		Enter to configure the remote Autonomous system number that identifies the BGP router to other routers and tags the routing information passed along. This value ranges from 1 to 4294967295 or 0.1 to 65535.65535. The no form of the command removes the configured BGP confederation identifier and resets the identifier to its default value. **NOTE:** When four-bit-asn is enabled, This value ranges from 1 to 4294967295or between 0.1 and 65535.65535. **NOTE:** When four-bit-asn is disabled, This value ranges from 1 to 65535. or between 0.1 and 0.65535 **NOTE:** When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.6553. A value of zero indicates that this entry is not valid and will not be matched for when the Local Pref value for an update is calculated
<ip-address>		Enter to configure the route-prefix IPv4 and IPv6 on which MED policy needs to be applied.
<prefixlen>		Enter to configure the number of high-order bits in the IP address. This is the length of the IP address prefix in the Network Layer Reachability Information (NLRI) field. These bits are common among all hosts within a network. This value ranges from 0 to 32 for ipv4 address and 0 to 128 for ipv6 address. A value of zero indicates that this entry is not valid and will not Be matched for when the MED value for an update is calculated.

Parameter	Type	Description
intermediate-as<AS-no list-AS1,AS2,...>		Enter to configure the sequence of intermediate AS numbers through which the route update is expected to travel or a Comma separated list of AS numbers that are to be checked against the AS_PATH attribute of the updates. This value is a list with the maximum size as 100.
value <value>		Enter to configure the value assigned to the MED attribute for the route present in NLRI. This value ranges from 0 to 2147483647.
direction		Enter to specify the direction of application of MED policy.
in		Enter to indicate a received route-update with other matching attributes such as as-number, intermediate-as numbers.
out		Enter to indicate a route-update that needs to be advertised to peer.
override		Enter to decide whether the configured MED value will override the received MED value.
nonbgproute-advt		Enter to configure the peer type to whom non-bgp routes can be propagated and controls the advertisement of Non-BGP routes either to the external peer or both to internal and external peer. The no form of the command resets the Non BGP routes advertisement policy to its default value. The Administrator can effectively control the advertisement of the route learnt through Redistribution
external		Enter to indicate that the non-BGP routes can be exported only to external peers. All types of non-bgp routes can be propagated to external peers.
both		Enter to indicate that the non-BGP routes can be propagated to both internal and external peers. This is the default option.
redistribute-internal		Enter to enable IBGP routes to be redistributed to other IGP protocols. The no form of the command disables IBGP routes to be redistributed to other IGP protocols. By default, IBGP route redistribution is disabled.

Parameter	Type	Description
router-id		Enter to configure fixed BGP router identifier for a BGP-speaking router. If loopback interface exists, the router ID is set to the highest address for loopback interface otherwise it is set to the highest ip configured on the ip interfaces. Peering sessions will be reset if the router ID is changed. BGP router id is a unique number associated with the BGP speaker. This router-id is advertised to other peers and identifies the BGP speaker uniquely. Administrator can set the router-id of BGP to any value. If router-id is changed, then all active peer sessions will go DOWN and will be re-started with the new configured router-id. The no form of the command resets the BGP Identifier of the BGP Speaker to its default value.
A.B.C.D (<ucast_addr>)		Enter an unicast IP address representing BGP identifier. As default, The highest interface address is used as the router id
trap		Enter to enable or disable the BGP trap notification.
enable		Enter to enable the trap notification for the BGP system. When there is any change in the graceful restart state of the router or peer, the BGP system sends the notification messages to the SNMP manager. For every graceful restart, appropriate trace messages is generated. This is the default option.
disable		Enter to disable the trap notification for the BGP system and not send the notification messages to the SNMP manager.
update-delay		Enter to configure the selection deferral time interval. This time interval represents the time (in seconds) until which the router defers its route selection. This time interval should be configured to provide enough time for all peers of the restarting speaker to send all routes to the restarting speaker. The no form of the command resets the time interval to its default value.
<(60-1800)seconds>		Enter a value for the deferral time interval. This value ranges from 60 to 1800 seconds with a default of 60 seconds.
update-filter		Enter to configure an entry in Update Filter Table which contains rules to filter out updates based on the AS from which it is received, Network Layer Reachability Information (NLRI) and AS through which it had passed. The no form of the command deletes the entry from Update Filter Table.The defaults are as follows: • remote-as - 0 • direction - in • ip-address - 0.0.0.0 • prefixlen - 0

Parameter	Type	Description
<1-100>		Enter a value for the entry containing information about the updates that are to be filtered—it ranges from 1 to 100.
deny		Enter to filter the routes when passing through filter policy test.
permit		Enter to allow the route to pass filter policy test.
remote-as <AS no>		Enter to configure the remote Autonomous system numberthat identifies the BGP router to other routers and tags the routing information passed along. This value ranges from 1 to 4294967295 or 0.1 to 65535.65535. The no form of the command removes the configured BGP confederation identifier and resets the identifier to its default value. **NOTE:** When four-bit-asn is enabled, This value ranges from 1 to 4294967295or between 0.1 and 65535.65535. **NOTE:** When four-bit-asn is disabled, This value ranges from 1 to 65535. or between 0.1 and 0.65535 **NOTE:** When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.6553. A value of zero indicates that this entry is not valid and will not be matched for when the Local Pref value for an update is calculated
<ip-address>		Enter to configure the route prefix IPv4 and IPv6 in the Network Layer Reachability Information on which the filter policy needs to be applied.
<prefixlen>		Enter to configure the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges from 0 to 32.
intermediate-as<AS-no list-AS1,AS2,...>		Enter to configure the sequence of intermediate AS numbers through which the route update is expected to travel or a Comma separated list of AS numbers that are to be checked against the AS_PATH attribute of the updates. This value is a list with the maximum size as 100.
direction		Enter to specify the direction of the application of filters with which the entry is to be associated.
in		Enter to indicate a received route-update with other matching attributes such as as-number, intermediate-as numbers.
out		Enter to indicate a route-update that needs to be advertised to a peer.

Mode

BGP Router Configuration Mode

Examples

iS5comm (config-router)# always-compare-med

iS5comm (config-router)# bgp asnotation dot

iS5comm (config-router)# bgp client-to-client reflection

iS5comm (config-router)# bgp bestpath med confed

iS5comm (config-router)# bgp cluster-id 10.0.0.1

iS5comm (config-router)# bgp comm-filter 75100 deny in

iS5comm (config-router)# bgp comm-policy 24.5.0.0 10 set-none

iS5comm (config-router)# bgp comm-route additive 24.5.0.0 16 comm-value 429490

iS5comm (config-router)# bgp confederation identifier 1000

iS5comm (config-router)# bgp confederation peers 100

iS5comm (config-router)# bgp dampening 1000 300 2000 5000

iS5comm (config-router)# bgp ecomm-filter 01:01:22:33:23:43:44:22 deny in

iS5comm (config-router)# bgp comm-policy 24.5.0.0 10 set-none

iS5comm (config-router)# bgp ecomm-route additive 12.0.0.0 2 ecomm-value 01:01:22:33:44:55:66:77

iS5comm (config-router)# bgp graceful-restart restart-time 33 stalepath 789

iS5comm (config-router)# bgp local-preference 5 remote-as 200 21.3.0.0 16 intermediate-as 150 value 250 direction out override

iS5comm (config-router)# bgp med 5 remote-as 200 212.23.45.0 24 intermediate-as 150 value 50 direction in override

iS5comm (config-router)# bgp nonbgproute-advt both

iS5comm (config-router)# bgp redistribute-internal

iS5comm (config-router)# bgp router-id 10.0.0.1

iS5comm (config-router)# bgp trap enable

iS5comm (config-router)# bgp update-delay 90

iS5comm (config-router)# bgp update-filter 6 deny remote-as 145 72.93.0.0 14 intermediate-as 150 direction in

26.4. clear bgp ipv6

To dynamically reset the BGPv6 connection for inbound / outbound route policy, use the command **clear bgp ipv6** in Privileged EXEC Mode. If the keyword soft and the associated direction are not specified, then this causes hard clear, that is, the BGP session with peer is reset.

clear ip bgp

```
clear ip bgp
 <* | ipv6-address> [soft [in [prefix-filter] | out]
```

Parameters

Parameter	Type	Description
*		Enter to configure all BGP peers.
ipv6-address		Enter to configure the remote IP address which is associated with specific BGP peer
soft		Enter to configure the Soft rest; that is, the BGP session with peer is not reset).
in		Enter to perform a dynamic soft inbound reset.
prefix-filter		Enter to push out prefix-list ORF and initiate inbound soft reconfiguration.
out		Enter to perform a dynamic soft outbound reset.

Mode

Privileged EXEC Mode

Examples

iS5comm# clear bgp ipv6 1111::2222

26.5. clear ip bgp

To clear the BGP inbound and outbound route policy, use the command **clear ip bgp** in Privileged EXEC Mode. The inbound routing tables are updated dynamically or by generating new updates using stored update information. If the keyword soft and the associated direction are not specified, then this causes hard clear, that is, the BGP session with peer is reset.

clear ip bgp

```
clear ip bgp
 {dampening [<random_str> <num_str>] | flap-statistics [<random_str>
<num_str>] | {* | <AS no> | external | ipv4 | ipv6| <random_str> } [soft
[{in [prefix-filter] |out}]]}
```

Parameters

Parameter	Type	Description
dampening		Enter to clear the dampening related configuration for the BGP.
<random_str>		Enter to clear the dampening information for the specified ipv4/ipv6 address.
<num_str>		Enter to specify the prefix length of the route. This value ranges from 0 to 128.
*		Enter to reset all BGP peers.
<AS no>		Enter to clear peers with the specified AS number. This value ranges from 1 to 4294967295 or 0.1 to 65535.65535. **NOTE:** When four-bit-asn is enabled, This value ranges from 1 to 4294967295 or between 0.1 and 65535.65535 **NOTE:** When four-bit-asn is disabled, This value ranges from 1 to 65535 or between 0.0 and 0.65535 **NOTE:** When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.65535.
external		Enter to clear all external peers.
ipv4		Enter to reset the bgp connection dynamically for all ipv4 address family peers.
ipv6		Enter to reset the bgp connection dynamically for all ipv6 address family peers
soft		Enter to configure the Soft clear which is automatically assumed when the route refresh capability is supported
in		Enter to initiate inbound soft reconfiguration which causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy
prefix-filter		Enter to push out prefix-list ORF and initiates inbound soft reconfiguration.
out		Enter to initiate outbound soft configuration which does not have any memory overhead and does not require any preconfiguration. An outbound reconfiguration can be triggered on the other side of the BGP session to make the new inbound policy take effect.

Mode

Privileged EXEC Mode

Examples

iS5comm# clear ip bgp dampening 12.0.0.1 0

26.6. debug ip bgp

To enable the tracing of the BGP module as per the configured debug levels, use the command **debug ip bgp** in Privileged EXEC Mode. The trace statements are generated for the configured trace levels. The no form of the command disables the tracing of the BGP module as per the configured debug levels. The trace statements are not generated for the configured trace levels. The no form of the command disables the tracing of the BGP module as per the configured debug levels. The trace statements are not generated for the configured trace levels.

debug ip bgp

```
debug ip bgp
 [{peer | update | fdb | keep [prefix-filter] | in | out | damp | events |
gr | vpls}] [{all |ipv4 unicast |ipv6 unicast | <random_str>}]
```

no debug ip bgp

```
no debug ip bgp
 [peer | update | fdb | keep [prefix-filter] | in | out | damp | events | gr
| vpls | all]
```

Parameters

Enter a parameter to generate a debug statement for the trace code related to the specified parameter.

Mode

Privileged EXEC Mode

Examples

iS5comm# debug ip bgp peer

26.7. default-information

To enable and control redistribution of default routes of a protocol or network into the *BGP* and advertisement of the default route (0.0.0.0/0), use the command **default-information** in Global Configuration Mode. The default route advertisement is possible only if the default route is present in the IP FDB or it is received from any peers. The no form of the command disables redistribution and advertisement of the default route. The default routes are not redistributed into BGP.

default-information

```
default-information originate
```

no default-information

```
no default-information originate
```

Parameters

Parameter	Type	Description
originate		Enter to enable and control redistribution of default routes of a protocol or network into the BGP and advertisement of the default route (0.0.0.0/0.

Mode

Global Configuration Mode

Default

Default Information Originate is disabled.

Examples

iS5comm(config)# default-information originate

26.8. default-metric

To configure the default IGP metric value for routes redistributed into BGP with the redistribute command, use the command **default-metric** in *BGP* Router Configuration Mode. A default metric can be configured to solve the problem of redistributing routes with incompatible metrics. Assigning the default metric will allow redistribution to occur. The no form of the command resets the Default IGP Metric value to its default value 0. If configured to 0, the metric received from the IGP route will be used. If configured to any other value, the MED value of the redistributed routes take this value. This value has no effect on the Direct routes.

default-metric

```
default-metric <Default Metric Value(1-2147483647)>
```

no default-metric

```
no default-metric
 <Default Metric Value(1-2147483647)>
```

Parameters

Parameter	Type	Description
<Default Metric Value(1-2147483647)	integEr	Enter a value for the default IGP metric value. This value ranges from 1 to 2147483647.

Mode

BGP Router Configuration Mode

Default

0

Examples

iS5comm(config-router)# default-metric 300

26.9. distance

To configure the administrative distance value which is used as a preference parameter in IP for best route selection, use the command **distance** in *BGP* Router Configuration Mode. Distance can be set for only one route map. Another route map can be assigned, only if the already assigned route map is disabled. The no form of the command disables the administrative distance.

distance

```
distance <1-255> [route-map <name(1-20)>]
```

no distance

```
no distance [route-map <name(1-20)>]
```

If Routemap is disabled

```
distance <1-255>
```

```
no distance
```

Parameters

Parameter	Type	Description
<1-255>	Integer	Enter a value for the administrative distance—it ranges from 1 to 255.
route-map		Enter to configure the name of the route map for which the distance value should be enabled and set.
<name(1-20)>		Enter a name for the route map —a string with the maximum size as 20.

Mode

BGP Router Configuration Mode

Examples

iS5comm (config-router)# distance 10 route-map rmap-test

26.10. distribute-list

To enable route map filtering for inbound or outbound routes and define the conditions for distributing the routes from one routing protocol to another, use the command **distribute-list** in *BGP* Router Configuration Mode. Only one route map can be set for inbound or outbound routes. Another route map can be assigned, only if the already assigned route map is disabled. The no form of the command disables inbound filtering for the routes.

distribute-list

```
distribute-list route-map <name(1-20)> {in | out}
```

no distribute-list

```
no distribute-list
```

Parameters

Parameter	Type	Description
route-map		Enter to enable route map filtering for inbound or outbound routes.
<name(1-20>		Enter to specify the name of the route map to be used for filtering. This value is a string with the maximum size as 20.
in		Enter to set filtering for inbound routes.
out		Enter to set filtering for outbound routes.

Mode

BGP Router Configuration Mode

Examples

iS5comm (config-router)# distribute-list route-map rmap-test in

26.11. do shutdown ip bgp

To set the BGP Speaker Global Admin status down, use the command **do shutdown ip bgp** in Global Configuration Mode. The shutdown command does not affect all configurations. All peer sessions go down and routes learnt through redistribution are lost. If RFD is enabled, then routes history is cleared. The BGP Speaker Global Admin status can be made UP only if the BGP Speaker Local AS Number is configured. As default, the BGP Speaker Global Admin status is down. The no form of the command sets the BGP Speaker Global Admin status UP. BGP functionally is active only when the global admin status is UP

do shutdown ip bgp

```
do shutdown ip bgp
```

no shutdown ip bgp

```
no shutdown ip bgp
```

Mode

Global Configuration Mode

Examples

iS5comm# do shutdown ip bgp

26.12. ip bgp

To enable 4-byte *ASN* support in *BGP* speaker, configure the *BGP* speaker's policy for handling the overlapping routes, and enable synchronization between *BGP* and *IGP*, use the command **ip bgp** in Global Configuration Mode. The no form of the command disables 4-byte *ASN* support in *BGP*, resets Overlap route policy to its default values, and disables the synchronization between *BGP* and *IGP*.

ip bgp

```
ip bgp
 {four-byte-asn | overlap-policy {more-specific | less-specific |
less-specific |both} |synchronization}
```

no ip bgp

```
no ip bgp {four-byte-asn | overlap-policy |synchronization}
```

Parameters

Parameter	Type	Description
`four-byte-as`		Enter to enable 4-byte *ASN* support in *BGP* speaker. **NOTE:** This command executes only when *BGP* Speaker Global Admin status is shut down in the system.
`overlap-policy`		Enter to configure the configure the *BGP* speaker's policy for handling the overlapping routes. **NOTE:** This command executes only if *BGP* Speaker Local AS number is configured and BGP Administrative status is down.
`more-specific`		Enter to configure the overlap policy for *BGP* speaker as more-specific. This implies that when an overlapping route is received, more-specific routes are installed in the *RIB* tree.
`less-specific`		Enter to configure the overlap policy for *BGP* speaker as less-specific. This implies that when an overlapping route is received, less-specific routes are installed in the *RIB* tree.
`both`		Enter to configure the overlap policy for *BGP* speaker as both. This implies that when an overlapping route is received, both the more-specific and less-specific routes are installed in the *RIB* tree. This is default.
`synchronization`		Enter to enable synchronization between *BGP* and *IGP*. BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the *IGP*. This command allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems. **NOTE:** This command executes only if BGP Speaker local AS number is configured.

Mode

Global Configuration Mode

Default

4-byte ASN support —enabled

`overlap-policy`—both

Synchronization between *BGP* and *IGP* is disabled

Examples

iS5comm(config)# ip bgp four-byte-asn

iS5comm(config)# ip bgp overlap-policy more-specific

iS5comm(config)# ip bgp synchronization

26.13. label-allocation-mode

To configure the label allocation policy used for allocating the VPN label to be used for advertising the VPN routes, use the command **label-allocation-mode** in *BGP* Router Configuration Mode.

label-allocation-mode

```
label-allocation-mode {per-route}
```

Parameters

Parameter	Type	Description
per-route	Integer	Enter to configure label allocation policy as per route to advertise all routes learnt in the router with the unique label.

Mode

BGP Router Configuration Mode

Examples

iS5comm (config-router)# label-allocation-mode per-route

26.14. maximum-paths

To set the BGP multipath count, use the command **maximum-paths** in *BGP* Router Configuration Mode. This is the maximum number BGP multipath routes to be added per destination network in the routing table. Note that this configuration is effective only after hard/soft reset. The no form of the command resets the bgp multipath count to its default value.

maximum-paths

```
maximum-paths [{ibgp |eibgp}] <maximum path>
```

no maximum-paths

```
no maximum-paths [{ibgp |eibgp}]
```

Parameters

Parameter	Type	Description
ibgp	Integer	Enter to set the maximum number of internal bgp multipath routes to be added per destination network in the routing table.
eibgp		Enter to set the maximum number of external plus internal BGP multipath routes (with same AS PATH) to be added per destination network in Routing table.
<maximum path>		Enter to configure the maximum path count for the specified IBGP/ EIBGP. This value ranges from 1 to 64. **NOTE:** If this is set to 1, only the best route is added to the forwarding table **NOTE:** If the command is executed without the parameter ibgp/eibgp , the maximum path count is configured for ebgp.

Default

1

Note

If the no command is executed without the parameter ibgp/eibgp , the maximum path count is set to the default value 1 only for ebgp.

Mode

BGP Router Configuration Mode

Examples

iS5comm (config-router)# maximum-paths eibgp 1

iS5comm (config-router-af4)# maximum-paths ibgp 1

26.15. neighbor

To configure neighbor information, use the command **neighbor** in *BGP* Router Configuration Mode. The no form of the commands is also available for the most of the parameters.

neighbor

```
neighbor {<ip-address | ip6-address>
```

```
 gateway {<ip-address | ip6-address>
 | network-address {<ip-address | ip6-address>
 | password password-string
 | peer-group {<ip-address | ip6-address>
 | tcp-ao {mkt <Key ID (0-255)> | icmp-accept}
 | update-source {<ip-address | ip6-address>}
 | {<ip-address | ip6-address | peer-group-name>
 allow-autostop
 | as-override
 | capability {ipv4-unicast | ipv6-unicast |route-refresh |orf prefix-list
{send | receive | both}}
 | connect-retry-count <value(1-50)> | damp-peer-oscillations |
default-originate | delay-open
 | ebgp-multihop [ttl <(1-255)>]
 | fall-over bfd
 | local-as <AS no>
 | maximum-prefix <prefix-limit (1-2147483647)> | next-hop-self
 | remote-as <AS no> [allow-autostart [idlehold-time <seconds(1-65535)>]]
 | route-reflector-client
 | send-community {both | standard | extended}
 | shutdown
 | timers {keepalive <(1-21845) seconds> | holdtime <(3-65535)seconds>
|delayopentime <(0-65535)seconds>}
 | transport connection-mode <active | passive>
 | {route-map <name(1-20)> | prefix-list <ipprefixlist_name(1-20)>} {in |
out}
 | {advertisement-interval <seconds(1-65535)> | as-origination-interval
<seconds(1-65535)> | connect-retry-interval <seconds(1-65535)>}
 | hold-advertised-routes
 | peer-group
```

no neighbor

```
no neighbor
```

Parameters

Parameter	Type	Description
<ip-address>		Enter the BGP peer's IP address for which the configuration is performed.
<ip6-address>		Enter to configure the BGP peer's IPv6 address for which the configuration is performed.
gateway		Enter to configure gateway router’s address that will be used as nexthop in the routes advertised to the peer. This ensures that the traffic coming from this peer is routed through the gateway configured. The no form of the command resets the configured gateway router’s address. Note that this command executes only if Peer is created and Peer AS is configured
network-address		Enter to configure peer’s remote IPv6 network address for IPv4 peer and peer’s remote IPv4 network address for IPv6 peer. The peer’s network address carries the IPv6 network address if the peer’s remote-address is an IPv4 address. The peer’s network address carries the IPv4 network address if the peer’s remote-address is an IPv6 address.The no form of the command resets network-address configured for the peer. **NOTE:** This command executes only if Peer is created and Peer AS is configured. The peer’s remote network address can be configured only after configuring the peer’s remote address and the corresponding local interface
password		Enter to enables Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers where each segment sent on the TCP connection between the peers is verified. The MD5 authentication must be configured with the same password on both BGP peers; else, the connection between them will not be made.This command executes only if Peer is created. The no form of the command resets the TCP-MD5 password set for the peer. By default, the MD5 password setting is disabled.
password-string		Enter a TCP MD5 Authentication Password that has to be sent with all TCP packets originated from the peer. This value is a string with the maximum size as 80.
peer-group		Enter to create a peer group with the specified peer group name.
<peer-group-name>		Enter a peer group name - a string with the maximum size as 20.
tcp-ao		Enter for TCP-AO related configuration.

Parameter	Type	Description
mkt		Enter for configure the Key ID of the MKT which needs to be associated with the peer.
<Key Id(0-255)>		Enter a value for the Key ID of the MKT which needs to be associated with the peer. This value ranges from 0 to 255.
icmp-accept		Enter for action on ICMPv4 type 3 and ICMPv6 type 1 messages on this peer session.
update-source		Enter to configure the source-address for routing updates and allows BGP sessions to use any operational interface for TCP connection establishment with a peer. By default, the source address is set as 0.0.0.0, and the TCP fills the source address of the TCP session. The no form of the command disables configured source-address for routing updates and for TCP connection establishment with a peer.
allow-autostop		Enter to enable the auto stop option to stop the BGP peer and BGP connection automatically. This command executes only if Peer/ Peer Group is created and Peer AS is configured. By default, the Auto stop option is disabled. The no form of this command disables the auto stop option.
as-override		Enter to configure the override capability for a CE Peer. This command executes only if Peer/ Peer Group is created and Peer AS is configured. By default, the override capability is disabled. The no form of the command disables the override capability for the CE peer.
capability		Enter to enable the specific BGP capability to be advertised and received from the peer. The no form of the command disables the capability for the peer
ipv4-unicast		Enter to set the IPv4 unicast address family capability.
ipv6-unicast		Enter to set the MP IPv6 unicast address family capability.
route-refresh		Enter to set the Route refresh capability.
orf prefix-list		Enter to enable the address prefix-based Outbound Route Filter (ORF) for the specified BGP peer group.
send		Enter to enable ORF send capability.
receive		Enter to enable ORF receive capability.
both		Enter to enable both send and receive ORF Capability

Parameter	Type	Description
connect-retry-count		Enter to set the retry count for the BGP peer. This counter denotes the number of times the BGP Peer should try to establish a TCP-Connect issue with its neighboring peers. The default value for the counter is set as 5. If the BGP Peer exceeds the maximum count value, automatic stop event takes place and the BGP Peer is brought down to the Idle State.This command executes only if Peer / Peer Group is created and Peer AS is configured. The no form of the command resets the retry count of the BGP peer.
<value(1-50)>		Enter a value for retry count for the BGP peer. This value ranges from 1 to 50 with a default of 5.
damp-peer-oscillations		Enter to enable the damp peer oscillation option On implementing this logic, it damps the oscillations of BGP peers in the face of sequences of automatic start and automatic stop in the IDLE state.5.
default-originate		Enter to enable advertisement of the default route to the peer or neighbor for use as a default route. This command overrides the global default route configuration and sends a default route to the peer with self next-hop. The advertisement occurs irrespective of the presence of default route in FDB. This command does not require the presence of 0.0.0.0 in the local router. When used with a route map, the default route 0.0.0.0 is injected if the route map contains a match ip address clause. The route map can contain other match clauses also.By default, the advertisement of default route to the peer is disabled. This command executes only if Peer/ Peer Group is created and Peer AS is configured. The no form of the command disables advertisement of the default route to the peer.
delay-open		Enter to configure a delay in sending the first OPEN message to the BGP peer for a specific time period. By default, the delay open option is disabled. This command executes only if Peer/ Peer Group is created and Peer AS is configured. The no form of the command disables the delay open option.

Parameter	Type	Description
ebgp-multihop		Enter to enable the BGP to establish connection with external peers residing on networks that are not directly connected. By default, external BGP peers need to be directly connected. If external BGP peer are not connected directly, then ebgp-multihop is enabled to initiate the connection with that external peer. If ebgp-multihop is disabled and external BGP peers are indirectly connected, then BGP peer session will not be established. • EBGP Multihop is disabled. • ttl-1 This command executes only if Peer/ Peer Group is created and Peer AS is configured. The no form of the command disables the peer EBGP-Multihop feature.
ttl <(1-255)>		Enter a value for the maximum hop limit that is allowed for indirect BGP session. This value ranges from 1 to 255.
fall-over bfd		Enter to enable the BFD monitoring for the peer IP address or peer-group name. On enabling, BGP registers with BFD for IP path monitoring when the session state becomes ESTABLISHED. By default, BFD Monitoring is disabled.
local-as		Enter to update the local AS used for the peer connection. This command executes only if Peer/ Peer Group is created and Peer AS is configured. The no form of the command resets the local AS used for the peer connection to the global local-As.
<AS no>		Enter to configure the Autonomous system number for the specified IP address of the peer/peer group name. This value ranges from 1 to 4294967295 or 0.1 to 65535.65535. **NOTE:** When four-bit-asn is enabled, This value ranges from 1 to 4294967295 or between 0.1 and 65535.65535 **NOTE:** When four-bit-asn is disabled, This value ranges from 1 to 65535 or between 0.0 and 0.65535 **NOTE:** When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.65535.
maximum-prefix		Enter to configure the maximum number of peers supported by BGP. BGP speaker imposes a locally-configured, upper bound on the number of address prefixes the speaker is willing to accept from a neighbor. This command executes only if Peer/ Peer Group is created and Peer AS is configured. The no form of the command resets the max number of routes that is learned from that particular peer.

Parameter	Type	Description
<prefix-limit (1-2147483647)>		Enter a value for the maximum number of address prefixes that the BGP Peer is willing to accept from the neighbor. This value ranges from 1 to 2147483647 with a default of 100.
next-hop-self		Enter to configure the router as the next hop for BGP-speaking neighbor or peer group and enables BGP to send itself as the next hop for advertised routes. Administrator uses this command to make BGP speaker fill its address when advertising routes to the BGP peer. This command is useful in non-meshed networks where BGP neighbors may not have direct access to all other neighbors on the same IP subnet. This command executes only if Peer / Peer Group is created and Peer AS is configured. The no form of the command resets the peer nexthop-self status to default. The next hop will be generated based on the IP address of the destination and the present next hop in the route information..
remote-as		Enter to create a peer and to initiate the connection to the peer and adds an entry to the BGP or multiprotocol BGP neighbor table. This specifies a neighbor with an autonomous system number that identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered as external. By default, neighbors that are defined using this command in router configuration mode exchange only unicast address prefixes. The administrator can create a peer and set the Peer AS number with this command. The configured Peer AS number is compared with the AS number received in the open message and a peer session is initiated only if both the AS numbers matchThe no form of the command disables the peer session and deletes the peer information.
<AS no>		Enter to configure the AS of the peer. This value ranges from 1 to 4294967295 or 0.1 to 65535.65535. **NOTE:** When four-bit-asn is enabled, This value ranges from 1 to 4294967295 or between 0.1 and 65535.65535 **NOTE:** When four-bit-asn is disabled, This value ranges from 1 to 65535 or between 0.0 and 0.65535 **NOTE:** When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.65535.

Parameter	Type	Description
allow-autostart		Enter to start the BGP session with the associated peer automatically. The peer session is automatically started in the IDLE state, after a BGP Peer session is brought down either by Autostop or through reception of invalid BGP message. The BGP session is automatically started after an interval specified by idle hold time. By default, allow-autostart is disabled.
[idlehold-time		Enter to configure the idle hold time. This specifies the length of time the BGP peer is held in the Idle state prior to the next automatic restart.
<seconds(1-65535)>		Enter a value for the idle hold time. This value ranges from 1 to 65535. by default, idlehold-time is 60 seconds. **NOTE:** The IdleHoldTime can be configured only when the allow-autostart is enabled. **NOTE:** After each dampening, the value of the Idle Hold Time is doubled consecutively.
route-reflector-client		Enter to control client-to-client reflection and configures the specified Peer as Client of the Route Reflector. All the neighbors configured with this command will be members of the client group and the remaining IBGP peers will be members of the nonclient group for the local route reflector. This command executes only if Peer is created. The no form of the command resets the Peer as conventional BGP Peer.
send-community		Enter to send community attribute to a BGP neighbor and to enable advertisement of community attributes (standard/extended) to peer. This command executes only if Peer/ Peer Group is created and Peer AS is configured. The no form of the command disables advertisement of community attributes (standard/extended) to peer.
both		Enter to send both standard and extended communities to peer. This is the default option.
standard		Enter to send only standard communities to the peer.
extended		Enter to send only extended communities to the peer.

Parameter	Type	Description
shutdown		Enter to disable the Peer session and terminates any active session for the specified neighbor or peer group and removes all associated routing information. In the case of a peer group, a large number of peering sessions could be terminated suddenly. This command executes only if Peer/ Peer Group is created and Peer AS is configured. The no form of the command enables the Peer session for the specified neighbor.
timers		Enter to configure neighbor KeepAlive Time and Hold Time Intervals and sets the timers for a specific BGP peer or peer group. This command executes only if Peer/ Peer Group is created and Peer AS is configured.
keepalive		Enter to configure the keep alive interval (in seconds) or frequency with keep alive messages are sent to its peer for the peer session.
<(1-21845) seconds>		Enter a value for the keep alive interval. The keep-alive value must always be less than the configured hold-time value— it ranges from 1 to 21845. The default is 30 seconds.
holdtime		Enter to configure the hold-time interval (in seconds) for the peer, which is sent in the OPEN message to the peer. This is the time interval in seconds for the Hold Time configured for BGP speaker with the peer. The system declares a peer dead, after ensuring that keep alive message is not received within this time period from the peer.
<(3-65535) seconds>		Enter a value for the hold-time interval. This value ranges from 3 to 65535 seconds. The default is 90 seconds.
delayopentime		Enter to configure the delay open time which is the amount of time that the BGP peer should delay in sending the OPEN message to the remote peer.
<(0-65535) seconds>		Enter a value for the delay open time. This value ranges from 0 to 65535. The default is 0 seconds. **NOTE:** The value 0 implies that the BGP Peer can send an OPEN message without any delay to its neighbor.
transport connection-mode		Enter to configure the BGP Peer Transport Connection status as active or passive. This command executes only if Peer/ Peer Group is created and Peer AS is configure.
active		Enter for active BGP Peer Transport Connection status. When a peer transport connection is made active, then the peer will immediately initiate the session with the peer by sending an open message to it. This is the default option.

Parameter	Type	Description
passive		Enter for passive BGP Peer Transport Connection status. When the peer transport connection is passive, then the peer will not immediately initiate the session, instead, it waits for the peer to send the open message so that it can respond to it to create the session.
route-map		Enter to enable the route map or IP prefix list for the neighbor. This command executes only if Peer/ Peer Group is created and Peer AS is configured. The no form of the command disables routemap or IP prefix list for the neighbor.
<name(1-20)>		Enter a name of the Route Map— a string with the maximum size as 20.
prefix-list		Enter to configure IP prefix list for neighbor.
<iipprefilist_name (1-20)>		Enter a value for the IP prefix list for neighbor. This value is a string with the maximum size as 20.
in		Enter to enable / disable Route map or IP Prefix List for inbound routes.
out		Enter to enable / disable Route map or IP Prefix List for outbound routes.
advertisement-interval		Enter to configure Time-interval (in seconds) for spacing advertisement of successive external route-updates to the same destination.
<seconds(1-65535)>		Enter a value for the advertisement-interval - the range is from 1 to 65535 seconds.
as-origination-interval		Enter to configure the as-origination-interval.
<seconds(1-65535)>		Enter a value for the as-origination-interval- the range is from 1 to 65535 seconds.
connect-retry-interval		Enter to configure the connect-retry-interval.
<seconds(1-65535)>		Enter a value for the connect-retry-interval - the range is from 1 to 65535 seconds.
hold-advertised-routes		Enter to enable holding of advertised routes to peer. This command executes only if Peer/ Peer Group is created and Peer AS is configured. The no form of the command disables holding of advertised routes to peer and sets to its default.

Parameter	Type	Description
peer-group		Enter to adds the neighbor as the member of the specified peer group. The no form of the command removes the neighbor as the member of the specified peer group. This command executes only if • Peer is created and Peer AS is configured. • Peer Group is created.
<string(20)>		Enter a name of the BGP peer group - a string of 20 characters.

Mode

BGP Router Configuration Mode

Examples

iS5comm(config)# router bgp 100

iS5comm (config-router)# neighbor 23.45.0.1 gateway 10.0.0.1

iS5comm (config-router)# neighbor 23.45.0.1 network-address 3399::11

iS5comm (config-router)# neighbor 3399::11 network-address 23.45.0.1

iS5comm (config-router)# neighbor 10.0.0.2 password abcdef

iS5comm (config-router)# neighbor a1 peer-group

iS5comm (config-router)# neighbor 20.45.0.1 tcp-ao mkt 2

iS5comm (config-router)# neighbor 23.45.0.1 update-source 40.0.0.1

iS5comm (config-router)# neighbor 12.0.0.1 allow-autostop

iS5comm (config-router)# neighbor 23.45.0.1 as-override

iS5comm (config-router)# neighbor 23.45.0.1 capability ipv4-unicast

iS5comm (config-router)# neighbor 12.0.0.1 connect-retry-count 50

iS5comm (config-router)# neighbor 12.0.0.1 damp-peer-oscillations

iS5comm (config-router)# neighbor 23.45.0.1 default-originate

iS5comm (config-router)# neighbor 12.0.0.1 delay-open

iS5comm (config-router)# neighbor 23.45.0.1 ebgp-multihop ttl 20

iS5comm (config-router)# neighbor 12.0.0.1 fall-over bfd

iS5comm (config-router)# neighbor 10.3.4.5 local-as 1

iS5comm (config-router)# neighbor 23.45.0.1 maximum-prefix 255

iS5comm (config-router)# neighbor 23.45.0.1 next-hop-self

iS5comm (config-router)# neighbor 23.45.0.1 remote-as 66

iS5comm (config-router)# neighbor 23.45.0.1 route-reflector-client

iS5comm (config-router)# neighbor 23.45.0.1 send-community both

iS5comm (config-router)# neighbor 23.45.0.1 shutdown

iS5comm (config-router)# neighbor 23.45.0.1 timers keepalive 40

iS5comm (config-router)# neighbor 10.3.4.5 transport connection-mode passive

iS5comm (config-router)# neighbor 10.3.4.5 route-map r1 in

iS5comm (config-router)# neighbor 23.45.0.1 hold-advertised-routes

iS5comm (config-router)# neighbor advertisement-interval 1

iS5comm (config-router)# neighbor 10.3.4.5 peer-group a1

26.16. network

To configure the local network address that will be advertised to BGP, use the command **network** in *BGP* Router Configuration Mode. The no form of the command disables the local network address advertised to BGP.

network

```
network <ipv4-address | ipv6-address> mask <prefixLen>
```

no network

```
no network <ipv4-address | ipv6-address> mask <prefixLen>
```

Parameters

Parameter	Type	Description
<ipv4-address>		Enter to configure the local network IPv4 address that will be advertised to BGP.
<ipv6-address>		Enter to configure the local network IPv6 address that will be advertised to BGP.
mask		Enter to configure the subnet mask with prefix length for the local network address that will be advertised to BGP.
<prefixLen>		Enter prefix length for the local network address that will be advertised to BGP. This prefix length ranges from 1 to 32 or 0 to 128.

Mode

BGP Router Configuration Mode

Notes

The route-map filters are not applied for prefixes advertised via network command when redistribution is enabled with route-map.

Examples

iS5comm (config-router)# network 12.0.0.1 mask 1

26.17. redistribute

To control redistribution of Direct, Static and RIP routes into *BGP*, configure the protocol from which the routes have to be redistributed into *BGP* after applying the specified route map, and configure the redistribution of OSPF routes into *BGP*, use the command **redistribute** in *BGP* Router Configuration Mode. If this is set to enable, only the routes from the protocols are imported into *BGP* and *BGP* routes will not be distributed. If this is set as disable, then the routes learned from protocols are removed from *BGP* and no route is distributed. The no form of the command disables the redistribution of routes from the given protocol into BGP and the redistribution of routes from the OSPF protocol into *BGP*. The route map is disassociated from the redistribution, if the no form of the command specifies the route map.

redistribute

```
redistribute {{static | connected | rip | all} [route-map <string(20)>]
[metric <integer (0-4294967295)>]}
```

```
 | ospf [match {external | internal | nssa-external}] [route-map <string>]
[metric] <integer (0-4294967295)>]}
```

no redistribute

```
no redistribute
 {{static | connected | rip | all} [route-map <string(20)>] [metric]}
 | ospf [match {external | internal | nssa-external}] [route-map <string>]
[metric]}
```

Parameters

Parameter	Type	Description
`static`		Enter to redistribute routes, configured statically, in the BGP routing process.
`connected`		Enter to redistribute directly connected networks routes, in the BGP routing process.
`rip`		Enter to redistribute routes that are learnt by the RIP process, in the BGP routing process.
`all`		Enter to redistribute routes, that are learnt by the all processes (RIP statically configured and connected routes), in the *BGP* routing process.
`route-map`		Enter to identify the specified route-map in the list of route-maps during redistribution of routes to BGP. If this is not specified, all routes are redistributed.
`<string(20)>`		Enter a value for the route map—a string with the maximum size of 20.
`metric`		Enter to specify the metric value for the routes to redistribute to BGP. If this is not specified, all routes are redistributed. If the metric value not specified, default metric value is considered.
`integer (0-4294967295)`	Integer	Enter a metric value for the route map—ranges from 0 to 4294967295.
`ospf`		Enter to configure the redistribution of OSPF routes into *BGP*.
`match`		Enter to match the OSPF route type to be redistributed into *BGP*.
`external`		Enter to redistribute OSPF external routes.
`internal`		Enter to redistribute OSPF internal routes.
`nssa-external`		Enter to redistribute OSPF NSSA external routes.

Mode

BGP Router Configuration Mode

Default

Redistribution is disabled

Metric - 0

Notes

Redistribution can be configured for only one route map. Another route map can be assigned, only if the already assigned route map is disabled.

Examples

iS5comm(config-router)# redistribute all route-map rm metric 500

iS5comm (config-router)# redistribute ospf match external route-map rm metric 500

26.18. restart-reason

To configure the reason for the graceful restart of the BGP router, use the command **restart-reason** in *BGP* Router Configuration Mode. The reason for restart can be unknown, software upgrade, scheduled restart or switch to redundant router. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent. The no form of the command resets the reason for restart.

restart-reason

```
restart-reason [{unknown |softwareRestart |swReloadUpgrade}]
```

no restart-reason

```
no restart-reason [{unknown |softwareRestart |swReloadUpgrade}]
```

Parameters

Parameter	Type	Description
`unknown`		Enter to configure a reason for graceful restart of the BGP router as restart due to unplanned events (such as restarting after a crash).
`softwareRestart`		Enter to configure a reason for graceful restart of the BGP router as restart due to restart of software.
`swReloadUpgrade`		Enter to configure a reason for graceful restart of the BGP router as restart due to reload or upgrade of software.

Mode

BGP Router Configuration Mode

Examples

iS5comm (config-router)# restart-reason swReloadUpgrade

26.19. restart-support

To enable the graceful restart support, use the command **restart-support** in *BGP* Router Configuration Mode. Graceful restart support is provided for both planned and unplanned restart, if the command is executed without any option.The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent. The no form of the command disables the graceful restart support.

restart-support

```
restart-support [plannedOnly]
```

no restart-support

```
no restart-support [plannedOnly]
```

Parameters

Parameter	Type	Description
plannedOnly		Enter to support only the planned restarts (such as restarting a control plane after a planned downtime).

Mode

BGP Router Configuration Mode

Examples

iS5comm (config-router)# restart-support

26.20. router bgp

To enable the *ASN* of the *BGP* Speaker and enter into *BGP* router configuration mode, use the command **router bgp** in Global Configuration Mode. The no form of the command configures the AS number of the BGP Speaker to its default value.

router bgp

```
router bgp
```

no router bgp

```
no router bgp
```

Parameters

Parameter	Type	Description
<AS no>		Enter the *ASN* that identifies the *BGP* router to other routers and tags the routing information passed along. This command also allows setting up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems. **NOTE:** When four-byte *ASN* is enabled, this value ranges from 1 to 4294967295or between 0.1 and 65535.65535. **NOTE:** When four-byte *ASN* is disabled, this value ranges from 1 to 65535. or between 0.1 and 0.65535 **NOTE:** When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.65535.

Mode

Global Configuration Mode

Default

0

Note

If the *ASN* value is already configured to a non-zero value, it must be reset to zero (using no form of the command) before reconfiguring.

The "no router bgp" or "no router bgp command deletes all BGP configurations done on all VRs.

Examples

iS5comm(config)# router bgp 100

iS5comm (config-router)#

26.21. show bgp-version

To display the BGP Version information, use the command **show bgp-version** in Privileged EXEC Mode.

show bgp-version

```
show bgp-version
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show bgp-version

```
    Is5BGP Version : 4
```

26.22. show ip bgp

To display the BGP related information, use the command **show ip bgp** in Privileged EXEC Mode. When you specify a parameter, the command displays information only for the specified parameter.

show ip bgp

```
show ip bgp
 {extcommunity {route |policy |filter}
 | peer-group [<peer-group-name> [summary]]
 |tcp-ao mkt summary [<random_str>]
 | {EndOfRIBMarkerStatus [neighbor [<peer-addr>]]}
 {[neighbor [<peer-addr [received prefix-filter] [advertised-routes]]] |
[rib] | [stale] |[<ip_addr>] [prefix-len]}
 | aggregate
 | community {route |policy |filter}
 | confed info
 | dampening [{flap-statistics | dampened-paths}]
 | filters
 | info
 | local-pref
 | med
 | restartexitreason
 | restartreason
 | restartstatus
 | restartsupport
```

```
 | rfl info
 | summary
 | timers
 | vpnv4 {all | vrf <string(32)> | <ip-addr> [prefix-len]} {restartmode
[neighbor
 | [<peer-addr>]]}
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show ip bgp restartreason

```
    Context Name : default
    -------------
    Is5 BGP4: Restart reason is software restart
```

26.23. synchronization

To enable synchronization between *BGP* and *IGP*, use the command **synchronization** in *BGP* Router Configuration Mode. BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the *IGP*. This command allows routers and access servers within an autonomous system to have the route before *BGP* makes it available to other autonomous systems.The no form of the command disables the enable synchronization between *BGP* and *IGP*.

synchronization

```
synchronization
```

no synchronization

```
no synchronization
```

Mode

BGP Router Configuration Mode

Default

The synchronization between the *BGP* and *IGP* is disabled

Note

This command is a complete standardized implementation of the existing command and operates similar to that of the command ip bgp synchronization.

Examples

iS5comm(config)# router bgp 100

iS5comm (config-router)# synchronization

26.24. tcp-ao mkt key-id

To create a TCP-AO Master Key Tuple (MKT) in the BGP instance, use the command **tcp-ao mkt key-id** in *BGP* Router Configuration Mode. This command executes only if BGP Speaker Local AS number is configured. The no form of the command deletes a TCP-AO MKT in the BGP instance.

tcp-ao mkt key-id

```
tcp-ao mkt key-id <Key Id(0-255)> receive-key-id <Rcv Key Id (0-255)> algo-
rithm {hmac-sha-1 | aes-128-cmac} key <master-key> [tcp-option-exclude]
```

no tcp-ao mkt key-id

```
no tcp-ao mkt key-id <Key Id(0-255)>
```

Parameters

Parameter	Type	Description
`key-id <Key Id(0-255)>`	Integer	Enter to set the send KeyID of the MKT. This value is used to fill the key-id field in the TCP-AO option in the TCP header. This value ranges from 0 to 255.
`receive-key-id <Rcv Key Id (0-255)>`		Enter to set the Receive Key-id of the MKT. The MKT ready at the sender to be used for authenticating received segments is indicated to the peer by filling the receive key id of the MKT in of the TCP-AO option in TCP header. This value ranges from 0 to 255.
`algorithm`		Enter to configure the algorithm used for TCP-AO MAC or KDF calculation.
`hmac-sha-1`		Enter to configure the algorithm type as hmac-sha-1.
`aes-128-cmac`		Enter to configure the algorithm type as aes-128-cmac.
`key <master-key>`		Enter to configure the master key corresponding to the MKT. This value is an octet string with the size between 1 and 80.
`tcp-option-exclude`		Enter to set the exclude TCP option which excludes the TCP options other than TCP-AO during MAC calculation, If this is not set TCP-AO MAC will be calculated on TCP segment including all other TCP options.

Default

algorithm - hmac-sha-1

Mode

BGP Router Configuration Mode

Examples

iS5comm (config-router)# tcp-ao mkt key-id 1 receive-key-id 1 algorithm hmac-sha-1 key key1

IGMP Snooping

27. IGMP Snooping

Internet Group Multicast Protocol (IGMP) is the protocol used by a host to inform a router when it joins (or leaves) an Internet multicast group. IGMP is only used on a local network; a router must use another multicast routing protocol to inform other routers of group membership.

IGMP Snooping (IGS) is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers. In IGS, a host computer uses IGMP to inform a router that it intends to listen to a specific multicast address. If another computer snoops such packets, it can learn the multicast sessions to which other computers on the local network are listening. The multicast packet transfer happens only between the source and the destination computers. Broadcasting of packets is avoided.

IGMP snooping significantly reduces traffic from streaming media and other bandwidth-intensive IP multicast applications.

27.1. debug ip igmp snooping

To specifies the debug levels for IGMP snooping module, use the command **debug ip igmp snooping** in Privileged EXEC Mode. The no form of the command resets the debug level for IGMP snooping module. This command configures the various debug and trace statements to handle error and event management in the IGMP snooping module. The traces are enabled by passing the necessary parameters.

debug ip igmp snooping

```
debug ip igmp snooping ([init] [resources] [tmr] [src] [grp] [qry]  [redun-
dancy] [pkt] [fwd] [vlan] [entry] [exit] [mgmt] [np] [buffer] [icch] [trace]
[all]) [switch <switch_name>]
```

no debug ip igmp snooping

```
no debug ip igmp snooping ([init] [resources] [tmr] [src] [grp] [qry]
[redundancy] [pkt] [fwd] [vlan] [entry] [exit] [mgmt] [np] [buffer] [icch]
[trace] [all]) [switch <switch_name>]
```

Parameters

Parameter	Type	Description
init		Enter to generate Init and Shutdown trace messages at the instances when the module is initiated or shut down. The information is logged in a file.
resources		Enter to generate System Resources management trace messages when there is a change in the resource status. The information is logged in a file.
tmr		Enter to generate Timer trace messages at the instances where timers are involved. The information is logged in a file.
src		Enter to generate trace messages when Source Information is involved.
grp		Enter to generate trace messages when Group Information is involved.
qry		Enter to generate trace messages when Query messages are sent or received.
redundancy		Enter to generate debug statements for redundancy code flow traces. This trace is generated when there is a failure in redundancy processing.
pkt		Enter to generate debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.
fwd		Enter to generate traces messages when forwarding Database is involved.
vlan		Enter to generate trace messages when VLAN related Information is involved
entry		Enter to generate trace messages to specify function entry points.
exit		Enter to generate trace messages to specify function exit points.
mgmt		Enter to generate debug statements for management configuration. Currently, it is default.
np		Enter to generate NPAPI related configuration messages
buffer		Enter to generate buffer information messages.
icch		Enter to generate ICCH related messages.
trace		Enter to generate trace for the protocol.
all		Enter to generate all types of trace messages.
switch		Enter to generate trace messages for the specified switch context.
<switch_name>		Enter a switch name. Currently, it is default.

Mode

Privileged EXEC Mode

Prerequisites

Debugging is Disabled.

Examples

iS5comm# debug ip igmp snooping fwd

27.2. ip igmp snooping

To configure the port leave mode for an interface, maximum limit type for an interface, or multicast profile index for a downstream interface, use the command **ip igmp snooping** in Interface Configuration Mode. The no form of the command configures the maximum limit type as none for an interface or resets the multicast profile index to default value.

ip igmp snooping

```
ip igmp snooping
 {leavemode {exp-hosttrack | fastLeave | normalleave} [InnerVlanId <short
(1-4094)>]
 | limit {channels | groups} | normalleave} [InnerVlanId <short (1-4094)>]
 | filter-profileid <integer> [InnerVlanId <short (1-4094)>]}
```

no ip igmp snooping

```
no ip igmp snooping
 {limit [InnerVlanId <short (1-4094)>]
 | filter-profileid [InnerVlanId <short (1-4094)>]}
```

Parameters

Parameter	Type	Description
leavemode		Enter to configure the port leave mode for an interface. The mechanism to process the leave messages in the downstream is selected. The switch sends an IGMP query message to find if there is any host interested in the multicast group.
exp-hosttrack		Enter to process the leave messages using the explicit host tracking mechanism. The decision to remove the interface is made based on the tracked host information.
fastLeave		Enter to configure the leave messages using the fast leave mechanism. On receiving a leave message, the interface is removed from the group registration and the leave message is sent to the router ports.
normalleave		Enter to send a group or group specific query on the interface for every received leave message.The port is configured to use the normal leave mode. The normal leave mode is applicable only for v2 hosts. When the system receives a v2 leave message, it sends a group specific query on the interface. For v3 hosts, normal leave has no effect.
InnerVlanId		Enter to configure the inner VLAN ID value. In provider bridging domain, the customer VLAN itag is denoted as InnerVlanId. • If InnerVlanId is specified, multicast forwarding mode must be IP based and enhanced mode must be enabled in the snooping system. • If InnerVlanId is not specified, leave mode can be configured irrespective of multicast forwarding mode and enhanced mode status.
<short (1-4094)>	Integer	Enter a value for the inner VLAN ID. It ranges from 1 to 4094.
limit		Enter to configure the maximum limit type for an interface. The maximum limit is the number of unique registrations for a channel or group.
channels		Enter to configure the snooping maximum limit as channels (group, source). Channel limit is applied for IGMPv3 include and allow reports.
groups		Enter to configure the snooping maximum limit as groups. Group limit is applied for all IGMP reports.
<interger32>	Integer	Enter a value for the snooping maximum limit. This value ranges from 0 to 4294967295.

Parameter	Type	Description
InnerVlanId		Enter to configure the maximum limit type for the Inner VLAN ID. If InnerVlanId is specified, enhanced mode should be enabled; otherwise, enhanced mode does not need to be enabled.
<short (1-4094)>	Integer	Enter a value for the inner VLAN ID. It ranges from 1 to 4094.
filter-profileid		Enter to configure the multicast profile index for a downstream interface. This profile contains a set of allowed or denied rules to be applied for the IGMP packets received through the downstream interface.
<integer>	Integer	Enter a value to configure the multicast filter profile index for a downstream interface.
InnerVlanId		Enter to configure the multicast filter profile index for the Inner VLAN identifier. If InnerVlanId is specified, then enhanced mode should be enabled; otherwise, enhanced mode does not need to be enabled.
<short (1-4094)>	Integer	Enter a value for the Inner VLAN ID. It ranges from 1 to 4094.

Mode

Interface Configuration Mode

Default

- exp-host track/fastLeave/normalleave - Normalleave
- The limit is set as 0 so that no limiting is done.
- profileid - the profile ID is 0.

Prerequisites

- The leave process configuration level has to be port.
- limit
  - The IGMP snooping filter must be enabled for this configuration to have the effect.
  - Even without enabling IGMP snooping filter, control plane data structure update takes place. But the benefits can be realized only when IGMP Snooping filter is enabled.
- filter-profileid
  - The IGMP snooping filter must be enabled for this configuration to have the effect.
  - Even without enabling IGMP snooping filter, control plane data structure update takes place. But the benefits can be realized only when IGMP Snooping filter is enabled.

– IGMP Snooping multicast forwarding mode must be IP based.

Examples

iS5comm(config)# int gi 0/1

iS5comm(config-if)# ip igmp snooping leavemode fastLeave InnerVlanId 1

iS5comm(config-if)# ip igmp snooping limit groups 10 InnerVlanId 1

iS5comm(config-if)# ip igmp snooping filter-profileid 2 InnerVlanId 1

27.3. ip igmp snooping

To enable IGMP snooping system enhanced and sparse mode in the switch and fast leave processing and IGMP snooping for a specific VLAN, configure the snooping filter and proxy reporting, the IGMP general query transmission feature, the time interval (in seconds) after which the switch sends a group specific query, the IGMP snooping router time-out interval (in seconds) after which port is deleted if no IGMP router control packets are received, the multicast VLAN feature related configuration on a port, to specify if IGMP reports should be forwarded on all VLAN member ports or router ports or non-edge ports and set the IGMP snooping report-suppression time interval for which IGMPv2 report messages will not get forwarded to the router, use the command **ip igmp snooping** in Global Configuration Mode. The no form of the command disables IGMP snooping in the switch (or specific VLAN). When IGMP snooping is disabled globally, it is disabled in all VLAN interfaces.

ip igmp snooping

```
ip igmp snooping
 [enhanced-mode {enable | disable}]
 [filter]
 [group-query-interval <(2-5) seconds>]
 [mrouter-time-out <(60 – 600) seconds>]
 [multicast-vlan {enable | disable}]
 [port-purge-interval <(130 - 1225) seconds>]
 [proxy]
 [proxy-reporting]
 [query-forward {all-ports | non-router-ports}]
 [report-forward {all-ports | router-ports | non-edge-ports}]
 [report-suppression-interval <(1 - 25) seconds>]
 [retry-count <(1 - 5>]
 [send-query {enable | disable}]
 [source-only learning age-timer <short(130-1225)>]
```

```
 [sparse-mode {enable | disable}]
 [vlan
<vlanid/vfi_id> | <vlanid (1-4094)>
 {immediate-leave | mrouter <ifXtype> <iface_list>}]
```

no ip igmp snooping

```
no ip igmp snooping
 [filter]
 [group-query-interval]
 [mrouter-time-out]
 [port-purge-interval]
 [proxy]
 [proxy-reporting]
 [report-forward]
 [report-suppression-interval]l
 [retry-count]
 [source-only learning age-timer]
 [vlan <vlanid/vfi_id> | <vlanid (1-4094)>]
 {immediate-leave | mrouter <ifXtype> <iface_list>}]
```

Parameters

Parameter	Type	Description
enhanced-mode		Enter to configure the snooping system enhanced mode in the switch. It is provided to enhance the operation of IGMP snooping module to duplicate multicast traffic by learning multicast group entries based on the port and inner VLAN. This mode of operation is applied when the downstream devices are less intelligent or not capable of duplicating multicast traffic.
enable		Enter to enable snooping system enhanced mode in the switch. **NOTE:** Enhanced mode is in enabled state only when the snooping mode is set as IP Based.
disable		Enter to disable snooping system enhanced mode in the switch. This is default.
filter		Enter to configure the IGMP snooping filter. The IGS filtering feature restricts channel registration from being added to the database. In transparent snooping, the filtered packet will not be added to the snooping database but will be forwarded upstream. When disabled, all filter related configurations remain but the incoming reports will not be subject to filtering. IGS module programs the hardware to remove the configured rate limit. It flushes all registrations learnt through a port if a threshold limit is configured for this interface.
group-query-interval		Enter to set the time interval (in seconds) after which the switch sends a group specific query to find out if there are any interested receivers in the group when it receives a leave message. If it does not receive a response from the group, the port is removed from the group membership information in the forwarding database.
<(2-5) seconds>	Integer	Enter a value to set the time interval (in seconds). It ranges from 2 to 5. The default is 2 seconds.
mrouter-time-out		Enter to set the IGMP snooping router time-out interval (in seconds) after which port is deleted if no IGMP router control packets are received
<(60 - 600) seconds>	Integer	Enter a value to set the IGMP snooping router time-out interval (in seconds). It ranges from 2 to 5.
multicast-vlan		Enter to configure the snooping system enhanced mode in the switch. It is provided to enhance the operation of IGMP snooping module to duplicate multicast traffic by learning multicast group entries based on the port and inner VLAN. This mode of operation is applied when the downstream devices are less intelligent or not capable of duplicating multicast traffic.

Parameter	Type	Description
enable		Enter to enable snooping system enhanced mode in the switch.
disable		Enter to disable snooping system enhanced mode. This is the default.
port-purge-interval		Enter to set the time interval (in seconds) after which the switch sends a group specific query to find out if there are any interested receivers in the group when it receives a leave message. If it does not receive a response from the group, the port is removed from the group membership information in the forwarding database.
<(130 - 1225) seconds>	Integer	Enter a value to set the time interval (in seconds). It ranges from 2 to 5. The default is 260 seconds.
proxy		Enter to configure proxy reporting in the IGMP snooping switch. In proxy mode, the switch acts as a querier for all downstream interfaces and as a host for all upstream interfaces. The switch sends general query to all downstream interfaces at the query interval and collects information about the member ports. The proxy sends current consolidated report and state change report to upstream interfaces. By default, the proxy is disabled in the IGMP snooping switch. **NOTE:** Proxy can be enabled in the IGMP snooping switch only if the proxy reporting is disabled in the snooping switch.
proxy-reporting		Enter to configure proxy reporting in the IGMP snooping switch. When enabled, the switch supports the multicast router to learn the membership information of the multicast group. It forwards the multicast packets based on group membership information. The proxy-reporting switch acts as a querier to the downstream hosts. It sends proxy-reporting to upstream queriers. By default, proxy-reporting is enabled. **NOTE:** Proxy reporting can be enabled in the IGMP snooping switch only if the proxy is disabled in the switch.
query-forward		Enter to configure the snooping system enhanced mode in the switch. It is provided to enhance the operation of IGMP snooping module to duplicate multicast traffic by learning multicast group entries based on the port and inner VLAN. This mode of operation is applied when the downstream devices are less intelligent or not capable of duplicating multicast traffic.
all-ports		Enter to configure the query messages to be sent to all member ports of VLAN. the IGMP query forward administrative control status as all VLAN member ports. This is done to find out if there are any interested listeners in the network.

Parameter	Type	Description
non-router-ports		Enter to configure the query messages to be sent only to non-router ports. This is done to reduce the traffic in the network. This is default.
report-forward		Enter to specify if IGMP reports should be forwarded on all VLAN member ports or router ports or non-edge ports. The configuration enables the switch to forward IGMP report messages to the selected ports thus avoiding flooding of the network.
all-ports		Enter to configure the IGMP reports to be forwarded to all ports of a VLAN.
router-ports		Enter to configure the IGMP reports to be forwarded only to router ports of a VLAN. This is the default.
non-edge-ports		Enter to configure the IGMP reports to be forwarded only to router ports of a VLAN.
non-router-ports		Enter to configure the IGMP reports to be forwarded only to STP non-edge ports of a VLAN.
report-suppression-interval		Enter to set the IGMP snooping report-suppression time interval for which IGMPv2 report messages will not get forwarded to the router ports for the same group. The switch forwards IGMPv2 report messages to a multicast group. A timer is started immediately after forwarding the report message and runs for set period of time. During this interval, the switch does not forward another IGMPv2 report message addressed to the same multicast group to the router ports. **NOTE:** The ip igmp snooping report-suppression-interval is used only when the proxy and proxy-reporting are disabled.
<(1 - 25) seconds>	Integer	Enter a value to set the time interval (in seconds). It ranges from 2 to 5. The default is 5 seconds.
retry-count		Enter to set the maximum number of group specific queries sent on a port on reception of a IGMPv2 leave message. This command sets the maximum number of group specific queries sent by the switch to check if there are any interested v2 receivers for the group when it receives a leave message in the proxy/ proxy-reporting mode. The port is deleted from the group membership information in the forwarding database if the maximum retry count exceeds set number.
<1 - 5>	Integer	Enter a value to set he maximum number of group specific queries sent on a port on reception of a IGMPv2 leave message. It ranges from 1 to 5.
send-query		Enter to configure the IGMP general query transmission feature upon topology change in the switch.

Parameter	Type	Description
enable		Enter to enable the snooping query transmission status which generates IGMP query messages
disable		Enter to disable the snooping query transmission status which stops the switch from generating IGMP query messages
source-only		Enter to configure the IGMP snooping port purge time interval after which the port gets deleted if IGMP reports are not received. When a port receives reports from hosts, the timer is initiated. If the port receives another report before the timer expires, the timer is restarted. If the port does not receive any report from hosts till the timer expires, then the port entry is purged from the multicast database.
learning		Enter to set learning age timer configuration.
age-timer		Enter to set interval (in seconds) after which port is deleted if no IGMP reports are received.
<short(130-1225)>	Integer	Enter a value for the interval (in seconds) after which a port is deleted if no IGMP reports are received. The default is 260 seconds.
sparse-mode		Enter to configure the snooping system sparse mode in the switch. In the sparse mode, the IGS module drops the unknown multicast traffic when there is no listener for the multicast data. In the non-sparse-mode, the IGS module forwards the unknown multicast traffic. The multicast data gets flooded to the member port of vlan. **NOTE:** Sparse mode is in enabled state only when the snooping mode is set as MAC Based.
enable		Enter to enable the snooping system sparse mode in the switch. It drops unknown multicast packets.
disable		Enter to disable the snooping system sparse mode in the switch. Floods unknown multicast packets. This is default.
vlan <vlanid(1-4094)>		Enter to enable fast leave processing and IGMP snooping for a specific VLAN. It enables IGMP snooping only for the specific VLAN when IGMP snooping is globally disabled. When the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received. The ID of the VLAN ranges between 1 and 4094.
immediate-leave		Enter to set fast leave processing configuration. By default, fast leave processing is disabled in all VLANs.

Parameter	Type	Description
mrouter		Enter to enable IGMP snooping and configures a list of multicast router ports for a specific VLAN, if IGMP snooping is globally enabled. This will enable IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled. Any IGMP message received on a switch is forwarded only on the router-ports and not on host ports. In this manner, the IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network.
<ifXtype>		Enter to configure the list of multicast router ports for the specified type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 gigabit per second.extreme-ethernet – A version of Ethernet that supports data transfer up to 10 gigabits per second. This Ethernet supports only full duplex links.
<iface_list>		Enter to set a list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided for interface types internal-lan and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3

Mode

Global Configuration Mode

Examples

iS5comm(config)# ip igmp snooping enhanced-mode enable

iS5comm(config)# ip igmp snooping filter

iS5comm(config)# ip igmp snooping group-query-interval 3

iS5comm(config)#ip igmp snooping mrouter-time-out 70

iS5comm(config)# ip igmp snooping multicast-vlan enable

iS5comm (config)# ip igmp snooping port-purge-interval 150

iS5comm(config)# ip igmp snooping report-suppression-interval 20

iS5comm(config)# ip igmp snooping query-forward all-ports

iS5comm(config)# ip igmp snooping report-forward all-ports

iS5comm(config)# ip igmp snooping report-suppression-interval 20

iS5comm (config)# ip igmp snooping retry-count 4

iS5comm(config)# ip igmp snooping send-query enable

iS5comm (config)# ip igmp snooping source-only learning age-timer 200

iS5comm(config)# ip igmp snooping sparse-mode enable

iS5comm (config)# ip igmp snooping vlan 1 immediate-leave

iS5comm(config)# ip igmp snooping vlan 1 mrouter gigabitethernet 0/1

27.4. ip igmp snooping

To enable fast leave processing and IGMP snooping for a specific VLAN and IGMP snooping configuring a list of multicast router ports for a specific VLAN when IGMP snooping is globally enabled, configure statically the blocked router ports for a VLAN, the IGMP snooping switch as a querier for a specific VLAN, IGMP snooping static multicast related information, and operating version of IGMP PROXY on the upstream router port for a VLAN, set parameters such as the maximum response code inserted in general queries sent to host, the router port purge time-out interval for a VLAN, the maximum time interval to decide that another querier is present in the network, the time period with which the general queries are sent by the IGMP snooping switch or the maximum number of general query messages sent out on switch startuphen configured as querier on a VLAN, use the command **ip igmp snooping** in VLAN Configuration Mode. The no form of the command disables IGMP snooping in the switch (or specific VLAN) and sets all parameters to their default values. When IGMP snooping is disabled globally, it is disabled in all VLAN interfaces.

ip igmp snooping

```
ip igmp snooping
 [blocked-router <ifXtype> <iface_list>}]
 [fast-leave]
 [max-response-code <(0 - 255)>]
 [mrouter <ifXtype> <iface_list>}]
 [mrouter-port <ifXtype> <iface_list> {time-out <short(60-600)>
 | version {v1 | v2 | v3}]
 [multicast-vlan profile profile <Profile ID (0-4294967295)>]
 [other-querier-present-interval <value (120-1215) seconds>]
```

```
 [querier {address | <ucast_addr>}]
 [query-interval <(60 - 600) seconds>]
 [startup-query-count <(2 - 5>]
 [startup-query-interv <(15 - 150) seconds>]
 [static-group <mcast_addr> ports <ifXtype> <iface_list>}]
 [version {v1 | v2 | v3}]
```

no ip igmp snooping

```
no ip igmp snooping
 [blocked-router <ifXtype> <iface_list>}]
 [fast-leave]
 [max-response-code]
 [mrouter <ifXtype> <iface_list>}]
 [mrouter-port <ifXtype> <iface_list> {time-out <short(60-600)> | version]
 [multicast-vlan profile
 [other-querier-present-interval
 [querier
 [query-interval
 [startup-query-count
 [startup-query-interv <(15 - 150) seconds>]
 [static-group <mcast_addr> ports <ifXtype> <iface_list>}]
```

Parameters

Parameter	Type	Description
`blocked-router`		Enter to configure statically the blocked router ports for a VLAN. When configured as a blocked router, the queries, PIM DVMRP and data messages are discarded. The corresponding port entry is removed from the forwarding database. The ports to be configured as blocked router ports must not be configured as static router ports. **NOTE:** The ports to be configured as blocked router ports must not be configured as static router ports.
`<ifXtype>`		Enter to configure tthe type of interface to be employed on the port. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 gigabit per second.extreme-ethernet – A version of Ethernet that supports data transfer up to 10 gigabits per second. This Ethernet supports only full duplex links.
`<iface_list>`		Enter to set a list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided for interface types internal-lan and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3
fast-leave		Enter to enable fast leave processing and IGMP snooping for a specific VLAN. It enables IGMP snooping only for the specific VLAN when IGMP snooping is globally disabled. When the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received. By default, fast leave processing is disabled. **NOTE:** Fast leave configurations done in a VLAN when IGMP snooping is disabled in a VLAN will be applied only when IGMP snooping is enabled in the VLAN.
`max-response-code`		Enter to set the maximum response code inserted in general queries sent to host. The unit of the response code is tenth of second.
<(0 - 255)>	Integer	Enter a value for the maximum response code inserted in general queries sent to host. It ranges from 0 to 255 with a default of 100.

Parameter	Type	Description
mrouter		Enter to enable IGMP snooping and configures a list of multicast router ports for a specific VLAN when IGMP snooping is globally enabled. This will enable IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled.Any IGMP message received on a switch is forwarded only on the router-ports and not on the host ports. In this manner, the IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network. **NOTE:** The list of multicast router ports configured while IGMP snooping is disabled in the VLAN is applied only when the IGMP snooping is enabled in the VLAN.
<ifXtype>		Enter to configure the list of multicast router ports for the specified type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 gigabit per second.extreme-ethernet – A version of Ethernet that supports data transfer up to 10 gigabits per second. This Ethernet supports only full duplex links.
<iface_list>		Enter to set a list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided for interface types internal-lan and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3
mrouter-port		Enter to configure the router port purge time-out interval for a VLAN. The time interval after which the proxy assumes there are no v1/v2 routers present on the upstream port. While the older querier timer is running, the proxy replies to all queries with consolidated v1/v2 reports. When the timer expires, if the v2/v3 queriers are not present and the port is dynamically learnt, the port is purged. If the port is static, router port, the proxy replies to all queries with new version of v2/v3 consolidated reports. **NOTE:** The router ports must be statically configured for the VLAN.

Parameter	Type	Description
<ifXtype>		Enter to configure the list of multicast router ports for the specified type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 gigabit per second.extreme-ethernet – A version of Ethernet that supports data transfer up to 10 gigabits per second. This Ethernet supports only full duplex links.
<iface_list>		Enter to set a list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided for interface types internal-lan and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3
time-out		Enter to configure the router port purge time-out interval.
<short(60-600)>	Integer	Enter a value for the router port purge time-out interval. This value ranges from 60 to 600 seconds with a default of 125.
version		Enter to configure operating version of the IGMP snooping. **NOTE:** The router ports must be statically configured for the VLAN.
v1		Enter for IGMP snooping Version 1.
v2		Enter for IGMP snooping Version 2.
v3		Enter for IGMP snooping Version 3. This is the default.

Parameter	Type	Description
multicast-vlan		Enter to configure profile ID to VLAN mapping for multicast VLAN classification. The switch is configured with list of entries such as multicast group, multicast source and filter mode. These entries are maintained in access profiles. Each profile is associated with a particular VLAN which is categorized as multicast VLAN. When any untagged report or leave message is received (that is, packet with no tag in a customer bridge or packet with no S-tag in a provider or 802.1ad bridge), and if the group and source address in the received packet matches any rule in this profile, then the received packet is classified to be associated to the VLAN (that is, multicast VLAN) to which the profile is mapped. **NOTE:** • Multicast snooping mode should be IP based. • This command can be executed only after creating a multicast profile and setting the action for the created profile as permit. • The configurations done by this command will take effect only if the profile is activated.
profile		Enter to configure profile ID to VLAN mapping for multicast VLAN classification.
<Profile ID (0-4294967295)>	Integer	Enter a value to the multicast profile ID for a particular VLAN. This value ranges from 0 to 4294967295. The default is 0.
other-querier-present-interval-vlan		Enter to set the maximum time interval for deciding that another querier is present in the network. Within this time interval, if the querier receives response from another querier, then the one with a higher IP address is announced as the querier for the network. The other querier present interval must be greater than or equal to ((Robustness Variable * Query Interval) + (Query Response Interval/2)). Here, Robustness value is 2. **NOTE:** The switch should be configured as a querier for the other querier present command to be effective.
<(130 - 1225) seconds>	Integer	Enter a value for the maximum time interval for deciding that another querier is present in the network. This time interval ranges between 120 and 1215 seconds. The default is 255 seconds.
querier		Enter to configure the IGMP snooping switch as a querier for a specific VLAN. When configured as a querier, the switch sends IGMP query messages. The query messages will be suppressed if there are any routers in the network. The default is Non-querier.

Parameter	Type	Description
address		Enter to denote the interface VLAN or switch IP address to be used as source address.
<ucast_addr>		Enter to configure the query messages to be sent to all member ports of VLAN. the IGMP query forward administrative control status as all VLAN member ports. This is done to find out if there are any interested listeners in the network.
query-interval		Enter to set the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN. The switch sends querier messages in proxy mode and proxy-reporting mode to all downstream interfaces for this time interval. The value range is between 60 to 600 seconds. **NOTE:** • The switch must be configured as a querier for this configuration to be imposed. • In proxy reporting mode, general queries are sent on all down-stream interfaces with this interval only if the switch is the Querier. • In proxy mode, general queries will be sent on all downstream interfaces with this interval.
<(60 - 600) seconds>	Integer	Enter a value for the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN. The value range is between 60 to 600 with default of 125.
startup-query-count		Enter to set the maximum number of general query messages sent out on switch startup when the switch is configured as a querier. Startup query messages are sent to announce the presence of the switch along with its identity. The startup query count is manually configured to change the existing count.
<2 - 5>	Integer	Enter a value for the maximum number of general query messages sent out on switch startup when the switch is configured as a querier. This value ranges from 2 to 5. The default is 2.
startup-query-interval		Enter to set the time period with which the general queries are sent by the IGMP snooping switch during startup of the querier election process. **NOTE:** The switch should be configured as querier for the startup query interval command to produce results. The startup query interval should be less than or equal to ¼ of the query interval

Parameter	Type	Description
<(15 - 150) seconds>	Integer	Enter a value for the time period with which the general queries are sent by the IGMP snooping switch during startup of the querier election process. This time interval ranges between 15 and 150 seconds and should be less than or equal to query interval/ 4. The default is 31 seconds.
static-group		Enter to configure IGMP snooping static multicast related information. **NOTE:** The command executes only when IGMP snooping is enabled in the switch.
<mcast_addr>		Enter to configure the multicast address. This value ranges from 225.0.0.0. to 239.255.255.255
ports		Enter to enable the snooping query transmission status which generates IGMP query messages.
<ifXtype>		Enter to configure the snooping static multicast for the specified type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 gigabit per second.extreme-ethernet – A version of Ethernet that supports data transfer up to 10 gigabits per second. This Ethernet supports only full duplex links.
<iface_list>		Enter to configure the snooping static multicast for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided for interface types internal-lan and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3
version		Enter to configure operating version of the IGMP snooping. **NOTE:** The router ports must be statically configured for the VLAN.
v1		Enter for IGMP snooping Version 1.
v2		Enter for IGMP snooping Version 2.
v3		Enter for IGMP snooping Version 3. This is the default.

Mode

VLAN Configuration Mode

Examples

iS5comm(config)# vlan 55

iS5comm (config-vlan)# ip igmp snooping blocked-router gigabitethernet 0/2

iS5comm (config-vlan)# ip igmp snooping fast-leave

iS5comm(config-vlan)# ip igmp snooping max-response-code 10

iS5comm (config-vlan)# ip igmp snooping mrouter gigabitethernet 0/1

iS5comm(config-vlan)# ip igmp snooping mrouter-port gigabitethernet 0/1 time-out 150

iS5comm(config-vlan)# ip igmp snooping mrouter-port gigabitethernet 0/1 version v1

iS5comm (config-vlan)# ip igmp snooping multicast-vlan profile 1

iS5comm(config-vlan) # ip igmp snooping other-querier-present-interval 1215

iS5comm (config-vlan)# ip igmp snooping querier

iS5comm(config-vlan) # ip igmp snooping startup-query-interval 100

iS5comm (config-vlan) # ip igmp snooping startup-query-count 4

iS5comm(config-vlan) # ip igmp snooping startup-query-interval 100

iS5comm (config-vlan)# ip igmp snooping static-group 225.3.2.2 ports gigabitethernet 0/2

iS5comm(config-vlan)#ip igmp snooping version v2

27.5. ip igmp

To configure the multicast profile index for an interface or the maximum number of multicast groups that can be learnt on the interface, use the command **ip igmp** in Interface Configuration Mode. The no form of the command deletes the multicast profile index from an interface or the maximum limit type that was configured for the interface.

ip igmp

```
ip igmp {filter <profile number> | max-groups <integer32>}
```

Parameters

Parameter	Type	Description
`filter`		Enter to configure the multicast profile index for an interface. **NOTE:** This command is a standardized implementation of the existing command: ip igmp snooping filter-profileId. It operates similar to the existing command.
`<profile number>`	Integer	Enter a value to configure the multicast profile index for an interface. This value ranges from 1 to 4294967295.
`max-groups`		Enter to configure the maximum number of multicast groups that can be learnt on the interface.
`<integer32>`	Integer	Enter a value to configure the maximum number of multicast groups that can be learnt on the interface. This value ranges from 0 to 254. **NOTE:** This command is a standardized implementation of the existing command: ip igmp snooping limit. It operates similar to the existing command.

Mode

Interface Configuration Mode

Examples

iS5comm(config-if)# ip igmp filter 1

iS5comm(config-if)# ip igmp max-groups 5

27.6. ip igmp snooping clear counters

To clear the IGMP snooping statistics maintained for VLAN, use the command **ip igmp snooping clear counters** in Privileged Exec Mode.

ip igmp snooping clear counters

```
ip igmp snooping clear counters [vlan <vlan-id/vfi-id>]
```

Parameters

Parameter	Type	Description
vlan		Enter to clear the IGMP snooping statistics maintained for the specified VLAN / VFI ID. This value ranges from 1 to 65535. • <vlan–id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id> - VFI ID is a VLAN created in the system which contains pseudo wires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535. **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries. **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW. **NOTE:** The theoretical maximum for the maximum number of VFI is 65535, but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

Mode

Privileged Exec Mode

Examples

iS5comm# ip igmp snooping clear counters vlan 4094

27.7. mvr

To configure the multicast VLAN feature on a port, use the command **mvr** in Global Configuration Mode. Multicast VLAN feature is used for applications where wide-scale deployment of multicast traffic is necessary. MVLAN registration allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on any of the multicast VLANs. Multicast VLANs enable efficient multicast data flow in separate M-VLANs, while normal data flows through VLANs. This command is a standardized implementation of the existing command: ip igmp snooping multicast-vlan. It operates similar to the existing command. The no form of this command disables the multicast VLAN feature.

mvr

```
mvr
```

no mvr

```
no mvr
```

Mode

Global Configuration Mode

Default

non-router-ports

Examples

iS5comm(config)# mvr

27.8. show ip igmp snooping

To display the router ports, IGMP snooping information, IGMP group information, IGMP snooping statistics, the blocked router ports, IGMP multicast host information, and IGS port configuration information for all VLANs or a specific VLAN for a given switch or for all switches (if no switch is specified) and the multicast VLAN statistics in a switch, use the **show ip igmp snooping** command in Privileged EXEC Mode.

show ip igmp snooping

```
show ip igmp snooping
 [blocked-router [vlan <vlan-id/vfi-id>] [switch <switch_name>]]
 [forwarding-database [vlan <vlan-id/vfi-id>] [{static | dynamic}] [switch
<switch_name>]]
 [globals [switch <switch_name>]]
 [groups [vlan <vlan-id/vfi-id> [Group <Address>]] [{static | dynamic}]
[switch <switch_name>]]
 {mrouter [vlan <vlan-id/vfi-id>] [detail] [switch <switch_name>]]
 | multicast-receivers [vlan <vlan-id/vfi-id>] [Group <Address>]] [switch
<switch_name>]]
 [multicast-vlan [switch <switch_name>]]
 [port-cfg [{interface <interface-type> <interface-id> [InnerVlanId
vlan-id(1-4094)] [switch <switch_name>]]
 [statistics [vlan <vlan-id/vfi-id>] [switch <switch_name>]
 [switch <switch_name>]
 [vlan <vlan-id/vfi-id>] [switch <switch_name>]
```

Parameters

Parameter	Type	Description
`blocked-router`		Enter to display blocked router ports for all VLANs or a specific VLAN for a given switch or for all switches (if no switch is specified).
`vlan <vlan-id/vfi-id>`	Integer	Enter to specify the blocked router ports for the VLAN / VFI ID to be displayed. This value ranges from 1 to 65535. • <vlan–id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id> - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.
`switch`		Enter to display the IGMP snooping statistics for the specified context.
`<switch_name>`		Enter a value representing unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.
`forwarding-database`		Enter to display multicast forwarding entries for all VLANs or a specific VLAN or specific VLAN and group address for a given switch or for all switch (if no switch is specified).
`vlan <vlan-id/vfi-id>`	Integer	Enter to specify multicast forwarding entries for the VLAN / VFI ID to be displayed. This value ranges from 1 to 65535. • <vlan–id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.
`static`		Enter to display only static multicast entries.
`dynamic`		Enter to display only dynamic multicast entries. If not specified, both static and dynamic entries are displayed.
`switch`		Enter to display the switch name/context name.
`<switch_name>`		Enter a value representing unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.

Parameter	Type	Description
globals		Enter to display IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switches (if switch is not specified). The optional switch name is not applicable for SI case.
switch		Enter to display the switch name/context name.
<switch_name>		Enter a value representing unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.
groups		Enter to display IGMP group information for all VLANs or a specific VLAN or specific VLAN and group address for a given switch or for all switch (if no switch is specified).
vlan <vlan-id/vfi-id>	Integer	Enter to specify IGMP snooping group information for the VLAN / VFI ID to be displayed. This value ranges from 1 to 65535. • <vlan–id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.
Group		Enter to display the multicast group address of the VLAN ID.
<Address>		Enter a value for the multicast group address of the VLAN ID to be displayed.
static		Enter to display only static multicast entries.
dynamic		Enter to display only dynamic multicast entries. If not specified, both static and dynamic entries are displayed.
switch		Enter to display the switch name/context name.
<switch_name>		Enter a value representing unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.
mrouter		Enter for display the router ports for all VLANs or a specific VLAN for a given switch or for all switches (if no switch is specified). The optional switch is not applicable for SI case. The interface details and the corresponding port number along with its type (static/dynamic) are displayed.

Parameter	Type	Description
vlan <vlan-id/vfi-id>	Integer	Enter to specify he router ports for the specified VLAN / VFI ID to be displayed.This value ranges from 1 to 65535. • <vlan–id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535. **NOTE:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries. **NOTE:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW. **NOTE:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
detail		Enter to display detailed information about the router ports.
switch		Enter to display the router ports for the specified context.
<switch_name>		Enter a value representing unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.
multicast-vlan		Enter to display Multicast VLAN statistics for all VLANs or a specific VLAN for a given switch or for all switches (if switch is not specified). The optional switch name is not applicable for SI case.
switch		Enter to display the switch name/context name.
<switch_name>		Enter a value representing unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.
port-cfg		Enter to display IGS port configuration information for all inner VLANs or a specific inner VLAN ID or a given switch.
<interface>		Enter to specify interface to be displayed.

Parameter	Type	Description
<interface-type>		Enter to specify interface type to be displayed. The interface can be: • Gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • Extreme-Ethernet – A version of ethernet that supports data transfer up to 10 Gigabits per second. This ethernet supports only full duplex links. • i-lan – Internal LAN created on a bridge per IEEE 802.1ap.
<interface-id>		Enter to display a specified interface ID. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash for interface type other than i-lan. Only i-lan ID is provided, for interface type i-lan.
InnerVlanId		Enter to specify the Inner VLAN identifier to be displayed.
<VlanId(1-4094)>	Integer	Enter a value for the Inner VLAN identifier to be displayed. This value ranges from 1 to 4094.
switch		Enter to display the switch name/context name.
<switch_name>		Enter a value representing unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.
statistics		Enter to display IGMP snooping statistics for all VLANs or a specific VLAN for a given switch or for all switches (if no switch is specified).
vlan <vlan-id/vfi-id>	Integer	Enter to specify the IGMP snooping statistics for the VLAN / VFI ID to be displayed. This value ranges from 1 to 65535. • <vlan–id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id> - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.
switch		Enter to display the switch name/context name.
<switch_name>		Enter a value representing unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.

Parameter	Type	Description
vlan <vlan-id/vfi-id>	Integer	Enter to specify IGMP snooping information for the VLAN / VFI ID to be displayed.This value ranges from 1 to 65535. • <vlan–id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094. • <vfi-id> - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.
switch		Enter to display the switch name/context name.
<switch_name>		Enter a value representing unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.

Mode

Privileged EXEC Mode

Examples

iS5comm# show ip igmp snooping blocked-router

```
VlanPorts
---------
1Gi0/1, Gi0/2, Gi0/3, Gi0/4
2Gi0/6, Gi0/7, Gi0/8
```

iS5comm# show ip igmp snooping globals

```
Snooping Configuration
----------------------------
IGMP Snooping globally enabled
IGMP Snooping is operationally enabled
IGMP Snooping Enhanced mode is disabled
Transmit Query on Topology Change globally disabled
Multicast forwarding mode is MAC based
Proxy globally disabled
Proxy reporting globally enabled
Filter is disabled
Router port purge interval is 125 seconds
Port purge interval is 260 seconds
Report forward interval is 5 seconds
```

```
    Group specific query interval is 2 seconds
    Reports are forwarded on router ports
    Group specific query retry count is 2
    Multicast VLAN disabled
    Leave config level is Vlan based
```

iS5comm# show ip igmp snooping groups

```
    IGMP Snooping Group information
    -------------------------------
    VLAN ID:2  Group Address: 227.1.1.1
    Filter Mode: EXCLUDE
    Exclude sources: None
    V1/V2 Receiver Ports:
    Gi0/4
    V3 Receiver Ports:
      Port Number: Gi0/2
       Include sources: None
       Exclude sources:
       12.0.0.10, 12.0.0.20
    Port Number: Gi0/3
    Include sources: None
       Exclude sources:
       12.0.0.40, 12.0.0.30
```

iS5comm# show ip igmp snooping mrouter

```
    Vlan   Ports
    -----  ------
        1  Gi0/1(dynamic), Gi0/2(static)
        2  Gi0/1(static), Gi0/2(dynamic)
```

iS5comm# show ip igmp snooping multicast-receivers

```
    Snooping Receiver Information
    -----------------------------
    VLAN ID: 1 Group Address: 225.0.0.10
    Receiver Port: Gi0/2
    Attached Hosts: 12.0.0.10
    Exclude Sources: None
    VLAN ID: 1 Group Address: 225.0.0.20
    Receiver Port: Gi0/2
    Attached Hosts: 12.0.0.20
    Include Sources: 14.0.0.10
    Receiver Port: Gi0/4
    Attached Hosts: 12.0.0.40
```

```
    Include Sources: 14.0.0.20
```

iS5comm# show ip igmp snooping multicast-vlan

```
    Multicast VLAN Statistics
    =========================
    ------------------------------
    Multicast VLAN disabled
    Profile ID -- Multicast VLAN
    ---------- -- --------------
        1      --          1
        2      --          2
    ------------------------------
```

iS5comm# show ip igmp snooping port-cfg

```
    Snooping Port Configurations
    ----------------------------
    Snooping Port Configuration for Port 2
    Leave Process mode is Normal Leave
    Rate limit on the interface is 100
    Max limit Type is Groups
    Max limit is 20
    Current member count is 0
    Profile Id is 0
    Snooping Port Configuration for Port 3
    Leave Process mode is Fast Leave
    Rate limit on the interface is -1
    Max limit Type is Channels
    Max limit is 500
    Current member count is 0
    Profile Id is 0
```

iS5comm# show ip igmp snooping statistics

```
    IGMP Snooping Statistics for VLAN 1
     IGMP Snooping General queries received : 3
     IGMP Snooping Group specific queries received : 0
     IGMP Snooping Group and source specific queries received : 0
     IGMP Snooping V1/V2 reports received : 10
     IGMP Snooping V3 reports received : 0
     IGMP Snooping V3 IS_INCLUDE messages received : 0
     IGMP Snooping V3 IS_EXCLUDE messages received : 0
     IGMP Snooping V3 TO_INCLUDE messages received : 0
     IGMP Snooping V3 TO_EXCLUDE messages received : 0
     IGMP Snooping V3 ALLOW messages received : 0
```

```
IGMP Snooping V3 Block messages received : 0
IGMP Snooping V2 Leave messages received : 0
IGMP Snooping General queries transmitted : 0
IGMP Snooping Group specific queries transmitted : 2
IGMP Snooping V1/V2 reports transmitted : 0
IGMP Snooping V3 reports transmitted : 3
IGMP Snooping V2 leaves transmitted : 0
IGMP Snooping Packets dropped : 1
```

iS5comm# show ip igmp snooping vlan 1

```
Snooping VLAN Configuration for the VLAN 1
  IGMP Snooping enabled  IGMP configured version is V3
  Fast leave is disabled
  Snooping switch is acting as Non-Querier
  Query interval is 125 seconds
  Port Purge Interval is 260 seconds
  Max Response Code is 100, Time is 10 seconds
```

iS5Comm# show ip igmp snooping

NOTE: If a switch is not configured as querier, it will neither send any query, nor will participate in querier election. Hence Elected querier IP is not shown for "Non-querier" switch. Examples of both will be shown with some text put in bold to highlight the differences.

This text below is from a switch which has been configured as a querier.

```
Snooping VLAN Configuration for the VLAN 1
IGMP Snooping enabled
IGMP configured version is V3
Fast leave is disabled
Snooping switch is configured as Querier
Snooping switch is acting as Querier
Elected Querier is 192.168.10.2
Startup Query Count is 2
Startup Query Interval is 31 seconds
Query interval is 125 seconds
Other Querier Present Interval is 255 seconds
Port Purge Interval is 260 seconds
Max Response Code is 100, Time is 10 seconds
```

This text below is from a switch which has been configured as a Non-querier.

```
Snooping VLAN Configuration for the VLAN 1
IGMP Snooping enabled
IGMP configured version is V3
Fast leave is disabled
Snooping switch is configured as Non-Querier
```

```
Snooping switch is acting as Non-Querier
Elected Querier is 0.0.0.0
Startup Query Count is 2
Startup Query Interval is 31 seconds
Query interval is 125 seconds
Other Querier Present Interval is 255 seconds
Port Purge Interval is 260 seconds
Max Response Code is 100, Time is 10 seconds
```

27.9. shutdown snooping

To shut down snooping in the switch, use the command **shutdown snooping** in Global Configuration Mode. When you don't require the IGMP snooping module to be running, it can be shut down. When shut down, all resources acquired by the Snooping Module are released to the system. For the IGS feature to be functional on the switch, the 'system-control' status must be set as 'start' and the 'state' must be 'enabled.'The no form of the command starts and enables IGS snooping in the switch.

shutdown snooping

```
shutdown snooping
```

no shutdown snooping

```
no shutdown snooping
```

Mode

Global Configuration Mode

Default

Snooping is enabled

Prerequisites

Snooping cannot be started in the switch, if the base bridge mode is configured as transparent bridging.

Examples

iS5comm(config)# shutdown snooping

27.10. snooping leave-process

To specify the level of configuring the leave processing mechanisms, use the command **snooping leave-process** in Global Configuration Mode.

snooping leave-process

```
snooping leave-process config-level {vlan | port}
```

Parameters

Parameter	Type	Description
config-level		Enter to specify the level of configuring the leave processing mechanisms. When the switch intercepts a leave group message on a switch port, it normally sends a query to that multicast group through the same switch port. If no hosts respond to the query and no multicast routers have been discovered on the switch port, that port is removed from the multicast group.
vlan		Enter to configure leave processing mechanisms at VLAN level. In VLAN-based leave processing mode, the fast leave functionality configurable per VLAN, or normal leave configurations are available for processing leave messages.
port		Enter to configure the leave processing mechanisms at interface level. In Port-based leave processing mode, the explicit host tracking functionality, the fast leave functionality ,or normal leave configurable on an interface are used for processing the leave messages

Mode

Global Configuration Mode

Default

vlan

Examples

iS5comm(config)# snooping leave-process config-level port

27.11. snooping report-process

To set the level of configuring the report processing mechanisms, use the command **snooping report-process** in Global Configuration Mode.

snooping report-process

```
snooping report-process config-level {non-router-ports | all-ports}
```

Parameters

Parameter	Type	Description
config-level		Enter to set the level of configuring the report processing mechanisms. The report processing mechanism configuration can be set to non-router ports or all ports.
non-router-ports		Enter to configure that the incoming report messages are processed only in the non-router ports. Report message received on the router ports are not processed in this configuration.
all-ports		Enter to configure that the incoming report messages are processed in all ports inclusive of router ports.

Mode

Global Configuration Mode

Default

non-router-ports

Examples

iS5comm(config)# snooping report-process config-level all-ports

RMON

28. RMON

RMON (Remote Monitoring) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data.

The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

28.1. rmon alarm

To set an alarm on a MIB object, use the command **rmon alarm** in Global Configuration Mode. The no form of the command deletes the alarm configured on the MIB object. The Alarm group periodically takes statistical samples from variables in the probe and compares them to thresholds that have been configured.

rmon alarm

```
rmon alarm <alarm number (1-65535)> <mib-object-id (255)>
<sample-interval-time (1-65535)>

 {absolute | delta} rising-threshold <value (0-2147483647)>
<rising-event-number (1-655350)>

 falling-threshold <value (0-2147483647)> [<falling-event-number(1-65535)>]

 [owner <ownername (127)>]
```

no rmon alarm

```
no rmon alarm <alarm number (1-65535)>
```

Parameters

Parameter	Type	Description
<alarm number (1-65535)>	Integer	Enter a value for the statistic during the last sampling period. This value remains available until the current sampling period is completed. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This value is compared with the rising and falling thresholds. This value ranges from 1 to 65535.
<mib-object-id (255)>		Enter a value for the MIB object.
<sample-interval-time (1-65535)>	Integer	Enter a value for an entry in the alarm table. Each such entry defines a diagnostic sample at a particular level for a MIB object in the device. This value ranges from 1 to 65535 seconds.
absolute		Enter to configure comparison of the value of the selected variable with the thresholds at the end of the sampling interval.
delta		Enter to configure subtracting of the value of the selected variable at the last sample from the current value, and the difference is compared with the thresholds at the end of the sampling interval
rising-threshold		Enter to configure the rising threshold value. If the startup alarm is set as Rising alarm or RisingOrFalling alarm and if the configured threshold value is reached, then an alarm is raised. When the current sampled value is greater than or equal to the configured Rising threshold, and the value at the last sampling interval is less than this configured threshold, a single event will be generated
<value (0 - 2147483647)>	Integer	Enter a value for the rising threshold. This value ranges from 0 to 2147483647.
<rising-event-number (1-655350)>	Integer	Enter a value to raise the index of the event, when the Rising threshold is reached. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. This value ranges from 1 to 65535.
falling-threshold		Enter to configure the falling threshold value. If the startup alarm is set as Falling alarm or RisingOrFalling alarm and if the configured threshold value is reached, then an alarm is raised. When the current sampled value is lesser than or equal to the configured Falling threshold, and the value at the last sampling interval is greater than this threshold, a single event will be generated.

Parameter	Type	Description
<value (0 - 2147483647)>	Integer	Enter a value for the falling threshold value. This value ranges from 0 to 2147483647.
<falling-event-number(1-65535)>	Integer	Enter to configure raising of the index of the event when the Falling threshold is reached. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object
owner		Enter for Alarm owner configuration.
<ownername (127)>		Enter a value for the owner's name.

Mode

Global Configuration Mode

Default

By default, the least event number in the event table is assigned for the rising and falling threshold as its event number.

Prerequisites

- RMON events must have been configured
- RMON collection stats must be configured
- we cannot monitor all mib objects through RMON. This will be applicable only to the Ethernet interfaces and VLANs

Examples

iS5comm(config)# rmon alarm 1 1.3.6.1.2.1.16.1.1.1.5.2 1 delta rising-threshold 2 falling-threshold 1

28.2. rmon collection

To enable RMON history collection of interface/ VLAN statistics in the buckets for the specified time interval or statistic collection on the interface /VLAN, use the command **rmon collection** in Interface Configuration Mode / Config VLAN Mode. The no form of the command disables history and statistics collection on the interface/VLAN.

rmon collection

```
rmon collection {history <index (1-65535)> [buckets <bucket-number
(1-65535)>] [interval <seconds (1-3600)>] [owner <ownername (127)>]
 | stats <index (1-65535)> [owner <ownername (127)>]}
```

no rmon collection

```
no rmon collection {history <index (1-65535)> | stats <index (1-65535)>
```

Parameters

Parameter	Type	Description
history		Enter to enable history collection of interface/ VLAN statistics in the buckets for the specified time interval. **NOTE:** In Config VLAN Mode, this command executes only if either VLAN is set as active or if the member ports are associated with the VLAN.
<index (1-65535)>	Integer	Enter a value for the entry in the history control table. Each such entry defines a set of samples at a particular interval for an interface on the device. This value ranges from 1 to 65535.
buckets		Enter to configure he maximum number of buckets desired for the RMON collection history group of statistics. This is the requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this History Control Entry. The polling cycle is the bucket interval where the interface statistics details are stored.
<bucket-number (1-65535)>	Integer	Enter a value for the maximum number of buckets desired for the RMON collection history group of statistics. This value ranges from 1 to 65535. The default is 50.
interval		Enter to configure the time interval over which the data is sampled for each bucket. This value ranges from 1 to 3600. The default is 1800 seconds.
<seconds (1-3600)>	Integer	Enter a value for the time interval over which the data is sampled for each bucket. This value ranges from 1 to 3600.
owner		Enter to configure the name of the owner of the RMON group of statistics.
<ownername (127)>		Enter a value for the name of the owner of the RMON group of statistics.
stats		Enter to enable RMON statistic collection on the interface/ VLAN.
<index (1-65535)>	Integer	Enter a value for the entry in the statistics table. This value ranges from 1 to 65535.
owner		Enter to configure the name of the owner of the RMON group of statistics.
<ownername (127)>		Enter a value for the name of the owner of the RMON group of statistics.

Mode

Interface Configuration Mode / Config VLAN Mode

Examples

iS5comm(config-if)# rmon collection history 1 buckets 2 interval 20

iS5comm(config-if)# rmon collection stats 1

iS5comm(config) vlan 1

iS5comm(config-vlan) rmon collection history 2

iS5comm(config-vlan) rmon collection stats 2

28.3. rmon event

To add an event to the RMON event table, use the command **rmon event** in Global Configuration Mode. The no form of the command deletes an event from the RMON event table. The added event is associated with an RMON event number.

rmon event

```
rmon event <number (1-65535)> [description <event-description (127)>] [log]
[owner <ownername (127)>] [trap <community (127)>]
```

no rmon event

```
no rmon event <number (1-65535)>
```

Parameters

Parameter	Type	Description
<number (1-65535)>	Integer	Enter a value for the number of events to be added in the event table. This value ranges from 1 to 65535.
description		Enter to configure a description for the event.
<event-description (127)>		Enter a value for a description for the event. This value is a string with a maximum length of 127.
log	Integer	Enter to create an entry in the log table for each event.
owner		Enter for event owner configuration.
<ownername (127)>	Integer	Enter a value for the owner name. This value is a string with a maximum value of 127.
trap		Enter to generate a trap. The SNMP community string is to be passed for the specified trap.
<community (127)>		Enter a value for the SNMP community string. This value is a string with a maximum value of 127.

Mode

Global Configuration Mode

Examples

iS5comm(config)# rmon event 1 log owner iS5Com trap netman

28.4. set rmon

To enable or disable the Remote Monitoring (RMON) feature, use the command **set rmon** in Global Configuration Mode.

set rmon

```
set rmon {disable | enable}
```

Parameters

Parameter	Type	Description
disable		Enter to disable the RMON feature in the system. Upon disabling, the RMON's network monitoring is called off. This is default.
enable		Enter to enable the RMON feature in the system. Upon enabling, the RMON starts monitoring both local and remote networks and provides network fault diagnosis.

Mode

Global Configuration Mode

Default

disable

Examples

iS5comm(config)# set rmon enable

28.5. show rmon

To display the RMON statistics, alarms, events, and history configured on the interface, use the command **show rmon** in Privileged EXEC Mode.

show rmon

```
show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events] [history
[<history-index (1-65535)>] [overview]]
```

Parameters

Parameter	Type	Description
statistics		Enter to specify a collection of statistics for a particular Ethernet Interface. to be displayed.
<stats-index (1-65535)>	Integer	Enter a value for the a collection of statistics for a particular Ethernet Interface to be displayed.
alarms		Enter to specify the value of the statistic during the last sampling period to be displayed. This value remains available until the current sampling period is completed.
events		Enter to generate events whenever an associated condition takes place in the device to be displayed. The Conditions may be alarms. Alarms are generated when a sampled statistical variable value exceeds the defined threshold value. Alarm module calls events module.
history		Enter to specify the history of the configured RMON to be displayed.
<history-index (1-65535)>	Integer	Enter a value for the history of the configured RMON to be displayed.
overview		Enter to specify only the overview of RMON history entries to be displayed.

Mode

Privileged EXEC Mode

Examples

iS5comm# show rmon statistics

```
RMON is enabled
Collection 1 on Gi0/1 is active, and owned by monitor,
 Monitors ifEntry.1.1 which has
 Received 0 octets,0 packets,
 0 broadcast and 0 multicast packets,
 0 undersized and 0 oversized packets,
 0 fragments and 0 jabbers,
 0 CRC alignment errors and 0 collisions.
 0 out FCS errors and 0 Drop events,
```

```
 # of packets received of length (in octets):
 64: 0, 65-127: 0, 128-255: 0,
 256-511: 0, 512-1023: 0, 1024-1518: 0, 1519-1522: 0
Collection 2 on Vlan 1 is active, and owned by monitor,
 Monitors Vlan 1 which ha
s Received 0 octets, 0 packets,
 0 broadcast and 0 multicast packets,
 0 undersized and 0 oversized packets,
 0 fragments and 0 jabbers,
 0 CRC alignment errors and 0 collisions.
 0 out FCS errors and 0 Drop events,
 # of packets received of length (in octets):
 64: 0, 65-127: 0, 128-255: 0,
 256-511: 0, 512-1023: 0, 1024-1518: 0,
 1519-1522: 0
Number of statistics collection on interface: 1
Number of statistics collection on Vlan     : 1
```

show rmon

```
RMON is enable
```

iS5comm# show rmon history

```
RMON is disabled
Entry 1 is active,  and owned by monitor
 Monitors ifEntry.1.2 every 1800 second(s)
 Requested # of time intervals, i.e. buckets, is 50,
 Granted # of time intervals, i.e. buckets, is 50,Entry 4 is active,
and owned by monitor
 Monitors Vlan 40 every 1800 second(s)
 Requested # of time intervals, i.e. buckets, is 50,
 Granted # of time intervals, i.e. buckets, is 50,
Number of history collection on interface: 1
Number of history collection on Vlan     : 1
```

iS5comm# show rmon event

```
RMON is enabled
Entry 1 is active,  and owned by monitor
 Monitors ifEntry.1.1 every 20 second(s)
 Requested # of time intervals, i.e. buckets, is 2,
 Granted # of time intervals, i.e. buckets, is 2,
  Sample 16 began measuring at Jun  5 21:46:34 2019
   Received 0 octets, 0 packets,
   0 broadcast and 0 multicast packets,
```

```
    0 undersized and 0 oversized packets,
    0 fragments and 0 jabbers,
    0 CRC alignment errors and 0 collisions,
    # of dropped packet events is 0
    Network utilization is estimated at 0
   Sample 17 began measuring at Jun  5 21:46:54 2019
    Received 0 octets, 0 packets,
    0 broadcast and 0 multicast packets,
    0 undersized and 0 oversized packets,
    0 fragments and 0 jabbers,
    0 CRC alignment errors and 0 collisions,
    # of dropped packet events is 0
    Network utilization is estimated at 0
Number of history collection on interface: 1
```

iS5comm# show rmon alarms

```
RMON is enabled
Alarm 1 is active,  owned by
 Monitors 1.3.6.1.2.1.16.1.1.1.5.2 every 1 second(s)
 Taking delta samples, last value was 0
 Rising threshold is 2, assigned to event 1
 Falling threshold is 1, assigned to event 1
 On startup enable rising or falling alarm
```

iS5comm# show rmon statistics 2 alarms events history 1

```
RMON is enabled
Collection 2 on Vlan 1 is active, and owned by monitor,
 Monitors Vlan 1 which has
 Received 0 octets, 0 packets,
 0 broadcast and 0 multicast packets,
 0 undersized and 0 oversized packets,
 0 fragments and 0 jabbers,
 0 CRC alignment errors and 0 collisions.
 0 out FCS errors and 0 Drop events,
 # of packets received of length (in octets):
 64: 0, 65-127: 0, 128-255: 0, 256-511: 0,
 512-1023: 0, 1024-1518: 0, 1519-1522: 0
Alarm table is empty
Event table is empty
Entry 1 is active,  and owned by monitor
 Monitors ifEntry.1.1 every 20 second(s)
 Requested # of time intervals, i.e. buckets, is 2,
```

```
 Granted # of time intervals, i.e. buckets, is 2,
  Sample 20 began measuring at Jun  5 21:47:55 2019
   Received 0 octets, 0 packets,
   0 broadcast and 0 multicast packets,
   0 undersized and 0 oversized packets,
   0 fragments and 0 jabbers,
   0 CRC alignment errors and 0 collisions,
   # of dropped packet events is 0
   Network utilization is estimated at 0
  Sample 21 began measuring at Jun  5 21:48:15 2019
   Received 0 octets, 0 packets,
   0 broadcast and 0 multicast packets
,    0 undersized and 0 oversized packets,
   0 fragments and 0 jabbers,
   0 CRC alignment errors and 0 collisions,
   # of dropped packet events is 0
   Network utilization is estimated at 0
```

iS5comm# show rmon history overview

```
RMON is enabled
Entry 1 is active,  and owned by monitor
 Monitors ifEntry.1.1 every 20 second(s)
 Requested # of time intervals, i.e. buckets, is 2,
 Granted # of time intervals, i.e. buckets, is 2,
Number of history collection on interface: 1
```

QoS

29. QoS

QoS (Quality of Service) defines the ability to provide different priorities to different applications, users or data flows or the ability to guarantee a certain level of performance to a data flow. QoS refers to resource reservation control mechanisms rather than the achieved service quality and specifies a guaranteed throughput level.

Raptor's QoS provides a complete Quality of Service solution across VPNs and helps in implementing service provisioning policies for application or customers, who desire to have an enhanced performance for their traffic on the Internet.

29.1. class-map

To add a class-map entry, use the command **class-map** in Global Configuration Mode. The no form of the command deletes a class map entry.

class-map

```
class-map <class-map-Id(1-65535)>
```

no class-map

```
no class-map <class-map-Id(1-65535)>
```

Parameters

Parameter	Type	Description
<class-map-Id (1-65535)>	Integer	Enter a value for a priority map entry. It configures an index that enumerates the Multi Field Classifier table entries. This value ranges from 1 to 65535.

Mode

Global Configuration Mode

Prerequisites

- This command executes only if QoS is started in the system.

Examples

iS5comm(config)# class-map 1

iS5comm(config-cls-map)#

29.2. clear meter-stats

To clear the meter statistics counter, use the command **clear meter-stats** in Privileged EXEC Mode.

clear meter-stats

```
clear meter-stats [meter-id [<integer (1-65535)>]
```

Parameters

Parameter	Type	Description
meter-id		Enter to specify an index that enumerates the meter entries.
<integer(1-65535)>	Integer	Enter a value for the index that enumerates the meter entries. The value ranges from 1 to 65535.

Mode

Privileged EXEC Mode

Prerequisites

To clear meter statistics for a specific meter-id, a Meter id and a policy map related configuration should be already created.

Examples

iS5comm# clear meter-stats meter-id 1

29.3. debug qos

To set the debug levels for QoS module, use the command **debub qos** in Privileged EXEC Mode. The no form of the command resets the debug level for QoS module.

debug qos

```
debug qos {initshut | mgmt | ctrl | dump | os | failall | buffer}
```

no debug qos

```
no debug qos {initshut | mgmt | ctrl | dump | os | failall | buffer}
```

Parameters

Parameter	Type	Description
initshut		Enter to generate debug statements for Init and shutdown traces.
mgmt		Enter to generate debug statements for Management traces.
ctrl		Enter to generate debug statements for Control plane traces.
dump		Enter to generate debug statements for Packet dump traces.
os		Enter to generate debug statements for traces related to all resources except buffers.
failall		Enter to generate debug statements for all failure traces.
buffer		Enter to generate debug statements for buffer allocation / release traces.

Mode

Privileged EXEC Mode

Examples

iS5comm# debug qos initshut

29.4. map

To add a priority map entry for mapping an incoming priority to a regenerated priority, use the command **map** in Priority Map Configuration Mode. The no form of the command sets a default value for the Interface, VLAN, and regenerated inner priority.

map

```
map {interface <iftype> <ifnum> | in-priority-type {vlanPri | dot1P
<integer(0-1)> | ipDscp} in-priority <integer(0-63)> regen-priority
<integer(0-63)> [regen-color {green | yellow | red}]
```

no map

```
no map {interface | vlan | regen-inner-priority}
```

Parameters

Parameter	Type	Description
interface		Enter to configure type of interface for the outbound queue.
<iftype>		Enter to configure an interface type. Supports everything except port-channel. The options are: • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
<ifnum>		Enter to configure he type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface types internal-lan.
in-priority-type		Enter to configure the incoming priority type for the specified interface.
vlanPri		Enter to set the priority type to VLAN Priority. vlan - 0. This is default.
dot1P		Enter to configure VLAN Drop Eligibility Indicator.
<integer(0-1)>	Integer	Enter a value for the VLAN Drop Eligibility Indicator. This value ranges from 0 to 1.
ipDscp		Enter to set the priority type to IP Differentiated Services Code Point
in-priority		Enter to configure the Incoming priority value determined for the received frame. Incoming priority value determined for the received frame.(0-63) range is split into (0-7) for vlanPri, (0-63) for ipDscp.
<integer(0-63)>	Integer	Enter a value for the Incoming priority value determined for the received frame. This value ranges from 0 to 63. The default is 1.
regen-priority		Enter to configure regenerated priority value determined for the received frame.
<integer(0-63)>	Integer	Enter a value for regenerated priority value determined for the received frame. This value ranges from 0 to 63. The default is 0.

Parameter	Type	Description
regen-color		Enter to configure the type of the regenerated color.
green		Enter to indicate Conform Action.
yellow		Enter to indicate Exceed Action
red		Enter to indicate Violate Action.

Mode

Priority Map Configuration Mode

Prerequisites

Priority Map entry must be created.

Examples

iS5comm(config)# priority-map 1

iS5comm(config-pri-map)# map interface gi 0/1 in-priority-type vlanPri in-priority 0 regen-priority 7

29.5. match access-group

To sets class map parameters using L2 and/or L3 access control list (ACL) or priority map ID, use the command **match access-group** in Class Map Configuration Mode.

match access-group

```
match access-group mac-access-list <integer(0-65535)> | ip-access-list
<integer(1-65535)> | priority-map <integer(0-65535)>
```

Parameters

Parameter	Type	Description
mac-access-list		Enter to configure identifier of the MAC filter
<integer(0-65535)>	Integer	Enter a value for the Identifier of the MAC filter. This value ranges from 0 to 65535. The default is 0.
ip-access-list		Enter to configure the identifier of the IP filter.
<integer(0-65535)>	Integer	Enter a value for the identifier of the IP filter. This value ranges from 1 to 65535. The default is 0
priority-map		Enter to configure the priority map identifier for mapping incoming priority against received packet.
<integer(0-65535)>	Integer	Enter a value for the priority map identifier for mapping incoming priority against received packet. This value ranges from 1 to 65535. The default is 0

Mode

Class Map Configuration Mode

Examples

iS5comm(config)# class-map 1

iS5comm(config-cls-map)# match access-group priority-map 1

29.6. meter

To create a meter, use the command **meter** in Global Configuration Mode. The no form of the command deletes a meter.

meter

```
meter <meter-Id(1-1000)>
```

no meter

```
no meter <meter-Id(1-1000)>
```

Parameters

Parameter	Type	Description
<meter-Id(1-1000)>	Integer	Enter a value for meter. Configures an Index that enumerates the meter entries. This value ranges from 1 to 65535.

Mode

Global Configuration Mode

Prerequisites

- This command executes only if QoS is started in the system.

Examples

iS5comm(config)# meter 1

iS5comm(config-meter)#

29.7. meter-type

To set meter parameters CIR, CBS, EIR, EBS, meter type, and color awareness, use the command **meter-type** in Meter Configuration Mode.

meter-type

```
meter-type {srTCM | trTCM} [color-mode {aware | blind}] [cir
<integer(0-10485760)>] [cbs <integer(0-10485760)>] [eir
<integer(0-10485760)>] [ebs <integer(0-10485760)>]
```

Parameters

Parameter	Type	Description
srTCM		Enter to configure the meter type as single rate three color marker (srTCM) metering as defined by RFC 2697. Valid parameters supported are cir, cbs, and ebs.
trTCM		Enter to configure the meter type as two rate three color marker (trTCM) metering as defined by RFC 2698. Valid values for given meter type are CIR, CBS, EIR, and EBS.
color-mode		Enter to configure the color mode of the meter.
aware		Enter to indicate that the meter considers the pre-color of the packet.
blind		Enter to indicate that the meter ignores the pre-color of the packet. This is the default.
cir		Enter to configure the committed information rate (cir). Cir should be less than excess information rate (eir).
<integer(0-10485760)>	Integer	Enter a value for the committed information rate. This value ranges from 0 to 10485760.
cbs		Enter to configure the committed burst size (cbs).
<integer(0-10485760)>	Integer	Enter a value for the he committed burst size. This value ranges from 0 to 10485760.
eir		Enter to configure the excess information rate (eir).
<integer(0-10485760)>	Integer	Enter a value for the excess information rate. This value ranges from 0 to 10485760.
ebs		Enter to configure the excess burst size (ebs).
<integer(0-10485760)>	Integer	Enter a value for the excess burst size. This value ranges from 0 to 10485760.

Mode

Meter Configuration Mode

Prerequisites

Meter should have been created.

Examples

iS5comm(config)# meter 1

iS5comm(config-meter)# meter-type srTCM cir 20 cbs 20 ebs 20

29.8. mls qos

To enables multilayer security (mls) QoS, define an aggregate policer ,and configure the policer parameters., use the command **mls qos** in Global Configuration Mode. This command is a standardized implementation of the existing command “set meter” and operates similarly. The no form of the command disables the multilayer security QoS

mls qos

```
mls qos [aggregate-policer [<meter-id (1-65535)>] [<Bits per
second(1-65535)>] [<Normal burst bytes(1-65535)>] exceed-action {drop |
set-ip-dscp-transmit}]
```

no mls qos

```
no mls qos
```

Parameters

Parameter	Type	Description
aggregate-policer		Enter to configure the meter table identifier which is the index for the meter table.
<meter-id(1-65535)>	Integer	Enter a value for the meter table identifier. The value ranges from 1 to 65535.
<Bits per second(1-65535)>	Integer	Enter a value for the average traffic rate in bits per second. This value ranges from 1 to 65535.
<Normal burst bytes(1-65535)>	Integer	Enter a value for the normal burst size in bytes. The value ranges from 1 to 65535.
exceed-action		Enter to configure the action to be performed on the packet, when the packets are found to be In profile (exceed).
drop		Enter to configure dropping of the packet.
set-ip-dscp-transmit		Enter to configure to change the (Differentiated Services Code Point) DSCP of the packet to that specified in policed DSCP map.

Mode

Global Configuration Mode

Examples

iS5comm(config)# mls qos

iS5comm(config)# mls qos aggregate-policer 1 10 10 exceed-action drop

29.9. policy-map

To create a policy map, use the command **priority-map** in Global Configuration Mode. The no form of the command deletes a policy map.

policy-map

```
policy-map <policy-map-Id(1-65535)>
```

no policy-map

```
no policy-map <policy-map-Id(1-65535)>
```

Parameters

Parameter	Type	Description
<policy-map-Id (1-65535)>	Integer	Enter a value for a priority. It configures an index that enumerates the policy-map table entries. This value ranges from 1 to 65535.

Mode

Global Configuration Mode

Prerequisites

- This command executes only if QoS is started in the system.

Examples

iS5comm(config)# policy-map 1

iS5comm(config-ply-map)#

29.10. priority-map

To add a priority map entry, use the command **priority-map** in Global Configuration Mode. The no form of the command deletes a priority map entry.

priority-map

```
priority-map <priority-map-Id(1-65535)>
```

no priority-map

```
no priority-map <priority-map-Id(1-65535)>
```

Parameters

Parameter	Type	Description
<priority-map-Id(1-65535)>	Integer	Enter a value for a priority map entry. It configures the priority map index for the incoming packets received over ingress Port/VLAN with specified incoming priority. This value ranges from 1 to 65535.

Mode

Global Configuration Mode

Prerequisites

- This command executes only if QoS is started in the system.

Examples

iS5comm(config)# priority-map 1

iS5comm(config-pri-map)#

29.11. qos pbit-preference

To set pbit preference value, use the command **qos pbit-preferenc**e in Interface Configuration Mode.

qos pbit-preference

```
qos pbit-preference {disable | enable}
```

Parameters

Parameter	Type	Description
disable		Enter to disable the feature. This is default.
enable		Enter to enable the feature. Setting this to enable indicates that if a frame includes both 802.1p and a DSCP field, then the “pbit” field takes precedence. For DSCP to take precedence, change to disable.

Mode

Interface Configuration Mode

Default

disable

Examples

iS5comm(config-if)# qos pbit-preference enable

29.12. qos

To enable or disable the Quality of Service (QoS) subsystem, use the command **qos** in Global Configuration Mode.

qos

```
qos {disable | enable}
```

Parameters

Parameter	Type	Description
`disable`		Enter to disable the QoS subsystem
`enable`		Enter to enable the QoS subsystem. This is default.

Mode

Global Configuration Mode

Default

Enabled

Prerequisites

- This command executes only when QoS is started in the system.
- QoS module programs the hardware and starts protocol operation, when set as enable.
- QoS module stops protocol operation by deleting the hardware configuration, when set as disabled.

Examples

iS5comm(config)# qos enable

29.13. queue

To create a queue and configure the queue parameters, use the command **queue** in Global Configuration Mode. The no form of the command deletes a queue.

queue

```
queue {<integer(1-8)> interface <iftype> <ifnum> [qtype <integer(1-65535)>]
[scheduler <integer(1-8)>] [weight <integer(1-1000)>] [priority
<integer(0-15)>] [queue-type {unicast | multicast}]
 | class <class (1-65535)> | queue-id <queue-id (1-65535)>
```

no queue

```
no queue <integer(1-65535)> interface <iftype> <ifnum>
```

Parameters

Parameter	Type	Description
<integer(1-8)>	Integer	Enter to create a queue and configure the queue parameters
interface		Enter to configure a specified interface.
<iftype>		Enter to configure an interface type. Supports everything except port-channel.
<ifnum>		Enter to configure an Interface number.
qtype		Enter for queue template type related configuration.
<integer(1-65535)>	Integer	Enter a value for queue template type. This value ranges from 0 to 65535.
scheduler		Enter to configure scheduler identifier that manages the specified queue.
<integer(1-8)>	Integer	Enter a value for scheduler identifier that manages the specified queue. This value ranges from 1 to 8.
weight		Enter for user assigned weight to the CoS queue.
<integer(0-1000)>	Integer	Enter a value for user assigned weight to the CoS queue. This value ranges from 0 to 1000. The default is 0.
priority		Enter for priority related configuration.
<integer(0-15)>	Integer	Enter a value for priority. This value ranges from 0 to 15.
queue-type		Enter a value for Queue template type related configuration
unicast		Enter for unicast (UC) queue to store known unicast packets.
multicast		Enter a multicast (MC) queue to store DLF, multicast, broadcast and mirrored packets
class		Enter to configure input class that should be mapped to anoutbound queue.
<class (1-65535)>	Integer	Enter a value for the input class (associated with an incoming packet) that should be mapped to an outbound queue. This value ranges from 0 to 65535.
queue-id		Enter to configure Queue identifier.
<cqueue-id (1-65535)>	Integer	Enter a value for Queue identifier that uniquely identifiesthe queue relative to an interface. This value ranges from 0 to 65535.

Mode

Global Configuration Mode

Prerequisites

- scheduler identifier is unique relative to an egress interface.
- User assigned weights are used only when scheduling algorithm is a weighted scheduling algorithm.
- User assigned priority is used only when the scheduler uses a priority based scheduling algorithm.

Examples

iS5comm(config)# queue 1 interface gigabitethernet 0/1 scheduler 1 weight 20 shaper 1

29.14. queue-map

To create a map for a queue with class or regenerated priority, use the command **queue-map** in Global Configuration Mode. The no form of the command deletes a queue-map entry.

queue-map

```
queue-map CLASS <integer(1-65535)> queue-id <integer(1-65535)>
```

no queue-map

```
no queue-map CLASS <integer(1-65535)>
```

Parameters

Parameter	Type	Description
CLASS		Enter to configure the Input CLASS (associated with an incoming packet) that needs to be mapped to an outbound queue. **NOTE:** Class needs to be created using the set class command to configure this parameter.
<integer(1-65535)>	Integer	Enter a value for the Input CLASS. This value ranges from 1 to 65535.
queue-id		Enter to configure the queue identifier that uniquely identifies a queue relative to an interface.
<integer(1-65535)>	Integer	Enter a value for the queue identifier that uniquely identifies a queue relative to an interface. This value ranges from 1 to 65535.

Mode

Global Configuration Mode

Prerequisites

- This command executes only if QoS is started in the system.

Examples

iS5comm(config)# queue-map CLASS 2 queue-id 20

29.15. scheduler

To create a scheduler and configure the scheduler parameters, use the command **scheduler** in Global Configuration Mode. The no form of the command deletes a scheduler.

scheduler

```
scheduler <integer(1-8)> interface <iftype> <ifnum> [sched-algo
{strict-priority | rr | wrr}]
```

no scheduler

```
no scheduler <integer(1-65535)> interface <iftype> <ifnum>
```

Parameters

Parameter	Type	Description
<integer(1-8)>	Integer	Enter a value for the scheduler identifier that uniquely identifies the scheduler in the system/egress interface. Use values from 1 to 8 as scheduler ID. An error message is displayed for any scheduler ID beyond this range.
interface		Enter to configure a specified interface.
<iftype>		Enter to configure an interface type. Supports everything except port-channel.
<ifnum>		Enter to configure an Interface number.
sched-algo		Enter to configure a packet scheduling algorithm for the port.
strict-priority		Enter to configure a Strict scheduling algorithm. This is the default scheduling algorithm.
rr		Enter to configure round Robin (rr) algorithm.
wrr		Enter to configure a weighted Round Robin (wrr) algorithm.

Mode

Global Configuration Mode

Examples

iS5comm(config)# scheduler 8 interface gigabitethernet 0/1 sched-algo rr

29.16. set class

To set class for L2 and/or L3 filters or priority map ID and add a class to priority map entry with regenerated priority, use the command **set class** in Class Map Configuration Mode. The no form of the command deletes a CLASS to priority map table entry.

set class

```
set class <class integer(0-65535)> [pre-color {green | yellow | red | none}]
```

no set class

```
no set class <class integer(0-65535)>
```

Parameters

Parameter	Type	Description
<class integer(0-65535)>	Integer	Enter a value for the Traffic CLASS to which an incoming frame pattern is classified. The default is 0.
pre-color		Enter to configure the color of the packet prior to metering.
green		Enter to indicate Traffic conforming to SLAs (Service Level Agreements.
yellow		Enter to indicate Traffic exceeding the SLAs
red		Enter to indicate Traffic violating the SLAs.
none		Enter to indicate Traffic is not pre-colored.

Mode

Class Map Configuration Mode

Examples

iS5comm(config)# class-map 1

iS5comm(config-cls-map)# set class 1000 pre-color none

29.17. set meter

To set policy parameters such as meter and meter actions, use the command **set meter** in Global Configuration Mode. The no form of the command deletes the meter from the policy and the meter actions.

set meter

```
set meter <integer (1-65535)>
 [conform-action [cos-transmit-set <short(0-7)> | de-transmit-set
<short(0-1)> | set-cos-transmit <short(0-7)> | set-de-transmit <short(0-1)>
|set-port <iftype> <ifnum> | inner-vlan-pri-set <short(0-7)>
|inner-vlan-de-set <short(0-1)> |set-inner-vlan-pri <short(0-7)> |
set-inner-vlan-de <short(0-1)> | set-mpls-exp-transmit <short(0-7)>
|set-ip-prec-transmit <short(0-7)> | set-ip-dscp-transmit <short(0-63)>]
```

```
 [exceed-action [drop | cos-transmit-set <short(0-7)> | de-transmit-set
<short(0-1)> | set-cos-transmit <short(0-7)> | set-de-transmit <short(0-1)>
| inner-vlan-pri-set <short(0-7)> | inner-vlan-de-set <short(0-1)> |
set-inner-vlan-pri <short(0-7)> | set-inner-vlan-de <short(0-1)> |
set-mpls-exp-transmit <short(0-7)> | set-ip-prec-transmit <short(0-7)> |
set-ip-dscp-transmit <short(0-63)>]

 [set-conform-newclass <integer (1-65535)>]

 [set-exceed-newclass <integer (1-65535)>]

 [set-violate-newclass <integer (1-65535)>]

 [violate-action [drop | cos-transmit-set <short(0-7)> | de-transmit-set
<short(0-1)> | set-cos-transmit <short(0-7)> | set-de-transmit <short(0-1)>
| inner-vlan-pri-set <short(0-7)> | inner-vlan-de-set <short(0-1)> |
set-inner-vlan-pri <short(0-7)> | set-inner-vlan-de <short(0-1)> |
set-mpls-exp-transmit <short(0-7)> | set-ip-prec-transmit <short(0-7)> |
set-ip-dscp-transmit <short(0-63)>]
```

no set meter

```
no set meter
```

Parameters

Parameter	Type	Description
<integer(1-65535)>	Integer	Enter a value for the meter table identifier which is the index for the meter table. The value ranges from 1 to 65535.
conform-action		Enter to configure action to be performed on the packet, when the packets are found to be In profile (conform).
cos-transmit-set		Enter to set the VLAN priority of the outgoing packet.
<short(0-7)>		Enter a value to set the VLAN priority of the outgoing packet. The value ranges from 0 to 7.
de-transmit-set		Enter to set the VLAN drop eligible indicator of the outgoing packet.
<short(0-1)>	Integer	Enter a value for the VLAN drop eligible indicator of the outgoing packet. The value ranges from 0 to 1.
set-cos-transmit		Enter to set the VLAN priority of the outgoing packet.
<short(0-7)>	Integer	Enter a value to set the VLAN priority of the outgoing packet. The value ranges from 0 to 7.
set-de-transmit		Enter to set the VLAN drop eligible indicator of the outgoing packet.
<short(0-1>)	Integer	Enter a value for the VLAN drop eligible indicator (DE) of the outgoing packet. The value ranges from 0 to 1.
set-port		Enter to set new port value.
<iftype>		Enter to set the interface type.
<ifnum>		Enter a set the interface type
inner-vlan-pri-set		Enter to set the inner VLAN priority of the outgoing packet.
<short(0-7)>	Integer	Enter a value to set the inner VLAN priority of the outgoing packet. The value ranges from 0 to 7.
inner-vlan-de-set		Enter to set the inner VLAN DE of the outgoing packet.
<short(0-1)>	Integer	Enter a value for the inner VLAN DE of the outgoing packet. The value ranges from 0 to 1.
set-inner-vlan-pri		Enter to set the inner VLAN priority of the outgoing packet.
<short(0-7)>	Integer	Enter a value to set the VLAN priority of the outgoing packet. The value ranges from 0 to 7.
set-inner-vlan-de		Enter to set the inner VLAN DE of the outgoing packet.

Parameter	Type	Description
<short(0-1)>	Integer	Enter a value for the VLAN DE of the outgoing packet. The value ranges from 0 to 1.
set-mpls-exp-transmit		Enter to set the MPLS experimental bits of the outgoing packet.
<short(0-7)>	Integer	Enter a value to set the MPLS experimental bits of the outgoing packet. The value ranges from 0 to 7.
set-ip-prec-transmit		Enter to set the new IP Type of Service.
<short(0-7)>	Integer	Enter a value for new IP Type of Service. It ranges from 0 to 1.
set-ip-dscp-transmit		Enter to set the new DSCP.
<short(0-63)>	Integer	Enter a value to set the new DSCP. The value ranges from 0 to 7.
exceed-action		Enter to configure the action to be performed on the packet, when the packets are found to be In profile (exceed)
drop		Enter to drop the packet.
cos-transmit-set		Enter to set the VLAN priority of the outgoing packet.
<short(0-7)>	Integer	Enter a value to set the VLAN priority of the outgoing packet. The value ranges from 0 to 7.
de-transmit-set		Enter to set the VLAN drop eligible indicator of the outgoing packet.
<short(0-1)>	Integer	Enter a value for the VLAN drop eligible indicator of the outgoing packet. The value ranges from 0 to 1.
set-cos-transmit		Enter to set the VLAN priority of the outgoing packet.
<short(0-7)>	Integer	Enter a value to set the VLAN priority of the outgoing packet. The value ranges from 0 to 7.
set-de-transmit		Enter to set the VLAN drop eligible indicator of the outgoing packet.
<short(0-1)>	Integer	Enter a value for the VLAN drop eligible indicator (DE) of the outgoing packet. The value ranges from 0 to 1.
inner-vlan-pri-set		Enter to set the inner VLAN priority of the outgoing packet.
<short(0-7)>	Integer	Enter a value to set the inner VLAN priority of the outgoing packet. The value ranges from 0 to 7.

Parameter	Type	Description
inner-vlan-de-set		Enter to set the inner VLAN DE of the outgoing packet.
<short(0-1)>		Enter a value for the inner VLAN DE of the outgoing packet. The value ranges from 0 to 1.
set-inner-vlan-pri	Integer	Enter to set the inner VLAN priority of the outgoing packet.
<short(0-7)>		Enter a value to set the VLAN priority of the outgoing packet. The value ranges from 0 to 7.
set-inner-vlan-de		Enter to set the inner VLAN DE of the outgoing packet.
<short(0-1)>		Enter a value for the VLAN DE of the outgoing packet. The value ranges from 0 to 1.
set-mpls-exp-transmit	Integer	Enter to set the MPLS experimental bits of the outgoing packet.
<short(0-7)>		Enter a value to set the MPLS experimental bits of the outgoing packet. The value ranges from 0 to 7.
set-ip-prec-transmit		Enter to set the new IP Type of Service.
<short(0-7)>		Enter a value for new IP Type of Service. It ranges from 0 to 1.
set-ip-dscp-transmit	Integer	Enter to set the new DSCP.
<short(0-63)>		Enter a value to set the new DSCP. The value ranges from 0 to 7.
set-conform-newclass		Enter to represent the Traffic class to which an incoming frame pattern is classified after metering.
<integer(0-65535)>		Enter a value the Traffic class to which an incoming frame pattern is classified after metering. The value ranges from 0 to 65535.
set-exceed-newclass		Enter to represent the Traffic class to which an incoming frame pattern is classified after metering.
<integer(0-65535)>		Enter a value the Traffic class to which an incoming frame pattern is classified after metering. The value ranges from 0 to 65535.
set-violate-newclass		Enter to represent the Traffic class to which an incoming frame pattern is classified after metering.

Parameter	Type	Description
<integer(0-65535)>	Integer	Enter a value the Traffic class to which an incoming frame pattern is classified after metering. The value ranges from 0 to 65535.
violate-action		Enter to configure the action to be performed on the packet, when the packets are found to be out of profile (violate).
drop		Enter to drop the packet.
cos-transmit-set		Enter to set the VLAN priority of the outgoing packet.
<short(0-7)>	Integer	Enter a value to set the VLAN priority of the outgoing packet. The value ranges from 0 to 7.
de-transmit-set		Enter to set the VLAN drop eligible indicator of the outgoing packet.
<short(0-1)>	Integer	Enter a value for the VLAN drop eligible indicator of the outgoing packet. The value ranges from 0 to 1.
set-cos-transmit		Enter to set the VLAN priority of the outgoing packet.
<short(0-7)>	Integer	Enter a value to set the VLAN priority of the outgoing packet. The value ranges from 0 to 7.
set-de-transmit		Enter to set the VLAN drop eligible indicator of the outgoing packet.
<short(0-1)>		Enter a value for the VLAN drop eligible indicator (DE) of the outgoing packet. The value ranges from 0 to 1.
inner-vlan-pri-set		Enter to set the inner VLAN priority of the outgoing packet.
<short(0-7)>	Integer	Enter a value to set the inner VLAN priority of the outgoing packet. The value ranges from 0 to 7.
inner-vlan-de-set		Enter to set the inner VLAN DE of the outgoing packet.
<short(0-1)>	Integer	Enter a value for the inner VLAN DE of the outgoing packet. The value ranges from 0 to 1.
set-inner-vlan-pri		Enter to set the inner VLAN priority of the outgoing packet.
<short(0-7)>	Integer	Enter a value to set the VLAN priority of the outgoing packet. The value ranges from 0 to 7.
set-inner-vlan-de		Enter to set the inner VLAN DE of the outgoing packet.
<short(0-1)>		Enter a value for the VLAN DE of the outgoing packet. The value ranges from 0 to 1.

Parameter	Type	Description
set-mpls-exp-transmit		Enter to set the MPLS experimental bits of the outgoing packet.
<short(0-7)>	Integer	Enter a value to set the MPLS experimental bits of the outgoing packet. The value ranges from 0 to 7.
set-ip-prec-transmit		Enter to set the new IP Type of Service.
<short(0-7)>	Integer	Enter a value for new IP Type of Service. It ranges from 0 to 1.
set-ip-dscp-transmit		Enter to set the new DSCP.
<short(0-63)>	Integer	Enter a value to set the new DSCP. It ranges from 0 to 7.

Mode

Policy Map Configuration Mode

Defaults

- set-cos-transmit - 0
- set-de-transmit - 0
- set-mpls-exp-transmit - 0
- set-inner-vlan-pri - 0

Prerequisites

VLAN priority can be set to a non-zero value only when MPLS Experimental bits is set to zero.

Examples

iS5comm(config)# policy-map 1

iS5comm(config-ply-map)# set meter 10 conform-action cos-transmit-set 5 exceed-action cos-transmit-set 5 set-conform-newclass 100 set-exceed-newclass 100 set-violate-newclass 10

29.18. set meter-stats

To set the meter statistics counter status, use the command **set meter-stats** in Global Configuration Mode.

set meter-stats

```
set meter-stats {disable | enable} [meter-id [<integer (1-65535)>]
```

Parameters

Parameter	Type	Description
disable		Enter to disable counter status for the meter statistics.
enable		Enter to enable counter status for the meter statistics.
meter-id		Enter to specify an index that enumerates the meter entries.
<integer(1-65535)>	Integer	Enter a value for the index that enumerates the meter entries. The value ranges from 1 to 65535.

Mode

Global Configuration Mode

Prerequisites

To enable or disable meter statistics to a specific meter-id, Meter id and policy map related configuration should be already created.

Examples

iS5comm(config)# set meter-stats enable meter-id 1

29.19. set policy

To set a class for policy, use the command **set policy** in Priority Map Configuration Mode. The no form of the command sets the default value for interface in this policy.

set policy

```
set policy [class <integer(0-65535>] {interface <iftype> <ifnum>
default-priority-type {none | vlanPri <integer(0-7)> | dot1P <integer<0-7)>
<integer<0-1)> | ipDscp <integer(0-63)>}}
```

no set policy

```
no set policy interface
```

Parameters

Parameter	Type	Description
class		Enter to specify the Traffic class for which the policy-map needs to be applied. **NOTE:** Class needs to be created using the set class command to configure this parameter.
<integer(0-63)>	Integer	Enter a value for the Traffic class. This value ranges from 0 to 63. The default is 0.
interface		Enter to configure type of interface for the outbound queue.
<iftype>		Enter to configure an interface type. Supports everything except port-channel. The options are: • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
<ifnum>		Enter to configure he type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface types internal-lan.
default-priority-type		Enter to Sets the Per-Hop Behavior (PHB) type to be used for filling the default (per-hop) behavior PHB for the policy map entry for the specified interface.
none		Enter to set the default PHB type as none.
vlanPri		Enter to set the PHB type as VLAN Priority.
<integer(0-7)>	Integer	Enter a value for the PHB type as VLAN Priority. It ranges from 0 to 1.
dot1P		Enter to set the PHB type as dot1P.
<integer(0-7)>	Integer	Enter a value for the PHB type as VLAN Priority. It ranges from 0 to 7.
<integer(0-1)>	Integer	Enter a value for the default DEI. This value ranges from 0 to 1.
ipDscp	Integer	Enter to set priority type to IP Differentiated Services Code Point.

Parameter	Type	Description
<integer(0-63)>	Integer	Enter a value for the PHB type as IP Differentiated Services Code Point. This value ranges from 0 to 63.

Mode

Policy Map Configuration Mode

Prerequisites

Policy Map entry must be created.

Examples

iS5comm(config)# policy 1

iS5comm(config-ply-map)# set policy class 1 interface gigabitethernet 0/1 default-priority-type none

iS5comm(config-ply-map)# set policy default-priority-type dot1P 7 0

29.20. shape-template

To create a shape-template, use the command **shape-template** in Global Configuration Mode. The no form of the command deletes a shape-template.

shape-template

```
shape-template <integer(1-65535)> [cir (1-10485760)>] [cbs (0-10485760)>]
```

no shape-template

```
no shape-template <integer(1-65535)>
```

Parameters

Parameter	Type	Description
<integer(1-65535)>	Integer	Enter a value for the shape Template table index. This value ranges from 1 to 65535.
cir		Enter to configure the committed information rate (cir) for packets through the queue. This value ranges from 1 to 10485760. Cir should be less than excess information rate (eir). For eir, see **meter-type** command.
<integer((1-10485760)>	Integer	Enter a value for the shape Template table index. This value ranges from 1 to 65535.
cbs		Enter to configure the committed burst size (cbs) for packets through the queue.
<integer((0-10485760)>	Integer	Enter a value for the committed burst size for packets through the queue. This value ranges from 0 to 10485760.

Mode

Global Configuration Mode

Examples

iS5comm(config)# shape-template 1 cir 20 cbs 40

29.21. show class-map

To display the class map entry, use the command **show class-map** in Privileged EXEC Mode. If executed without the optional parameters, this command displays all available class map information.

show class-map

```
show class-map <class-map-id (1-65535)>
```

Parameters

Parameter	Type	Description
<class-map-id(1-65535)>		Enter a value for the class map configurations for the specified class map entry to be displayed. The value ranges from 1 to 65535.

Mode

Privileged EXEC Mode

Examples

iS5comm# show class-map

```
    QoS Class Map Entries
    ---------------------
    ClassMapId                  : 1
    L2FilterId                  : None
    L3FilterId                  : None
    PriorityMapId               : 1
    VlanMapId                   : None
    CLASS                       : 1000
    PolicyMapId                 : None
    PreColor                    : None
    Status                      : Active
```

29.22. show meter

To display a meter entry, use the command **show meter** in Privileged EXEC Mode. Note that if executed without the optional parameters, this command displays all available meter information.

show meter

```
show meter [<meter-id (1-1000)>]
```

Parameters

Parameter	Type	Description
<meter-id(1-1000)>		Enter a value for the configurations for the index that enumerates the meter entries. The value ranges from 1 to 1000.

Mode

Privileged EXEC Mode

Examples

iS5comm# show meter

```
    QoS Meter Entries
    -----------------
    MeterId                     : 1
    Type                        : SRTCMC
    olor Mode                  : Color Blind
    Interval                    : None
    CIR                         : 20
    CBS                         : 20
    EIR                         : None
    EBS                         : 20
    NextMeter                   : None
    Status                      : Active

    MeterId                     : 10
    Type                        : Simple Token Bucket
    Color Mode                  : Color Blind
    Interval                    : None
    CIR                         : None
    CBS                         : None
    EIR                         : None
    EBS                         : None
    NextMeter                   : None
    Status                      : InActive
```

29.23. show policy-map

To display the policy map entry, use the command **show policy-map** in Privileged EXEC Mode. Note that if executed without the optional parameters, this command displays all available policy map information.

show policy-map

```
show policy-map [<policy-map-id (1-65535)>]
```

Parameters

Parameter	Type	Description
<policy-map-id(1-65535)>		Enter a value for the index that enumerates the policy map entry to be displayed. The value ranges from 1 to 65535.

Mode

Privileged EXEC Mode

Examples

iS5comm# show policy-map

```
    QoS Policy Map Entries
    ----------------------
    PolicyMapId  : 2
    IfIndex      : 0
    Class        : 0
    DefaultPHB   : Dot1P
    PHB Value    : 7
    DE Value     : 0
    MeterId      : 0
    ConNClass    : 0
    ExcNClass    : 0
    VioNClass    : 0
    ConfAct      : None.
    ExcAct       : None.
    VioAct       : None.

    PolicyMapId  : 3
    IfIndex      : 0
    Class        : 0
```

```
    DefaultPHB    : Dot1P
    PHB Value     : 7
    DE Value      : 0
    MeterId       : 0
    ConNClass     : 0
    ExcNClass     : 0
    VioNClass     : 0
    ConfAct       : None.
    ExcAct        : None.
    VioAct        : None.
```

29.24. show qos

To display QoS related global configuration, the meters statistics for conform, exceed, violate packets and octets count, the configured pbit reference for the tagged ports, and the queue statistics for EnQ, DeQ, discarded packets and octets count, management algorithm drop and queue occupancy, use the command **show qos** in Privileged EXEC Mode.

show qos

```
show qos {global info
 | meter-stats [<Meter-Id(1-65535)>]
 | pbit-preference-over-Dscp [interface <iftype> <ifnum>]
 queue-stats [interface <iftype> <ifnum>]}
```

Parameters

Parameter	Type	Description
`global info`		Enter to display QoS related global configuration.
`meter-stats`		Enter to display the meters statistics for conform, exceed, violate packets and octets count.
`<Meter-Id(1-65535)>`		Enter a value for the Index that enumerates the meter entries. The value ranges from 1 to 65535.
`pbit-preference-over-Dscp`		Enter to display the configured pbit reference for the tagged ports.
`interface`		Enter to configure type of interface for the outbound queue to be displayed.
`<iftype>`	Integer	Enter to configure an interface type. Supports everything except port-channel. The options are: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.
`<ifnum>`		Enter to configure he type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface types internal-lan.
`queue-stats`		Enter to display the queue statistics for EnQ, DeQ, discarded packets and octets count, management algorithm drop and queue occupancy.
`interface`		Enter to configure type of interface for the outbound queue to be displayed.

Parameter	Type	Description
<iftype>	Integer	Enter to configure an interface type. Supports everything except port-channel. The options are: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.
<ifnum>		Enter to configure he type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface types internal-lan.

Mode

Privileged EXEC Mode

Examples

iS5comm# show qos global info

```
    QoS Global Information
    ----------------------
    System Control               : Start
    System Control               : Enable
    Rate Unit                    : kbps
    Rate Granularity             : 64
    Trace Flag                   : 0
```

iS5comm# show qos meter-stats

```
    QoS Meter (Policer) Stats
    -------------------------
    Meter Index                  : 1
    Conform Packets              : 00
    Conform Octets              : 00
    Exceed Packets               : 00
```

```
    Exceed Octets               : 00V
    iolate Packets              : 00
    Violate Octets              : 0
```

iS5comm# show qos pbit-preference-over-Dscp

```
    QoS Default Pbit Preference Entries
    ---------------------------------
    IfIndex  Pbit preference over DSCP-------- ------------------------
    Gi0/1    Enabled
    Gi0/2    Enabled
    Gi0/3    Enabled
    Gi0/4    Enabled
    Gi0/5    Enabled
    Gi0/6    Enabled
    Gi0/7    Enabled
    Gi0/8    Enabled
    Gi0/9    Enabled
    Gi0/10   Enabled
    Gi0/11   Enabled
    Gi0/12   Enabled
    Gi0/13   Enabled
    Gi0/14   Enabled
    Gi0/15   Enabled
    Gi0/16   Enabled
    Gi0/17   Enabled
    Gi0/18   Enabled
    Gi0/19   Enabled
    Gi0/20   Enabled
    Gi0/21   Enabled
    Gi0/22   Enabled
    Gi0/23   Enabled
    Gi0/24   Enabled
    Ex0/1    Enabled
    Ex0/2    Enabled
    Ex0/3    Enabled
    Ex0/4    Enabled
```

iS5comm# show qos queue-stats

```
    QoS Queue Stats
    -------------------
    oS Queue Stats
    ---------------I
```

```
nterface Index              : Gi0/1
Queue Index                  : 1
EnQ Packets                  : 0
EnQ Octets                   : 0
DeQ Packets                  : 0
DeQ Octets                   : 0
Discard Packets              : 0
Discard Octets               : 0
Occupancy Octets             : 0
CongMgntAlgoDrop Octets      : 0
```

29.25. show queue

To display the configured queues, use the command **show queue** in Privileged EXEC Mode. Note that if executed without the optional parameters, this command displays all available queues entries.

show queue

```
show queue [interface <iftype> <ifnum>]
```

Parameters

Parameter	Type	Description
interface		Enter to configure type of interface for the outbound queue to be displayed.
<iftype>	Integer	Enter to configure an interface type. Supports everything except port-channel. The options are: • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
<ifnum>		Enter to configure he type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface types internal-lan.

Mode

Privileged EXEC Mode

Examples

iS5comm# show queue interface gi 0/1

```
QoS Queue Entries
-----------------
IfIndex  Queue  QTemplate  Scheduler  Weight  Priority  QType  ShapeIdx
GlobalId
-------  -----  ---------  ---------  ------  --------  -----  --------
--------
Gi0/1    1      1          8          NA      0         UC     none 1
Gi0/1    2      1          8          NA      1         UC     none 2
Gi0/1    3      1          8          NA      2         UC     none 3
Gi0/1    4      1          8          NA      3         UC     none 4
Gi0/1    5      1          8          NA      4         UC     none 5
Gi0/1    6      1          8          NA      5         UC     none 6
Gi0/1    7      1          8          NA      6         UC     none 7
Gi0/1    8      1          8          NA      7         UC     none 8
```

iS5comm# show queue 1

```
Queue Template Entries
----------------------
Q Template Id                : 1
Q Limit                      : 10000
Drop Type                    : Tail Drop
Drop Algo Status             : Disable
```

29.26. show queue-map

To display the configured queue maps, use the command **show queue-map** in Privileged EXEC Mode. Note that if executed without the optional parameters, this command displays all available queue map entries.

show queue-map

```
show queue-map [interface <iftype> <ifnum>]
```

Parameters

Parameter	Type	Description
interface		Enter to configure type of interface for the outbound queue to be displayed.
<iftype>	Integer	Enter to configure an interface type. Supports everything except port-channel. The options are: • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
<ifnum>		Enter to configure he type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface types internal-lan.

Mode

Privileged EXEC Mode

Examples

iS5comm# show queue-map

```
    QoS queue Map Entries
    ---------------------
    IfIndex    CLASS      PriorityType    Priority Value  Mapped Queue
    ---------- ---------- --------------- --------------- ---------------
    0          none       VlanPri         0               1
    0          none       VlanPri         1               2
    0          none       VlanPri         2               3
    0          none       VlanPri         3               4
    0          none       VlanPri         4               5
    0          none       VlanPri         5               6
    0          none       VlanPri         6               7
    0          none       VlanPri         7               8
```

29.27. show queue-template

To display the queue template entry and random detect configurations, use the command **show queue-template** in Privileged EXEC Mode. Note that if executed without the optional parameters, this command displays all available queue template information.

show

```
show queue-template [<queue-template-id (1-65535)>]
```

Parameters

Parameter	Type	Description
<queue-template-id(1-65535)>		Enter a value for queue template and random detect configurations for the specified queue template table index to be displayed. The value ranges from 1 to 65535.

Mode

Privileged EXEC Mode

Examples

iS5comm# show queue-template

```
    Q Queue Template Entries
    ----------------------
    Q Template Id               : 1
    Q Limit                     : 10000
    Drop Type                   : Tail Drop
    Drop Algo Status            : Disable
```

29.28. show scheduler

To display the configured scheduler, use the command **show scheduler** in Privileged EXEC Mode. Note that if executed without the optional parameters, this command displays all available scheduler information.

show scheduler

```
show scheduler [interface <iftype> <ifnum>]
```

Parameters

Parameter	Type	Description
interface		Enter to configure type of interface for the outbound queue to be displayed.
<iftype>		Enter to configure an interface type. Supports everything except port-channel. The options are: • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
<ifnum>		Enter to configure he type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface types internal-lan.

Mode

Privileged EXEC Mode

Examples

iS5comm# show scheduler interface gi 0/1

```
    QoS scheduler Entries
    ---------------------
    IfIndex    Scheduler Index Scheduler Algo       Shape Index Scheduler HL
    GlobalId
    ---------- --------------- -------------------- ----------- ------------
    ------------
    Gi0/1      8               strictPriority       0           0 29
```

29.29. show shape-template

To display the shape template entries, use the command **show shape-template** in Privileged EXEC Mode. Note that if executed without the optional parameters, this command displays all available shape template information.

show shape-template

```
show shape-template [<shape-template-id (1-65535)>]
```

Parameters

Parameter	Type	Description
<shape-template-id(1-65535)>		Enter a value for shape template index to be displayed. The value ranges from 1 to 65535.

Mode

Privileged EXEC Mode

Examples

iS5comm# show shape-template

```
    QoS shape template Entries
    --------------------------
    ShapeTemplate Id CIR            CBS             EIR             EBS
    ---------------- -------------- -------------- -------------- ----------
    1                20             40             10000          10000
```

ACL

30. ACL

Raptor offers a portable design that allows rapid integration of the solution with the choice of RTOS, CPU, and various chipsets. This section describes the CLI commands of the Raptor's Access Control list (ACL) features.

The ACL space is shared by Layer 2 ACLs, Layer 3 ACLs, and the filters used for trapping the protocol packets to CPU.

When all features are enabled in the build, all protocol filters will be in use. When certain features are not included in the build, then lesser number of protocol filters will be in use. Hence, a greater number of Layer 2 ACL and Layer 3 ACLs can possibly be created.

The ACL count also depends on the number of ports on which the ACL are applied. For example, for the build combination with the listed modules:

The ACL maximum is as follows:

- Maximum number of Layer 2 ACLs (MAC ACLs) – 767
- Maximum number of Layer 3 standard ACLs (IP-Standard) – 394
- Maximum number of Layer 3 extended ACLs (IP- Extended) – 788

NOTE: In this example, ACLs are considered to be applied to a port.

When an ACL is created, it becomes active in the control plane. When the ACL is applied on a port, the ACL gets provisioned in the hardware.

NOTE: Raptor does not support ACL counters. Also, the deny packets configured through ACL will not be displayed in the output of "show interface counters"– discard packet counters.

30.1. deny

To configure that traffic is denied for a particular protocol packet if the conditions defined in the deny statement are matched, use the command **deny** in Extended ACL IP Configuration Mode.

deny

```
deny {ip | ospf | pim <protocol-type (1-255)>}
 {any | host <src-ip-address>} | <src-ip-address>} <mask>}
 {any | host <dest-ip-address>} | <dest-ip-address>} <mask>}
 [{tos {max-reliability | max-throughput | min-delay | normal |<value(0-7)>}
| dscp <value (0-63)>}] {priority <value (1-255)>}]
```

```
 [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id
<vlan-id (1-4094)>] [cvlan-priority <value (0-7)>]

 [{single-tag | double-tag}]
```

Parameters

Parameter	Type	Description
ip		Enter to specify that traffic is denied for IP protocol packets.
ospf		Enter to specify that traffic is denied for OSPF protocol packets.
pim		Enter to specify that traffic is denied for PIM protocol packets.
<protocol-type (1-255)>		Enter a value for the protocol number for which traffic is allowed. **NOTE:** Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed
any		Enter to specify that packets are denied from any source.
host		Enter to specify the host source IPv4 address from which the packets are denied.
<src-ip-address>		Enter a value for the host source IPv4 address of the host that the packet is from.
mask		Enter to specify the mask of the host from where the packet is.
any		Enter to specify that packets are denied from any destination.
host		Enter to specify the destination IPv4 address to be used for forwarding the packets.
<dest-ip-address>		Enter a value for the address of the host that the packet is destined for and the network mask to use with the destination IP address.
mask		Enter to specify the mask of the host of the host that the packet is from.
tos		Enter to allow the protocol packets based on the following type of service configuration.
max-reliability		Enter to allow the protocol packets having TOS field set as high reliability.
max-throughput		Enter to allow the protocol packets having TOS field set as high throughput.
min-delay		Enter to allow the protocol packets having TOS field set as low delay
normal		Enter to allow all protocol packets. Does not check for the TOS field in the packets.

Parameter	Type	Description
<value(0-7)>		Enter to allow the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS. • 0 - Allows all protocol packets. Does not check for the TOS field in the packets. • 1 - Allows the protocol packets having TOS field set as high reliability. • 2 - Allows the protocol packets having TOS field set as high throughput. • 3 - Allows the protocol packets having TOS field set either as high reliability or high throughput. • 4 - Allows the protocol packets having TOS field set as low delay. • 5 - Allows the protocol packets having TOS field set either as low delay or high reliability. • 6 - Allows the protocol packets having TOS field set either as low delay or high throughput. • 7 - Allows the protocol packets having TOS field set either as low delay or high reliability or high throughput.
dscp		Enter to configure the Differentiated Services Code Point (DSCP) value to be checked against the packet.
<value((0-63)>		Enter a DSCP value. This value provides the quality of service control. This value ranges from 0 to 63.
priority		Enter to configure the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
<short (1-255)>		Enter a priority value. This value ranges from 1 to 255.
svlan-id		Enter to configure Service VLAN value to match against incoming packets.
<vlan-id (1-4094)>>		Enter a value for Service VLAN.
svlan-priority		Enter to configure the Service VLAN priority value to match against incoming packets
<value (0-7)>		Enter a Service VLAN priority value. This value ranges from 0 to 7.
cvlan-id		Enter to configure Customer VLAN priority value to match against incoming packets.

Parameter	Type	Description
<vlan-id (1-4094)>		Enter a customer vlan ID value. This value ranges from 0 to 7.
cvlan-priority		Enter to specify customer vlan related configuration
<value (0-7)>		Enter a customer vlan ID value. This value ranges from 0 to 7.
double-tag		Enter to specify that the filter is to be applied on double VLAN tagged packets
single-tag		Enter to specify that the filter is to be applied on Single VLAN tagged packets
redirect		Enter to redirect the action to the destination interface or set of interfaces.
<iftype>		Enter destination interface type. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links
<ifnum>		Enter to redirect the packets to the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface types Gigabitethernet, Fastethernet and Extreme-Ethernet.
<iface_list>		Enter to redirect the packets to the list of interfaces.
load-balance		Enter to specify the parameters based on which the traffic distribution needs to be done.
src-ip		Enter to specify that the traffic distribution is based on the source IP address.
dst-ip		Enter to specify that the traffic distribution is based on the destination IP address.
src-mac		Enter to specify that the traffic distribution is based on the source MAC address.

Parameter	Type	Description
dst-mac		Enter to specify that the traffic distribution is based on the destination MAC address.
vlanid		Enter to specify that the traffic distribution is based on the VLAN ID to be filtered.
src-tcpport		Enter to specify that the traffic distribution is based on the source TCP port number.
dst-tcpport		Enter to specify that the traffic distribution is based on the destination TCP Port number.
src-udpport		Enter to specify that the traffic distribution is based on the source UDP port number
dst-udpport		Enter to specify that the traffic distribution is based on the destination UDP port number.
sub-action		Enter to configure the VLAN specific sub action to be performed on the packet.
none		Enter to specify that the actions related to the VLAN ID will not be considered.
modify-vlan		Enter to specify to modify the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
<short (1-4094)>	Integer	Enter a value for the VLAN ID to which the packet gets classified. This value ranges from 1 to 4094.
nested-vlan		Enter to specify to add an outer VLAN tag to the packet with the specified VLAN ID (nested VLAN).
<short (1-4094)>	Integer	Enter a value for the outer VLAN tag to the packet with the specified VLAN ID. This value ranges from 1 to 4094.

Mode

Extended ACL IP Configuration Mode

Default

- protocol-type - 255
- priority - 1
- dscp - 0
- svlan-id - 0
- svlan-priority - 1

- cvlan-id - 0
- cvlan-priority - 1
- single-tag | double-tag - Single tag

Examples

is5comm (config)# ip access-list extended 1001

is5comm (config-ext-nacl)# deny ip any any priority 10

iS5comm(config-ext-nacl)#

30.2. deny

To configure the packets to be rejected based on the MAC address and the associated parameters, use the command **deny** in Extended ACL MAC Configuration Mode. This command allows non-IP traffic to be rejected if the conditions are matched.

deny

```
deny {any | host <src-ip-address>} | host <dest-mac-address>}

 [{aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 |
etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps |
netbios | vines-echo | vines-ip | xns-id | <protocol (0-65535)>

 | encaptype | <integer (1-65535)>] [vlan <vlan-id (1-4094)>] {priority
<value (1-255)>}]

 [outerEtherType < integer (1-65535)>] [svlan-id <vlan-id (1-4094)>]
[svlan-priority <value (0-7)>] [cvlan-priority <value (0-7)>]

 [{single-tag | double-tag}]

 [redirect {interface <iftype> <ifnum> | <iftype> <ifnum> [<iftype>
```

Parameters

Parameter	Type	Description
any		Enter to specify that control packets can be denied from any source.
host		Enter to specify the host source MAC address from which the control packets are denied.
<src-ip-address>		Enter a value for the host source MAC address to be used for forwarding the packets.
host		Enter to specify the destination MAC address from which the packets are denied.
<dest-mac-address>		Enter a value for the destination MAC address from which the packets are denied.
aarp		Enter to configure the non-IP protocol type as Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber		Enter to configure the non-IP protocol type as the address of the host that the packet is destined for.
dec-spanning		Enter to configure the non-IP protocol type as EtherType Digital Equipment Corporation spanning tree
decnet-iv		Enter to configure the non-IP protocol type as EtherType DECnet Phase IV protocol.
diagnostic		Enter to configure the non-IP protocol type as EtherType DEC-Diagnostic.
dsm		Enter to configure the non-IP protocol type as EtherType DEC-DSM/DDP.
etype-6000		Enter to configure the non-IP protocol type as EtherType 0x6000.
etype-8042		Enter to configure the non-IP protocol type as EtherType 0x8042.
lat		Enter to configure the non-IP protocol type as EtherType DEC-LAT.
lavc-sca		Enter to configure the non-IP protocol type as EtherType DEC-LAVC-SCA
mop-console		Enter to configure the non-IP protocol type as EtherType DEC-MOP Remote Console
mop-dump		Enter to configure the non-IP protocol type as EtherType DEC-MOP Dump.
msdos		Enter to configure the non-IP protocol type as EtherType DEC-MSDOS.
mumps		Enter to configure the non-IP protocol type as EtherType DEC-MUMPS.

Parameter	Type	Description
netbios		Enter to configure the non-IP protocol type as EtherType DEC- Network Basic Input/Output System.
vines-echo		Enter to configure the non-IP protocol type as EtherType Virtual Integrated Network
vines-ip		Enter to configure the non-IP protocol type as EtherType VINES IP
xns-id		Enter to configure the non-IP protocol type as EtherType Xerox Network Systems protocol suite
<protocol (0-65535)>		Enter to configure the non-IP protocol type to be filtered. This value ranges from 0 to 65535. The value 0 represents that filter is applicable for all protocols.
encaptype		Enter to configure the arbitary ether type of a packet with Ethernet II or SNAP encapsulation in decimal
<short (1-65535)>		Enter a value for the arbitary ether type of a packet. This value ranges from 1 to 65535.
vlan		Enter to specify the VLAN ID to be filtered.
<vlan-id (1-4094)>		Enter a value for the VLAN ID. This value ranges from 1 to 4094.
priority		Enter to specify the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
<short (1-255)>		Enter a priority value. This value ranges from 1 to 255.
outerEtherType		Enter to specify the EtherType value to match on Service vlan tag (OutEthertype)
<Integer (1-65535)>		Enter a value for OutEthertype. The value ranges from 1 to 65535.
svlan-id		Enter to configure Service VLAN ID value to match against incoming packets.
<vlan-id (1-4094)>		Enter a value for Service VLAN ID. This value ranges from 1 to 4094.
svlan-priority		Enter to configure Customer VLAN priority value to match against incoming packets.
<value (0-7)>		Enter a Service VLAN priority value. This value ranges from 0 to 7.

Parameter	Type	Description
cvlan-priority		Enter to configure Customer VLAN priority value to match against incoming packets.
<value (0-7)>		Enter a customer VLAN ID value. This value ranges from 0 to 7.
double-tag		Enter to specify he filter to be applied on double VLAN tagged packets.
single-tag		Enter to specify the filter to be applied on Single VLAN tagged packets.

Mode

Extended ACL MAC Configuration Mode

Default

- <protocol (0-65535)> - 0
- vlan-id - 0
- priority - 1
- outerEtherType - 0
- svlan-id - 0
- cvlan-priority - 1
- svlan-priority - 1
- single-tag | double-tag - Single tag

Examples

is5comm (config)# mac access-list extended 5

iS5comm(config-ext-macl)# deny any any priority 100

iS5comm(config-ext-macl)#

30.3. deny

To configure that traffic is denied if the conditions defined in the deny statement are matched, use the command **deny** in Standard ACL Configuration Mode.

deny

```
deny {any | host <src-ip-address> | <network-src-ip> <mask>}
 [{any | host <src-ip-address> | <network-src-ip> <mask>}]
```

```
priority <value (1-255)>
```

Parameters

Parameter	Type	Description
any		Enter to specify that packets can be forwarded from any source IP Address.
host		Enter to specify the host source IPv4 address to be used for forwarding the packets
<src-ip-address>		Enter a value for the host source IPv4 address to be used for forwarding the packets.
<network-src-ip>		Enter to specify the address of the host that the packet is from.
<mask>		Enter to specify the network mask to be used with the source IP address.
any		Enter to specify that packets can be denied to any destination
host		Enter to specify the destination IPv4 address from which the packets are denied.
<src-ip-address>		Enter a value for the destination IPv4 address from which the packets are denied.
<network-src-ip>		Enter to specify the address of the host that the packet is destined for.
<mask>		Enter to specify the network mask to use with the destination IP address
priority		Enter to specify the priority of the filter to be decided which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
<value (1-255)>	Integer	Enter a value for the priority of the filter. This value ranges from 1 to 255.

Mode

Standard ACL Configuration Mode

Default

priority - 1

Examples

is5comm (config)# ip access-list standard 1

is5comm (config-std-nacl)# deny any priority 10

30.4. deny icmp

To configure the ICMP (Internet Control Message Protocol) packets to be to be rejected based on the associated parameters, use the command **deny icmp** in Extended ACL IP Configuration Mode.

deny

```
deny icmp
 {any | host <src-ip-address>} | <src-ip-address>} <src-mask>}
 {any | host <dest-ip-address>} | <dest-ip-address>} <dest-mask>}
 [message-type <short (0-255)>] [message-code <short (0-255)>] {priority
<value (1-255)>}]
 [{tos {max-reliability | max-throughput | min-delay | normal |<value(0-7)>}
| dscp <value (0-63)>}] {priority <value (1-255)>}]
 [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id
<vlan-id (1-4094)>] [cvlan-priority <value (0-7)>]
 [{single-tag | double-tag}]
```

Parameters

Parameter	Type	Description
ICMP		Enter to configure the ICMP packets to be rejected based on the associated parameters.
any		Enter to specify that ICMP packets can be denied from any source.
host		Enter to specify the host source IPv4 address from which the packets are denied.
<src-ip-address>		Enter a value for the host source IPv4 address from which the packets are denied.
<src-mask>		Enter to specify the network mask to be used with the destination IP address.
any		Enter to specify that ICMP packets can be forwarded to any destination.
host		Enter to specify the host destination IPv4 address to be used for forwarding the packets. **NOTE:** Both source and destination port cannot be configured. Only either source or the destination port range can be configured.
<dest-ip-address>		Enter a value for the host destination IPv4 address to which the packets are denied.
<dest-mask>		Enter to specify the network mask to be used with the destination IP address.
message-type		Enter to configure the ICMP Message type to be checked against the packet. The packet is allowed if it matches with the message type.

Parameter	Type	Description
<short (0-255)>	Integer	Enter a ICMP Message type. This value ranges from 0 to 255. Some of the ICMP message types are: • Value ICMP Message type • 0 Echo reply • 3 Destination unreachable • 4 Source quench • 5 Redirect • 8 Echo request • 11 Time exceeded • 12 Parameter problem • 13 Timestamp request • 14 Timestamp reply • 15 Information request • 16 Information reply • 17 Address mask request • 18 Address mask reply • 55 No ICMP type
message-code		Enter to configure the ICMP Message code to be checked against the packet. The packet is allowed if it matches with the message type.
<short (0-255)>	Integer	Enter a ICMP Message code. This value ranges from 0 to 255. Some of the ICMP message Codes are: • Value ICMP code • 0 Network unreachable • 1 Host unreachable • 2 Protocol unreachable • 3 Port unreachable • 4 Fragment needed • 5 Source route fail • 6 Destination network unknown • 7 Destination host unknown8 Source host isolated • 9 Destination network administratively prohibited • 10 Destination host administratively prohibited • 11 Network unreachable TOS • 12 Host unreachable TOS • 255 No ICMP code

Parameter	Type	Description
gt		Enter to deny only the ICMP control packets having the ICMP destination port numbers greater than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
lt		Enter to deny only the ICMP control packets having the ICMP destination port numbers lesser than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
eq		Enter to deny only the ICMP control packets having the specified ICMP destination port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
range		Enter to deny only the ICMP control packets having the ICMP destination port numbers within the specified range.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
tos		Enter to deny the ICMP packets based on the following type of service configuration.
max-reliability		Enter to deny the ICMP packets having TOS field set as high reliability.
max-throughput		Enter to deny the ICMP packets having TOS field set as high throughput.
min-delay		Enter to deny the ICMP packets having TOS field set as low delay
normal		Enter to deny all ICMP packets. Does not check for the TOS field in the packets.

Parameter	Type	Description
<value(0-7)>		Enter to deny the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS. • 0 - Denies all protocol packets. Does not check for the TOS field in the packets. • 1 - Denies the protocol packets having TOS field set as high reliability. • 2 - Denies the protocol packets having TOS field set as high throughput. • 3 - Denies the protocol packets having TOS field set either as high reliability or high throughput. • 4 - Denies the protocol packets having TOS field set as low delay. • 5 -Denies the protocol packets having TOS field set either as low delay or high reliability. • 6 - Denies the protocol packets having TOS field set either as low delay or high throughput. • 7 - Denies the protocol packets having TOS field set either as low delay or high reliability or high throughput.
dscp		Enter to configure the Differentiated Services Code Point (DSCP) value to be checked against the packet
<value((0-63))>		Enter a DSCP value. This value provides the quality of service control. This value ranges from 0 to 63.
priority		Enter to configure the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
<short (1-255)>		Enter a priority value. This value ranges from 1 to 255.
svlan-id		Enter to configure Service VLAN value to match against incoming packets.
<vlan-id (1-4094)>		Enter a value for Service VLAN. This value ranges from 1 to 4094.
svlan-priority		Enter to specify Service VLAN related configuration.
<value (0-7)>		Enter a Service VLAN ID value. This value ranges from 0 to 7.
cvlan-id		Enter to configure Customer VLAN value to be matched against incoming packets.

Parameter	Type	Description
<vlan-id (1-4094)>		Enter a value for customer VLAN. This value ranges from 1 to 4094.
cvlan-priority		Enter to configure Customer priority value to be matched against incoming packets.
<value (0-7)>		Enter a Customer vlan ID value. This value ranges from 0 to 7.
double-tag		Enter to specify that the filter is to be applied on double VLAN tagged packets
single-tag		Enter to specify that the filter is to be applied on Single VLAN tagged packets

Mode

Extended ACL IP Configuration Mode

Default

- message-type / message code - 255
- priority - 1
- svlan-id - 0
- svlan-priority - 1
- cvlan-id - 0
- cvlan-priority - 1
- single-tag | double-tag - Single tag

Examples

is5comm (config)# ip access-list extended 1001

is5comm (config-ext-nacl)# deny icmp any any priority 1

30.5. deny tcp

To configure the TCP packets to be to be rejected based on the associated parameters, use the command **deny tcp** in Extended ACL IP Configuration Mode.

deny

```
deny tcp
```

```
 {any | host <src-ip-address>} | <src-ip-address>} <src-mask>}

 [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eg <port-number
(1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}]

 {any | host <dest-ip-address>} | <dest-ip-address>} <dest-mask>}

 [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eg <port-number
(1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] [{ack |
rst}]

 [{tos {max-reliability | max-throughput | min-delay | normal |<value(0-7)>}
| dscp <value (0-63)>}] {priority <value (1-255)>}]

 [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id
<vlan-id (1-4094)>] [cvlan-priority <value (0-7)>]

 [{single-tag | double-tag}]
```

Parameters

Parameter	Type	Description
tcp		Enter to configure the TCP packets to be rejected based on the associated parameters.
any		Enter to specify that TCP packets can be denied from any source.
host		Enter to specify the host source IPv4 address from which the packets are denied. **NOTE:** Both source and destination port cannot be configured. Only either source or the destination port range can be configured.
<src-ip-address>		Enter a value for the host source IPv4 address from which the packets are denied.
<src-mask>		Enter to specify the network mask to be used with the destination IP address.
gt		Enter to deny only the TCP control packets having the TCP source port numbers greater than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
lt		Enter to deny only the TCP control packets having the TCP source port numbers lesser than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
eq		Enter to deny only the TCP control packets having the specified TCP source port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
range		Enter to deny only the TCP control packets having the TCP source port numbers within the specified range.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
any		Enter to specify that TCP packets can be forwarded to any destination.
host		Enter to specify the host destination IPv4 address to be used for forwarding the packets. **NOTE:** Both source and destination port cannot be configured. Only either source or the destination port range can be configured.

Parameter	Type	Description
<dest-ip-address>		Enter a value for the host destination IPv4 address to which the packets are denied.
<dest-mask>		Enter to specify the network mask to be used with the destination IP address.
gt		Enter to deny only the TCP control packets having the TCP destination port numbers greater than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
lt		Enter to deny only the TCP control packets having the TCP destination port numbers lesser than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
eq		Enter to deny only the TCP control packets having the specified TCP destination port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
range		Enter to deny only the TCP control packets having the TCP destination port numbers within the specified range.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
ack		Enter to configure the TCP ACK bit to be checked against the packet.
rst		Enter to configure the TCP RST bit to be checked against the packet.
tos		Enter to deny the TCP packets based on the following type of service configuration.
max-reliability		Enter to deny the TCP packets having TOS field set as high reliability.
max-throughput		Enter to deny the TCP packets having TOS field set as high throughput.
min-delay		Enter to deny the TCP packets having TOS field set as low delay
normal		Enter to deny all TCP packets. Does not check for the TOS field in the packets.

Parameter	Type	Description
<value(0-7)>		Enter to deny the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS. • 0 - Denies all protocol packets. Does not check for the TOS field in the packets. • 1 - Denies the protocol packets having TOS field set as high reliability. • 2 - Denies the protocol packets having TOS field set as high throughput. • 3 - Denies the protocol packets having TOS field set either as high reliability or high throughput. • 4 - Denies the protocol packets having TOS field set as low delay. • 5 -Denies the protocol packets having TOS field set either as low delay or high reliability. • 6 - Denies the protocol packets having TOS field set either as low delay or high throughput. • 7 - Denies the protocol packets having TOS field set either as low delay or high reliability or high throughput.
dscp		Enter to configure the Differentiated Services Code Point (DSCP) value to be checked against the packet
<value((0-63))>		Enter a DSCP value. This value provides the quality of service control. This value ranges from 0 to 63.
priority		Enter to configure the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
<short (1-255)>		Enter a priority value. This value ranges from 1 to 255.
svlan-id		Enter to configure Service VLAN value to match against incoming packets.
<vlan-id (1-4094)>		Enter a value for Service VLAN. This value ranges from 1 to 4094.
svlan-priority		Enter to specify Service VLAN related configuration.
<value (0-7)>		Enter a Service VLAN ID value. This value ranges from 0 to 7.
cvlan-id		Enter to configure Customer VLAN value to be matched against incoming packets.

Parameter	Type	Description
<vlan-id (1-4094)>		Enter a value for customer VLAN. This value ranges from 1 to 4094.
cvlan-priority		Enter to configure Customer priority value to be matched against incoming packets.
<value (0-7)>		Enter a Customer vlan ID value. This value ranges from 0 to 7.
double-tag		Enter to specify that the filter is to be applied on double VLAN tagged packets
single-tag		Enter to specify that the filter is to be applied on Single VLAN tagged packets

Mode

Extended ACL IP Configuration Mode

Default

- any -Source and Destination address are not checked.
- gt - 0 (the packets are not checked for TCP port number)
- lt - 0 (the packets are not checked for TCP port number)
- eq - 0 (the packets are not checked for TCP port number)
- range - 0 for minimum port number, 65535 for maximum port number.
- tos-value - 0
- dscp - 1
- priority - 1
- svlan-id - 0
- svlan-priority - 1
- cvlan-id - 0
- cvlan-priority - 1
- single-tag | double-tag - Single tag

Examples

is5comm (config)# ip access-list extended 1001

is5comm (config-ext-nacl)# deny tcp any any priority 2

30.6. deny udp

To configure the UDP (User Datagram Protocol) packets to be to be rejected based on the associated parameters, use the command **deny udp** in Extended ACL IP Configuration Mode.

deny

```
deny udp
 {any | host <src-ip-address>} | <src-ip-address>} <src-mask>}
 [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eg <port-number
(1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}]
 {any | host <dest-ip-address>} | <dest-ip-address>} <dest-mask>}
 [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eg <port-number
(1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] [{ack |
rst}]
 [{tos {max-reliability | max-throughput | min-delay | normal |<value(0-7)>}
| dscp <value (0-63)>}] {priority <value (1-255)>}]
 [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id
<vlan-id (1-4094)>] [cvlan-priority <value (0-7)>]
 [{single-tag | double-tag}]
```

Parameters

Parameter	Type	Description
UDP		Enter to configure the UDP packets to be rejected based on the associated parameters.
any		Enter to specify that UDP packets can be denied from any source.
host		Enter to specify the host source IPv4 address from which the packets are denied. **NOTE:** Both source and destination port cannot be configured. Only either source or the destination port range can be configured.
<src-ip-address>		Enter a value for the host source IPv4 address from which the packets are denied.
<src-mask>		Enter to specify the network mask to be used with the destination IP address.
gt		Enter to deny only the UDP control packets having the UDP source port numbers greater than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
lt		Enter to deny only the UDP control packets having the UDP source port numbers lesser than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
eq		Enter to deny only the UDP control packets having the specified UDP source port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
range		Enter to deny only the UDP control packets having the UDP source port numbers within the specified range.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
any		Enter to specify that UDP packets can be forwarded to any destination.
host		Enter to specify the host destination IPv4 address to be used for forwarding the packets. **NOTE:** Both source and destination port cannot be configured. Only either source or the destination port range can be configured.

Parameter	Type	Description
<dest-ip-address>		Enter a value for the host destination IPv4 address to which the packets are denied.
<dest-mask>		Enter to specify the network mask to be used with the destination IP address.
gt		Enter to deny only the UDP control packets having the UDP destination port numbers greater than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
lt		Enter to deny only the UDP control packets having the UDP destination port numbers lesser than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
eq		Enter to deny only the UDP control packets having the specified UDP destination port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
range		Enter to deny only the UDP control packets having the UDP destination port numbers within the specified range.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
tos		Enter to deny the UDP packets based on the following type of service configuration.
max-reliability		Enter to deny the UDP packets having TOS field set as high reliability.
max-throughput		Enter to deny the UDP packets having TOS field set as high throughput.
min-delay		Enter to deny the UDP packets having TOS field set as low delay
normal		Enter to deny all UDP packets. Does not check for the TOS field in the packets.

Parameter	Type	Description
<value(0-7)>		Enter to deny the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS. • 0 - Denies all protocol packets. Does not check for the TOS field in the packets. • 1 - Denies the protocol packets having TOS field set as high reliability. • 2 - Denies the protocol packets having TOS field set as high throughput. • 3 - Denies the protocol packets having TOS field set either as high reliability or high throughput. • 4 - Denies the protocol packets having TOS field set as low delay. • 5 -Denies the protocol packets having TOS field set either as low delay or high reliability. • 6 - Denies the protocol packets having TOS field set either as low delay or high throughput. • 7 - Denies the protocol packets having TOS field set either as low delay or high reliability or high throughput.
dscp		Enter to configure the Differentiated Services Code Point (DSCP) value to be checked against the packet
<value((0-63))>		Enter a DSCP value. This value provides the quality of service control. This value ranges from 0 to 63.
priority		Enter to configure the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
<short (1-255)>		Enter a priority value. This value ranges from 1 to 255.
svlan-id		Enter to configure Service VLAN value to match against incoming packets.
<vlan-id (1-4094)>		Enter a value for Service VLAN. This value ranges from 1 to 4094.
svlan-priority		Enter to specify Service VLAN related configuration.
<value (0-7)>		Enter a Service VLAN ID value. This value ranges from 0 to 7.
cvlan-id		Enter to configure Customer VLAN value to be matched against incoming packets.

Parameter	Type	Description
<vlan-id (1-4094)>		Enter a value for customer VLAN. This value ranges from 1 to 4094.
cvlan-priority		Enter to configure Customer priority value to be matched against incoming packets.
<value (0-7)>		Enter a Customer vlan ID value. This value ranges from 0 to 7.
double-tag		Enter to specify that the filter is to be applied on double VLAN tagged packets
single-tag		Enter to specify that the filter is to be applied on Single VLAN tagged packets

Mode

Extended ACL IP Configuration Mode

Default

- dscp - 1
- priority - 1
- svlan-id - 0
- svlan-priority - 1
- vlan-id - 0
- cvlan-priority - 1
- single-tag | double-tag - Single tag

Examples

is5comm (config)# ip access-list extended 1001

is5comm (config-ext-nacl)# deny udp any any priority 255

30.7. egress access-list

To configure the default egress ACL mode as IP based or MAC based, use the command **egress access-list** in Global Configuration Mode.

egress access-list

```
egress access-list mode {ip | mac}
```

Parameters

Parameter	Type	Description
ip		Enter to configure the egress ACL mode as IP which supports IP based PCL (Policy Control List) at egress. **NOTE:** MAC access list configurations should be deleted before setting Egress Filter Mode as IP.
mac		Enter to configure the egress ACL mode as MAC which supports which supports MAC based PCL at egress. **NOTE:** IP access list configurations should be deleted before setting Egress Filter Mode as MAC.

Mode

Global Configuration Mode

Default

Default egress filtering mode is IP and it is running on the hardware.

Examples

iS5comm(config)# egress access-list mode ip

30.8. ip access-group

To enable access control for the packets on the interface and control access to a Layer 2 or Layer 3 interface, use the command **ip access-group** in Interface Configuration Mode. The no form of this command removes all access groups or the specified access group from the interface. The direction of filtering is specified using the token in or out.

ip access-group

```
ip access-group <access-list-number (1-65535)> {in | out}
```

no ip access-group

```
no ip access-group <access-list-number (1-65535)> {in | out}
```

Parameters

Parameter	Type	Description
<access-list-number(1-65535)>		Enter a value to specify the IP access control list number which is to be enabled on the interface. This value ranges from 1 to 65535.
in		Enter to configure the packets as Inbound packets.
out		Enter to configure the packets as Outbound packets. **NOTE:** Redirect Filter is not applicable for out bound packets.

Mode

Interface Configuration Mode

Prerequisites

This command executes only if IP access list with the same number has been created

iS5comm(config)# ip access-list standard 100

iS5comm(config-std-nacl)# exit

Examples

iS5comm(config)# int gi 0/1

is5comm (config-if)# ip access-group 100 in

iS5comm(config-if)# ip access-group 100 out

30.9. ip access-list

To configure IP access control lists (ACL)s and enter the IP Access-list Configuration mode, use the command **ip access-list** in Global Configuration Mode. Depending on the standard or extended option chosen by the user, this command returns a corresponding IP Access list configuration mode. ACLs on the system perform both access control and Layer 3 field classification. The no form of the command deletes the IP access list.

ip access-list

```
ip access-list {standard <access-list-number (1-1000)> | extended
<access-list-number (1001-65535)>}
```

no ip access-list

```
no ip access-list {standard <access-list-number (1-1000)> | extended
<access-list-number (1001-65535)>}
```

Parameters

Parameter	Type	Description
standard		Enter to configure a standard access list with the specified access list number. Standard access lists create filters based on IP address and network mask only (L3 filters only).
<access-list-number(1-1000)>	Integer	Enter an access list number for a standard access list. The value ranges from 1 to 1000.
extended		Enter to configure an extended access list with the specified access list number. Extended access lists enables specification of filters based on the type of protocol, range of TCP/UDP ports as well as the IP address and network mask (Layer 4 filters).
<access-list-number(1001-65535)>	Integer	Enter an access list number for an extended access list. The value ranges from 1001 to 65535.

Mode

Global Configuration Mode

Examples

is5comm (config)# ip access-list standard 1

is5comm (config-std-nacl)#

is5comm (config)# ip access-list extended 1001

is5comm (config-ext-nacl)#

30.10. mac access-group

To apply a MAC access control list (ACL) to a Layer 2 interface, use the command **mac access-group** in Interface Configuration Mode. The no form of this command removes the MAC ACLs from the interface.

mac access-group

```
mac access-group <access-list-number (1-65535)> {in | out}
```

no mac access-group

```
no mac access-group <access-list-number (1-65535)> {in | out}
```

Parameters

Parameter	Type	Description
<access-list-number(1-65535)>		Enter a value to specify the MAC access control list number which is to be enabled on the interface. This value ranges from 1 to 65535.
in		Enter to configure the packets as Inbound packets. **NOTE:** The MAC ACL defined with both protocol and encaptype combination cannot be applied to a Layer 2 Interface
out		Enter to configure the packets as Outbound packets. **NOTE:** Redirect Filter is not applicable for out bound packets.

Mode

Interface Configuration Mode

Prerequisites

MAC access list must have been created.

Examples

iS5comm(config)# interface gi 0/1

is5comm (config-if)# mac access-group 5 in

30.11. mac access-list

To configure Layer 2 MAC (Media Access Control) access control lists (ACL)s and enter the MAC Access-list Configuration mode, use the command **mac access-list** in Global Configuration Mode. ACLs on the system perform both access control and Layer 2 field classification. The MAC access list identifier value ranges from 1 to 65535. The no form of the command deletes the MAC ACL.

mac access-list

```
mac access-list extended <access-list-number (1001-65535)>}
```

no mac access-list

```
no mac access-list extended <access-list-number (1001-65535)>}
```

Parameters

Parameter	Type	Description
extended		Enter to configure the Layer 2 MAC (Media Access Control) access control lists (ACL)s and enter the MAC Access-list Configuration mode, use the command **mac access-list** in Global Configuration Mode. ACLs on the system perform both access control and layer 2 field classification.
<access-list-number(1001-65535)>	Integer	Enter a value for the Layer 2 MAC ACL number. The value ranges from 1001 to 65535.

Mode

Global Configuration Mode

Examples

is5comm (config)# mac access-list extended 5

is5comm (config-std-macl)#

30.12. permit

To configure traffic for a particular protocol packet if the conditions defined in the permit statement are matched, use the command **permit** in Extended ACL IP Configuration Mode.

permit

```
permit {ip | ospf | pim <protocol-type (1-255)>}
 {any | host <src-ip-address>} | <src-ip-address>} <mask>}
 {any | host <dest-ip-address>} | <dest-ip-address>} <mask>}
 [{tos {max-reliability | max-throughput | min-delay | normal |<value(0-7)>}
| dscp <value (0-63)>}] {priority <value (1-255)>}]
 [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id
<vlan-id (1-4094)>] [cvlan-priority <value (0-7)>]
 [{single-tag | double-tag}]
 [redirect {interface <iftype> <ifnum> | <iftype> <iface_list> [<iftype>
<iface_list>]
```

```
 load-balance {src-ip | dst-ip | src-mac | dst-mac | vlanid | src-tcpport |
dst-tcpport | src-udpport | dst-udpport}}]

 [sub-action {none | modify-vlan <short (1-4094)> | nested-vlan <short (1
-4094)>]
```

Parameters

Parameter	Type	Description
ip		Enter to specify that traffic is allowed for IP protocol packets.
ospf		Enter to specify that traffic is allowed for OSPF protocol packets.
pim		Enter to specify that traffic is allowed for PIM protocol packets.
<protocol-type (1-255)>		Enter a value for the protocol number for which traffic is allowed.
any		Enter to specify that packets can be forwarded from any source.
host		Enter to specify the host source IPv4 address to be used for forwarding the packets
<src-ip-address>		Enter a value for the host source IPv4 address to be used for forwarding the packets.
mask		Enter to specify the network mask to use with the source IP address.
any		Enter to specify that packets can be forwarded to any destination.
host		Enter to specify the host destination IPv4 address to be used for forwarding the packets
<src-ip-address>		Enter a value for the host destination IPv4 address to be used for forwarding the packets.
mask		Enter to specify the network mask to use with the destination IP address.
tos		Enter to allow the protocol packets based on the following type of service configuration.
max-reliability		Enter to allow the protocol packets having TOS field set as high reliability.
max-throughput		Enter to allow the protocol packets having TOS field set as high throughput.
min-delay		Enter to allow the protocol packets having TOS field set as low delay
normal		Enter to allow all protocol packets. Does not check for the TOS field in the packets.

Parameter	Type	Description
<value(0-7)>		Enter to allow the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS. • 0 - Allows all protocol packets. Does not check for the TOS field in the packets. • 1 - Allows the protocol packets having TOS field set as high reliability. • 2 - Allows the protocol packets having TOS field set as high throughput. • 3 - Allows the protocol packets having TOS field set either as high reliability or high throughput. • 4 - Allows the protocol packets having TOS field set as low delay. • 5 - Allows the protocol packets having TOS field set either as low delay or high reliability. • 6 - Allows the protocol packets having TOS field set either as low delay or high throughput. • 7 - Allows the protocol packets having TOS field set either as low delay or high reliability or high throughput.
dscp		Enter to configure the Differentiated Services Code Point (DSCP) value to be checked against the packet
<value((0-63)>		Enter a DSCP value. This value provides the quality of service control. This value ranges from 0 to 63.
priority		Enter to configure the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
<short (1-255)>		Enter a priority value. This value ranges from 1 to 255.
svlan-id		Enter to configure Service VLAN value to match against incoming packets.
<vlan-id (1-4094)>>		Enter a value for Service VLAN.
svlan-priority		Enter to specify Service VLAN related configuration
<value (0-7)>		Enter a Service VLAN ID value. This value ranges from 0 to 7.
cvlan-id		Enter to configure Customer VLAN value to match against incoming packets.

Parameter	Type	Description
<vlan-id (1-4094)>		Enter a value for Customer VLAN ID to match against incoming packets.
cvlan-priority		Enter to specify Customer VLAN priority value to match against incoming packets
<value (0-7)>		Enter a customer vlan ID value. This value ranges from 0 to 7.
double-tag		Enter to specify that the filter is to be applied on double VLAN tagged packets
single-tag		Enter to specify that the filter is to be applied on Single VLAN tagged packets
redirect		Enter to redirect the action to the destination interface or set of interfaces.
<iftype>		Enter redirect the packets to the specified type of interface.The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links
<ifnum>		Enter to redirect the packets to the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface types Gigabitethernet, Fastethernet and Extreme-Ethernet.
<iface_list>		Enter to redirect the packets to the list of interfaces.
load-balance		Enter to specify the parameters based on which the traffic distribution needs to be done.
src-ip		Enter to specify that the traffic distribution is based on the source IP address.
dst-ip		Enter to specify that the traffic distribution is based on the destination IP address.
src-mac		Enter to specify that the traffic distribution is based on the source MAC address.

Parameter	Type	Description
dst-mac		Enter to specify that the traffic distribution is based on the destination MAC address.
vlanid		Enter to specify that the traffic distribution is based on the VLAN ID to be filtered.
src-tcpport		Enter to specify that the traffic distribution is based on the source TCP port number.
dst-tcpport		Enter to specify that the traffic distribution is based on the destination TCP Port number.
src-udpport		Enter to specify that the traffic distribution is based on the source UDP port number
dst-udpport		Enter to specify that the traffic distribution is based on the destination UDP port number.
sub-action		Enter to configure the VLAN specific sub action to be performed on the packet.
none		Enter to specify that the actions related to the VLAN ID will not be considered.
modify-vlan		Enter to specify to modify the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
<short (1-4094)>	Integer	Enter a value for the VLAN ID to which the packet gets classified. This value ranges from 1 to 4094.
nested-vlan		Enter to specify to add an outer VLAN tag to the packet with the specified VLAN ID (nested VLAN).
<short (1-4094)>	Integer	Enter a value for the outer VLAN tag to the packet with the specified VLAN ID. This value ranges from 1 to 4094.

Mode

Extended ACL IP Configuration Mode

Default

- protocol-type - 255
- priority - 1
- dscp - 0
- svlan-id - 0
- svlan-priority - 1

- cvlan-id - 0
- cvlan-priority - 1
- single-tag | double-tag - Single tag

Examples

is5comm (config)# ip access-list extended 1001

is5comm (config-ext-nacl)# permit ospf any host 14.0.0.0 tos 5 priority 200 svlan-id 200 svlan-priority 3 cvlan-id 345 cvlan-priority 4 redirect gi 0/4 gi 0/10 load-balance dst-udpport sub-action nested-vlan 222

iS5comm(config-ext-nacl)#

30.13. permit

To configure the packets to be forwarded based on the MAC address and the associated parameters, use the command **permit** in Extended ACL MAC Configuration Mode. This command allows non-IP traffic to be forwarded if the conditions are matched.

permit

```
permit {any | host <src-ip-address>} | host <dest-mac-address>}

 [{aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 |
etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps |
netbios | vines-echo | vines-ip | xns-id | <protocol (0-65535)>

 | encaptype | <integer (1-65535)>] [vlan <vlan-id (1-4094)>] {priority
<value (1-255)>}]

 [outerEtherType < integer (1-65535)>] [svlan-id <vlan-id (1-4094)>]
[svlan-priority <value (0-7)>] [cvlan-priority <value (0-7)>]

 [{single-tag | double-tag}]

 [redirect {interface <iftype> <ifnum> | <iftype> <ifnum> [<iftype>
<iface_list>] load-balance {src-ip | dst-ip | src-mac | dst-mac | vlanid |
src-tcpport | dst-tcpport | src-udpport | dst-udpport}}]

 [sub-action {none | modify-vlan <short (1-4094)> | nested-vlan <short (1
-4094)> | strip-ether-hdr}}]

 [next-filter-type {l2 | l3 | user-defined} next-filter-id | <short
(1-65535)>}]

 dp {green | yellow | red} sub-action {modify-cfi-dei <short (0-1)>}]

 | user-priority <short (0-7)> cfi-dei <short (0-1)> sub-action {modify-dp
{green | yellow | red} | modify-dc <short (0-7)>}
```

Parameters

Parameter	Type	Description
any		Enter to specify that packets can be forwarded from any source MAC Address.
host		Enter to specify the host source MAC address to be used for forwarding the packets
<src-ip-address>		Enter a value for the host source MAC address to be used for forwarding the packets.
host		Enter to specify the destination MAC address from which the packets are denied.
<dest-mac-address>		Enter a value for the destination MAC address from which the packets are denied.
aarp		Enter to configure the non-IP protocol type as Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber		Enter to configure the non-IP protocol type as the address of the host that the packet is destined for.
dec-spanning		Enter to configure the non-IP protocol type as EtherType Digital Equipment Corporation spanning tree
decnet-iv		Enter to configure the non-IP protocol type as EtherType DECnet Phase IV protocol.
diagnostic		Enter to configure the non-IP protocol type as EtherType DEC-Diagnostic.
dsm		Enter to configure the non-IP protocol type as EtherType DEC-DSM/DDP.
etype-6000		Enter to configure the non-IP protocol type as EtherType 0x6000.
etype-8042		Enter to configure the non-IP protocol type as EtherType 0x8042.
lat		Enter to configure the non-IP protocol type as EtherType DEC-LAT.
lavc-sca		Enter to configure the non-IP protocol type as EtherType DEC-LAVC-SCA
mop-console		Enter to configure the non-IP protocol type as EtherType DEC-MOP Remote Console
mop-dump		Enter to configure the non-IP protocol type as EtherType DEC-MOP Dump.
msdos		Enter to configure the non-IP protocol type as EtherType DEC-MSDOS.

Parameter	Type	Description
mumps		Enter to configure the non-IP protocol type as EtherType DEC-MUMPS.
netbios		Enter to configure the non-IP protocol type as EtherType DEC- Network Basic Input/Output System.
vines-echo		Enter to configure the non-IP protocol type as EtherType Virtual Integrated Network
vines-ip		Enter to configure the non-IP protocol type as EtherType VINES IP
xns-id		Enter to configure the non-IP protocol type as EtherType Xerox Network Systems protocol suite
<protocol (0-65535)>		Enter to configure the non-IP protocol type to be filtered. This value ranges from 0 to 65535. The value 0 represents that filter is applicable for all protocols.
encaptype		Enter to configure the arbitary ether type of a packet with Ethernet II or SNAP encapsulation in decimal
<short (1-65535)>		Enter a value for the arbitary ether type of a packet. This value ranges from 1 to 65535.
vlan		Enter to specify the VLAN ID to be filtered.
<vlan-id (1-4094)>		Enter a value for the VLAN ID. This value ranges from 1 to 4094.
priority		Enter to specify the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
<short (1-255)>		Enter a priority value. This value ranges from 1 to 255.
outerEtherType		Enter to specify the EtherType value to match on Service vlan tag (OutEthertype).
<integer (1-65535)>		Enter a value for OutEthertype. The value ranges from 1 to 65535
svlan-id		Enter to configure Service VLAN ID value to match against incoming packets.
<vlan-id (1-4094)>		Enter a value for Service VLAN ID. This value ranges from 1 to 4094.
svlan-priority		Enter to configure Customer VLAN priority value to match against incoming packets.

Parameter	Type	Description
<value (0-7)>		Enter a Service VLAN priority value. This value ranges from 0 to 7.
cvlan-priority		Enter to configure Customer VLAN priority value to match against incoming packets.
<value (0-7)>		Enter a customer VLAN ID value. This value ranges from 0 to 7.
double-tag		Enter to specify double tag type of the packet.
single-tag		Enter to specify single tag type of the packet
redirect		Enter to redirect the action to the destination interface or set of interfaces.
<iftype>		Enter destination interface type.The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links
<ifnum>		Enter to redirect the packets to the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface types Gigabitethernet, Fastethernet and Extreme-Ethernet.
<iface_list>		Enter to redirect the packets to the list of interfaces.
load-balance		Enter to specify the parameters based on which the traffic distribution needs to be done.
src-ip		Enter to specify that the traffic distribution is based on the source IP address.
dst-ip		Enter to specify that the traffic distribution is based on the destination IP address.
src-mac		Enter to specify that the traffic distribution is based on the source MAC address.
dst-mac		Enter to specify that the traffic distribution is based on the destination MAC address.

Parameter	Type	Description
vlanid		Enter to specify that the traffic distribution is based on the VLAN ID to be filtered.
src-tcpport		Enter to specify that the traffic distribution is based on the source TCP port number.
dst-tcpport		Enter to specify that the traffic distribution is based on the destination TCP Port number.
src-udpport		Enter to specify that the traffic distribution is based on the source UDP port number
dst-udpport		Enter to specify that the traffic distribution is based on the destination UDP port number.
sub-action		Enter to configure the VLAN specific sub action to be performed on the packet.
none		Enter to specify that the actions related to the VLAN ID will not be considered.
modify-vlan		Enter to specify to modify the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
<short (1-4094)>	Integer	Enter a value for the VLAN ID to which the packet gets classified. This value ranges from 1 to 4094.
nested-vlan		Enter to specify to add an outer VLAN tag to the packet with the specified VLAN ID (nested VLAN).
<short (1-4094)>	Integer	Enter a value for the outer VLAN tag to the packet with the specified VLAN ID. This value ranges from 1 to 4094.
none		Enter to specify that the actions related to the VLAN ID will not be considered.
strip-ether-hdr		Enter to specify Strip outer Ethernet header for MPLS packets.
next-filter-type		Enter to specify the type of next access-control list.
L2		Enter to specify filtering to be done for MAC-based ACL.
L3		Enter to specify filtering to be done for IP-based ACL.
user-defined		Enter to specify User defined packets related configuration
next-filter-id		Enter to specify next filter ID related configuration

Parameter	Type	Description
<short (1-65535)>		Enter a value for next filter ID related configuration.
dp		Enter to configure the packets to be forwarded based on the drop precedence.
green		Enter to specify drop precedence as green which implies that green packets are forwarded. This is the default
red		Enter to specify drop precedence as red which implies that red packets are forwarded.
yellow		Enter to specify drop precedence as yellow which implies that yellow packets are forwarded.
sub-action		Enter to specify sub action related configuration.
modify-cfi-dei		Enter to modify cfi-dei bit value in the c-vlan tag or s-vlan tag of the packet to be applied in the filter. This value can be either 0 or 1.
user-priority		Enter to configures that the packets are forwarded based on the user priority.
<short (0-7)>		Enter a value for c-vlan user priority.
cfi-dei		Enter to configure the CFI DEI value in the c-vlan tag or s-vlan tag of the packet to be applied in the filter. The value can be 0 or 1
<short (0-7)>		Enter a value for CFI DEI value in the c-vlan tag or s-vlan tag of the packet.
sub-action		Enter to configure sub action to be performed on the packet.
modify-dp		Enter to configure the drop-precedence.
green		Enter to specify drop precedence as green which implies that green packets are forwarded. This is the default
red		Enter to specify drop precedence as red which implies that red packets are forwarded.
yellow		Enter to specify drop precedence as yellow which implies that yellow packets are forwarded.
sub-action		Enter to specify sub action related configuration.
modify-tc		Enter to configure traffic class value.
<short (0-1)>		Enter a traffic class value. The value ranges from 0 to 7

Mode

Extended ACL MAC Configuration Mode

Default

- protocol - 0
- sub-action - none
- vlan-id - 0
- priority - 1
- outerEtherType - 0
- svlan-id - 0
- cvlan-priority - 1
- svlan-priority - 1
- single-tag | double-tag - Single tag

Examples

is5comm (config)# mac access-list extended 5

iS5comm(config-ext-macl)# permit user-priority 1 cfi-dei 1 sub-action modify-dp green

is5comm (config-ext-macl)# permit dp red sub-action modify-cfi-dei 1

is5comm (config-ext-macl)# permit any any priority 255

30.14. permit

To configure the packets to be forwarded depending upon the associated parameters, use the command **permit** in Standard ACL Configuration Mode. Standard IP access lists use source addresses for matching operations.

permit

```
permit {any | host <src-ip-address> | <network-src-ip> <mask>}
 [{any | host <src-ip-address> | <network-src-ip> <mask>}]
 [redirect {interface <iftype> <ifnum> | <iftype> <iface_list> [ <iftype>
<iface_list>]
 load-balance {src-ip | dst-ip | src-mac | dst-mac | vlanid | src-tcpport |
dst-tcpport | src-udpport | dst-udpport}}]
 [sub-action {none | modify-vlan <short (1-4094)> | nested-vlan <short (1
-4094)>}]
 priority <value (1-255)>
```

Parameters

Parameter	Type	Description
any		Enter to specify that packets can be forwarded from any source IP Address.
host		Enter to specify the host source IPv4 address to be used for forwarding the packets
<src-ip-address>		Enter a value for the host source IPv4 address to be used for forwarding the packets.
<network-src-ip>		Enter to specify the address of the host that the packet is from.
<mask>		Enter to specify the network mask to be used with the source IP address.
any		Enter to specify that packets can be denied to any destination
host		Enter to specify the destination IPv4 address from which the packets are denied.
<src-ip-address>		Enter a value for the destination IPv4 address from which the packets are denied.
<network-src-ip>		Enter to specify the address of the host that the packet is destined for.
<mask>		Enter to specify the network mask to use with the destination IP address
redirect		Enter to redirect the action to the destination interface or set of interfaces.
<iftype>		Enter destination interface type.The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links
<ifnum>		Enter to redirect the packets to the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface types Gigabitethernet, Fastethernet and Extreme-Ethernet.
<iface_list>		Enter to redirect the packets to the list of interfaces.

Parameter	Type	Description
load-balance		Enter to specify the parameters based on which the traffic distribution needs to be done.
src-ip		Enter to specify that the traffic distribution is based on the source IP address.
dst-ip		Enter to specify that the traffic distribution is based on the destination IP address.
src-mac		Enter to specify that the traffic distribution is based on the source MAC address.
dst-mac		Enter to specify that the traffic distribution is based on the destination MAC address.
vlanid		Enter to specify that the traffic distribution is based on the VLAN ID to be filtered.
src-tcpport		Enter to specify that the traffic distribution is based on the source TCP port number.
dst-tcpport		Enter to specify that the traffic distribution is based on the destination TCP Port number.
src-udpport		Enter to specify that the traffic distribution is based on the source UDP port number
dst-udpport		Enter to specify that the traffic distribution is based on the destination UDP port number.
sub-action		Enter to configure the VLAN specific sub action to be performed on the packet.
none		Enter to specify that the actions related to the VLAN ID will not be considered.
modify-vlan		Enter to specify to modify the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
<short (1-4094)>	Integer	Enter a value for the VLAN ID to which the packet gets classified. This value ranges from 1 to 4094.
nested-vlan		Enter to specify to add an outer VLAN tag to the packet with the specified VLAN ID.
<short (1-4094)>	Integer	Enter a value for the outer VLAN tag to the packet with the specified VLAN ID. This value ranges from 1 to 4094.

Parameter	Type	Description
priority		Enter to specify the priority of the filter to be decided which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
<value (1-255)>	Integer	Enter a value for the priority of the filter. This value ranges from 1 to 255.

Mode

Standard ACL Configuration Mode

Default

priority - 1

Examples

is5comm (config)# ip access-list standard 1

is5comm (config-std-nacl)# permit any priority 255

30.15. permit icmp

To configure the ICMP (Internet Control Message Protocol) packets to be forwarded based on the associated parameters, use the command **permit icmp** in Extended ACL IP Configuration Mode.

permit

```
permit icmp
 {any | host <src-ip-address>} | <src-ip-address>} <src-mask>}
 {any | host <dest-ip-address>} | <dest-ip-address>} <dest-mask>}
 [message-type <short (0-255)>] [message-code <short (0-255)>] {priority
<value (1-255)>}]
 [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id
<vlan-id (1-4094)>] [cvlan-priority <value (0-7)>]
 [{single-tag | double-tag}]
 [redirect {interface <iftype> <ifnum> | <iftype> <iface_list> [<iftype>
<iface_list>]
 load-balance {src-ip | dst-ip | src-mac | dst-mac | vlanid | src-tcpport |
dst-tcpport | src-udpport | dst-udpport}}]
```

```
 [sub-action {none | modify-vlan <short (1-4094)> | nested-vlan <short (1
-4094)>]
```

Parameters

Parameter	Type	Description
icmp		Enter to specify the ICMP (Internet Control Message Protocol) to be forwarded based on the associated parameters.
any		Enter to specify that ICMP packets can be forwarded from any source.
host		Enter to specify the host source IPv4 address to be used for forwarding the packets. **NOTE:** Both source and destination port cannot be configured. Only either source or the destination port range can be configured.
<src-ip-address>		Enter a value for the host source IPv4 address to be used for forwarding the packets.
<src-mask>		Enter to specify the address of the host that the packet is destined for and the network mask to use with the destination IP address.
any		Enter to specify that ICMP packets can be forwarded to any destination.
host		Enter to specify the host destination IPv4 address to be used for forwarding the packets. **NOTE:** Both source and destination port cannot be configured. Only either source or the destination port range can be configured.
<dest-ip-address>		Enter a value for the host destination IPv4 address to be used for forwarding the packets.
<dest-mask>		Enter to specify the address of the host that the packet is destined for and the network mask to use with the destination IP address.
message-type		Enter to configure the ICMP Message type to be checked against the packet. The packet is allowed if it matches with the message type.

Parameter	Type	Description
<short (0-255)>	Integer	Enter a ICMP Message type. This value ranges from 0 to 255. Some of the ICMP message types are: • Value ICMP Message type • 0 Echo reply • 3 Destination unreachable • 4 Source quench • 5 Redirect • 8 Echo request • 11 Time exceeded • 12 Parameter problem • 13 Timestamp request • 14 Timestamp reply • 15 Information request • 16 Information reply • 17 Address mask request • 18 Address mask reply • 55 No ICMP type
message-code		Enter to configure the ICMP Message code to be checked against the packet. The packet is allowed if it matches with the message type.
<short (0-255)>	Integer	Enter a ICMP Message code. This value ranges from 0 to 255. Some of the ICMP message Codes are: • Value ICMP code • 0 Network unreachable • 1 Host unreachable • 2 Protocol unreachable • 3 Port unreachable • 4 Fragment needed • 5 Source route fail • 6 Destination network unknown • 7 Destination host unknown8 Source host isolated • 9 Destination network administratively prohibited • 10 Destination host administratively prohibited • 11 Network unreachable TOS • 12 Host unreachable TOS • 255 No ICMP code

Parameter	Type	Description
priority		Enter to configure the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
<short (1-255)>	Integer	Enter a priority value. This value ranges from 1 to 255.
svlan-id		Enter to configure Service VLAN value to match against incoming packets.
<vlan-id (1-4094)>	Integer	Enter a value for Service VLAN. This value ranges from 1 to 4094.
svlan-priority		Enter to specify Service VLAN related configuration.
<value (0-7)>	Integer	Enter a Service VLAN ID value. This value ranges from 0 to 7.
cvlan-id		Enter to configure Customer VLAN value to match against incoming packets.
<vlan-id (1-4094)>	Integer	Enter a value for Customer VLAN value to match against incoming packets.
cvlan-priority		Enter to configure Customer VLAN priority value to match against incoming packets.
<value (0-7)>		Enter a customer vlan ID value. This value ranges from 0 to 7.
double-tag		Enter to specify that the filter is to be applied on double VLAN tagged packets
single-tag		Enter to specify that the filter is to be applied on Single VLAN tagged packets
redirect		Enter to redirect the action to the destination interface or set of interfaces.

Parameter	Type	Description
<iftype>		Enter destination interface type.The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links
<ifnum>		Enter to redirect the packets to the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface types Gigabitethernet, Fastethernet and Extreme-Ethernet.
<iface_list>		Enter to redirect the packets to the list of interfaces.
load-balance		Enter to specify the parameters based on which the traffic distribution needs to be done.
src-ip		Enter to specify that the traffic distribution is based on the source IP address.
dst-ip		Enter to specify that the traffic distribution is based on the destination IP address.
src-mac		Enter to specify that the traffic distribution is based on the source MAC address.
dst-mac		Enter to specify that the traffic distribution is based on the destination MAC address.
vlanid		Enter to specify that the traffic distribution is based on the VLAN ID to be filtered.
src-tcpport		Enter to specify that the traffic distribution is based on the source TCP port number.
dst-tcpport		Enter to specify that the traffic distribution is based on the destination TCP Port number.
src-udpport		Enter to specify that the traffic distribution is based on the source UDP port number
dst-udpport		Enter to specify that the traffic distribution is based on the destination UDP port number.

Parameter	Type	Description
sub-action		Enter to configure the VLAN specific sub action to be performed on the packet.
none		Enter to specify that the actions related to the VLAN ID will not be considered.
modify-vlan		Enter to specify to modify the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
<short (1-4094)>	Integer	Enter a value for the VLAN ID to which the packet gets classified. This value ranges from 1 to 4094.
nested-vlan		Enter to specify to add an outer VLAN tag to the packet with the specified VLAN ID (nested VLAN).
<short (1-4094)>	Integer	Enter a value for the outer VLAN tag to the packet with the specified VLAN ID. This value ranges from 1 to 4094.

Mode

Extended ACL IP Configuration Mode

Default

- dscp - 1
- priority - 1
- svlan-id - 0
- svlan-priority - 1
- cvlan-id - 0
- cvlan-priority - 1
- single-tag | double-tag - Single tag

Examples

is5comm (config)# ip access-list extended 1001

is5comm (config-ext-nacl)# permit icmp any 14.0.0.0 255.0.0.0 message-type 0 message-code 18 priority 22 svlan-id 2 svlan-priority 2 cvlan-id 2 cvlan-priority 2 double-tag redirect interface gigabitethernet 0/10 sub-action none

iS5comm(config-ext-nacl)#

30.16. permit tcp

To configure the TCP packets to be forwarded based on the associated parameters, use the command **permit tcp** in Extended ACL IP Configuration Mode.

permit

```
permit tcp
 {any | host <src-ip-address>} | <src-ip-address>} <src-mask>}
 [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eg <port-number
(1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}]
 {any | host <dest-ip-address>} | <dest-ip-address>} <dest-mask>}
 [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eg <port-number
(1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] [{ack |
rst}]
 [{tos {max-reliability | max-throughput | min-delay | normal |<value(0-7)>}
| dscp <value (0-63)>}] {priority <value (1-255)>}]
 [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id
<vlan-id (1-4094)>] [cvlan-priority <value (0-7)>]
 [{single-tag | double-tag}]
 [redirect {interface <iftype> <ifnum> | <iftype> <iface_list> [<iftype>
<iface_list>]
 load-balance {src-ip | dst-ip | src-mac | dst-mac | vlanid | src-tcpport |
dst-tcpport | src-udpport | dst-udpport}}]
 [sub-action {none | modify-vlan <short (1-4094)> | nested-vlan <short (1
-4094)>]
```

Parameters

Parameter	Type	Description
tcp		Enter to configure the TCP packets to be forwarded based on the associated parameters.
any		Enter to specify that TCP packets can be forwarded from any source.
host		Enter to specify the host source IPv4 address to be used for forwarding the packets. **NOTE:** Both source and destination port cannot be configured. Only either source or the destination port range can be configured.
<src-ip-address>		Enter a value for the host source IPv4 address to be used for forwarding the packets.
<src-mask>		Enter to specify the network mask to be used with the destination IP address.
gt		Enter to allow only the TCP control packets having the TCP source port numbers greater than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
lt		Enter to allow only the TCP control packets having the TCP source port numbers lesser than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
eq		Enter to allow only the TCP control packets having the specified TCP source port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
range		Enter to allow only the TCP control packets having the TCP source port numbers within the specified range.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
any		Enter to specify that TCP packets can be forwarded to any destination.
host		Enter to specify the host destination IPv4 address to be used for forwarding the packets. **NOTE:** Both source and destination port cannot be configured. Only either source or the destination port range can be configured.

Parameter	Type	Description
<dest-ip-address>		Enter a value for the host destination IPv4 address to be used for forwarding the packets.
<dest-mask>		Enter to specify the address of the host that the packet is destined for and the network mask to use with the destination IP address.
gt		Enter to allow only the TCP control packets having the TCP destination port numbers greater than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
lt		Enter to allow only the TCP control packets having the TCP destination port numbers lesser than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
eq		Enter to allow only the TCP control packets having the specified TCP destination port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
range		Enter to allow only the TCP control packets having the TCP destination port numbers within the specified range.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
ack		Enter to configure the TCP ACK bit to be checked against the packet.
rst		Enter to configure the TCP RST bit to be checked against the packet.
tos		Enter to allow the TCP packets based on the following type of service configuration.
max-reliability		Enter to allow the TCP packets having TOS field set as high reliability.
max-throughput		Enter to allow the TCP packets having TOS field set as high throughput.
min-delay		Enter to allow the TCP packets having TOS field set as low delay
normal		Enter to allow all TCP packets. Does not check for the TOS field in the packets.

Parameter	Type	Description
<value(0-7)>		Enter to allow the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS. • 0 - Allows all protocol packets. Does not check for the TOS field in the packets. • 1 - Allows the protocol packets having TOS field set as high reliability. • 2 - Allows the protocol packets having TOS field set as high throughput. • 3 - Allows the protocol packets having TOS field set either as high reliability or high throughput. • 4 - Allows the protocol packets having TOS field set as low delay. • 5 - Allows the protocol packets having TOS field set either as low delay or high reliability. • 6 - Allows the protocol packets having TOS field set either as low delay or high throughput. • 7 - Allows the protocol packets having TOS field set either as low delay or high reliability or high throughput.
dscp		Enter to configure the Differentiated Services Code Point (DSCP) value to be checked against the packet
<value((0-63))>		Enter a DSCP value. This value provides the quality of service control. This value ranges from 0 to 63.
priority		Enter to configure the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
<short (1-255)>		Enter a priority value. This value ranges from 1 to 255.
svlan-id		Enter to configure Service VLAN value to match against incoming packets.
<vlan-id (1-4094)>		Enter a value for Service VLAN. This value ranges from 1 to 4094.
svlan-priority		Enter to specify Service VLAN related configuration.
<value (0-7)>		Enter a Service VLAN ID value. This value ranges from 0 to 7.
cvlan-id		Enter to configure Customer VLAN value to match against incoming packets.

Parameter	Type	Description
<vlan-id (1-4094)>		Enter a value for customer VLAN ID.
cvlan-priority		Enter to configure Customer VLAN priorityvalue to match against incoming packets.
<value (0-7)>		Enter a customer vlan ID value. This value ranges from 0 to 7.
double-tag		Enter to specify that the filter is to be applied on double VLAN tagged packets
single-tag		Enter to specify that the filter is to be applied on Single VLAN tagged packets
redirect		Enter to redirect the action to the destination interface or set of interfaces.
<iftype>		Enter destination interface type.The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links
<ifnum>		Enter to redirect the packets to the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface types Gigabitethernet, Fastethernet and Extreme-Ethernet.
<iface_list>		Enter to redirect the packets to the list of interfaces.
load-balance		Enter to specify the parameters based on which the traffic distribution needs to be done.
src-ip		Enter to specify that the traffic distribution is based on the source IP address.
dst-ip		Enter to specify that the traffic distribution is based on the destination IP address.
src-mac		Enter to specify that the traffic distribution is based on the source MAC address.

Parameter	Type	Description
dst-mac		Enter to specify that the traffic distribution is based on the destination MAC address.
vlanid		Enter to specify that the traffic distribution is based on the VLAN ID to be filtered.
src-tcpport		Enter to specify that the traffic distribution is based on the source TCP port number.
dst-tcpport		Enter to specify that the traffic distribution is based on the destination TCP Port number.
src-udpport		Enter to specify that the traffic distribution is based on the source UDP port number
dst-udpport		Enter to specify that the traffic distribution is based on the destination UDP port number.
sub-action		Enter to configure the VLAN specific sub action to be performed on the packet.
none		Enter to specify that the actions related to the VLAN ID will not be considered.
modify-vlan		Enter to specify to modify the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
<short (1-4094)>	Integer	Enter a value for the VLAN ID to which the packet gets classified. This value ranges from 1 to 4094.
nested-vlan		Enter to specify to add an outer VLAN tag to the packet with the specified VLAN ID (nested VLAN).
<short (1-4094)>	Integer	Enter a value for the outer VLAN tag to the packet with the specified VLAN ID. This value ranges from 1 to 4094.

Mode

Extended ACL IP Configuration Mode

Default

- any -Source and Destination address are not checked.
- gt - 0 (the packets are not checked for TCP port number)
- lt - 0 (the packets are not checked for TCP port number)
- eq - 0 (the packets are not checked for TCP port number)
- range - 0 for minimum port number, 65535 for maximum port number.

- tos-value - 0
- dscp - 1
- priority - 1
- svlan-id - 0
- svlan-priority - 1
- cvlan-id - 0
- cvlan-priority - 1
- single-tag | double-tag - Single tag

Examples

is5comm (config)# ip access-list extended 1001

is5comm (config-ext-nacl)# permit tcp any any priority 255

iS5comm(config-ext-nacl)#

30.17. permit udp

To specify the UDP (User Datagram Protocol) packets to be forwarded based on the associated parameters, use the command **permit udp** in Extended ACL IP Configuration Mode.

permit

```
permit udp
 {any | host <src-ip-address>} | <src-ip-address>} <src-mask>}
 [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eg <port-number
(1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}]
 {any | host <dest-ip-address>} | <dest-ip-address>} <dest-mask>}
 [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eg <port-number
(1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] [{ack |
rst}]
 [{tos {max-reliability | max-throughput | min-delay | normal |<value(0-7)>}
| dscp <value (0-63)>}] {priority <value (1-255)>}]
 [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id
<vlan-id (1-4094)>] [cvlan-priority <value (0-7)>]
 [{single-tag | double-tag}]
 [redirect {interface <iftype> <ifnum> | <iftype> <iface_list> [<iftype>
<iface_list>]
 load-balance {src-ip | dst-ip | src-mac | dst-mac | vlanid | src-tcpport |
dst-tcpport | src-udpport | dst-udpport}}]
```

```
 [sub-action {none | modify-vlan <short (1-4094)> | nested-vlan <short (1
-4094)>]
```

Parameters

Parameter	Type	Description
udp		Enter to specify the UDP (User Datagram Protocol) to be forwarded based on the associated parameters.
any		Enter to specify that UDP packets can be forwarded from any source.
host		Enter to specify the host source IPv4 address to be used for forwarding the packets. **NOTE:** Both source and destination port cannot be configured. Only either source or the destination port range can be configured.
<src-ip-address>		Enter a value for the host source IPv4 address to be used for forwarding the packets.
<src-mask>		Enter to specify the address of the host that the packet is destined for and the network mask to use with the destination IP address.
gt		Enter to allow only the UDP control packets having the UDP source port numbers greater than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
lt		Enter to allow only the UDP control packets having the UDP source port numbers lesser than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
eq		Enter to allow only the UDP control packets having the specified UDP source port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
range		Enter to allow only the UDP control packets having the UDP source port numbers within the specified range.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
any		Enter to specify that UDP packets can be forwarded to any destination.
host		Enter to specify the host destination IPv4 address to be used for forwarding the packets. **NOTE:** Both source and destination port cannot be configured. Only either source or the destination port range can be configured.

Parameter	Type	Description
<dest-ip-address>		Enter a value for the host destination IPv4 address to be used for forwarding the packets.
<dest-mask>		Enter to specify the address of the host that the packet is destined for and the network mask to use with the destination IP address.
gt		Enter to allow only the UDP control packets having the UDP destination port numbers greater than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
lt		Enter to allow only the UDP control packets having the UDP destination port numbers lesser than the specified port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
eq		Enter to allow only the UDP control packets having the specified UDP destination port number.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
range		Enter to allow only the UDP control packets having the UDP destination port numbers within the specified range.
<port-number (1-65535)>		Enter a value for the port number. This value ranges from 1 to 65535.
tos		Enter to allow the UDP packets based on the following type of service configuration.
max-reliability		Enter to allow the UDP packets having TOS field set as high reliability.
max-throughput		Enter to allow the UDP packets having TOS field set as high throughput.
min-delay		Enter to allow the UDP packets having TOS field set as low delay
normal		Enter to allow all UDP packets. Does not check for the TOS field in the packets.

Parameter	Type	Description
<value(0-7)>		Enter to allow the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS. • 0 - Allows all protocol packets. Does not check for the TOS field in the packets. • 1 - Allows the protocol packets having TOS field set as high reliability. • 2 - Allows the protocol packets having TOS field set as high throughput. • 3 - Allows the protocol packets having TOS field set either as high reliability or high throughput. • 4 - Allows the protocol packets having TOS field set as low delay. • 5 - Allows the protocol packets having TOS field set either as low delay or high reliability. • 6 - Allows the protocol packets having TOS field set either as low delay or high throughput. • 7 - Allows the protocol packets having TOS field set either as low delay or high reliability or high throughput.
dscp		Enter to configure the Differentiated Services Code Point (DSCP) value to be checked against the packet
<value((0-63)>		Enter a DSCP value. This value provides the quality of service control. This value ranges from 0 to 63.
priority		Enter to configure the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
<short (1-255)>		Enter a priority value. This value ranges from 1 to 255.
svlan-id		Enter to configure Service VLAN value to match against incoming packets.
<vlan-id (1-4094)>		Enter a value for Service VLAN. This value ranges from 1 to 4094.
svlan-priority		Enter to specify the Service VLAN priority value to match against incoming packets.
<value (0-7)>		Enter a Service VLAN priority value. This value ranges from 0 to 7.
cvlan-id		Enter to configure Customer VLAN value to match against incoming packets.

Parameter	Type	Description
<vlan-id (1-4094)>		Enter a value for Customer VLAN value to match against incoming packets.
cvlan-priority		Enter to configure Customer VLAN priority value to match against incoming packets.
<value (0-7)>		Enter a customer vlan ID value. This value ranges from 0 to 7.
double-tag		Enter to specify that the filter is to be applied on double VLAN tagged packets
single-tag		Enter to specify that the filter is to be applied on Single VLAN tagged packets
redirect		Enter to redirect the action to the destination interface or set of interfaces.
<iftype>		Enter destination interface type.The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links
<ifnum>		Enter to redirect the packets to the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface types Gigabitethernet, Fastethernet and Extreme-Ethernet.
<iface_list>		Enter to redirect the packets to the list of interfaces.
load-balance		Enter to specify the parameters based on which the traffic distribution needs to be done.
src-ip		Enter to specify that the traffic distribution is based on the source IP address.
dst-ip		Enter to specify that the traffic distribution is based on the destination IP address.
src-mac		Enter to specify that the traffic distribution is based on the source MAC address.

Parameter	Type	Description
dst-mac		Enter to specify that the traffic distribution is based on the destination MAC address.
vlanid		Enter to specify that the traffic distribution is based on the VLAN ID to be filtered.
src-tcpport		Enter to specify that the traffic distribution is based on the source TCP port number.
dst-tcpport		Enter to specify that the traffic distribution is based on the destination TCP Port number.
src-udpport		Enter to specify that the traffic distribution is based on the source UDP port number
dst-udpport		Enter to specify that the traffic distribution is based on the destination UDP port number.
sub-action		Enter to configure the VLAN specific sub action to be performed on the packet.
none		Enter to specify that the actions related to the VLAN ID will not be considered.
modify-vlan		Enter to specify to modify the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
<short (1-4094)>	Integer	Enter a value for the VLAN ID to which the packet gets classified. This value ranges from 1 to 4094.
nested-vlan		Enter to specify to add an outer VLAN tag to the packet with the specified VLAN ID (nested VLAN).
<short (1-4094)>	Integer	Enter a value for the outer VLAN tag to the packet with the specified VLAN ID. This value ranges from 1 to 4094.

Mode

Extended ACL IP Configuration Mode

Default

- dscp - 1
- priority - 1
- svlan-id - 0
- svlan-priority - 1
- cvlan-id - 0

- cvlan-priority - 1
- single-tag | double-tag - Single tag

Examples

is5comm (config)# ip access-list extended 1001

is5comm (config-ext-nacl)# permit udp any any priority 1

iS5comm(config-ext-nacl)#

30.18. rate-limit

To enable the rate limiting by configuring the egress packet rate of an interface, use the command **rate-limit** in Interface Configuration Mode. The no form of this command disables the rate limiting on an egress port.

rate-limit

```
rate-limit {output {rate-value <integer(0-80000000)> | pause | <packet rate
(1-2800)>}
```

no rate-limit

```
no rate-limit {output [rate-limit] | pause}
```

Parameters

Parameter	Type	Description
output		Enter to configure the egress packet rate of an interface.
rate-value		Enter to configure the rate-limit for the interface in Kbps. This is the number of packets that can be transferred on the port at a particular second.
<integer(1-80000000)>	Integer	Enter a value for the rate-limit for the interface in Kbps. This value ranges from 0 to 80000000. **NOTE:** The value 0 disables rate limiting for the port. It sets the port to full speed.
pause		Enter to configure that pause frames are sent.
<packet rate (1-2800)>	Integer	Enter a value for the packet rate above which pause frames are sent. This value ranges from 1 to 2800 packets per second.
rate-limit		Enter to disable the rate limiting rate limiting on an egress port. This is a part of the no form of the command.

Mode

Interface Configuration Mode

Default

- rate-value - 0

Examples

```
iS5comm # configure terminal
iS5comm(config)# interface gigabit 0/1
is5comm(config-if)# rate-limit output rate-value 1000
```

30.19. show access-lists

To display the access lists configuration, use the command **show access-lists** in Privileged EXEC Mode.

show access-lists

```
show access-lists
```

```
[{ip <access-list-number(1-65535)>
| mac <access-list-number(1-65535)>
| user-defined <access-list-number(1-65535)>}]
| <access-list-number(1-65535)>
```

Parameters

Parameter	Type	Description
ip		Enter to configure the configurations for the specified IP access-list to be displayed.
<access-list-number(1-65535)>		Enter a value for the configurations for the specified IP access-list to be displayed. The value ranges from 1 to 65535.
mac		Enter to configure the configurations for the specified MAC access-list to be displayed.
<access-list-number(1-65535)>		Enter a value for the configurations for the specified MAC access-list to be displayed. The value ranges from 1 to 65535.
user-defined		Enter to configure the configurations for the specified user-defined access-list to be displayed.
<access-list-number(1-65535)>		Enter a value for the configurations for the specified user-defined access-list to be displayed. The value ranges from 1 to 65535.
<access-list-number(1-65535)>		Enter a value for the configurations for the specified access-list to be displayed. The value ranges from 1 to 65535.

Mode

Privileged EXEC Mode

Examples

iS5comm# show access-list

```
    IP ACCESS LISTS
    -----------------
    Standard IP Access List 1
    ---------------------------
    Filter Priority                  : 10
     IP address Type                  : IPV4
     Source IP address                : 0.0.0.0
```

```
 Source IP address mask           : 0.0.0.0
 Source IP Prefix Length          : 0
 Destination IP address           : 0.0.0.0
 Destination IP address mask      : 0.0.0.0
 Destination IP Prefix Length     : 0
 Flow Identifier                  : 0
 In Port List                     : NIL
 Out Port List                    : NIL
 Filter Action                    : Deny
 Redirect Port List               : NIL
 TrafficDistField                 : Unknown
 Sub Action                       : NONE
 Sub Action Id                    : 0
 Status                           : InActive
Extended IP Access List 1001
-----------------------------
Filter Priority                 : 1
 Filter Protocol Type             : ICMP
 ICMP type                        : No
 ICMP types to be filtered ICMP code                          : No ICMP
codes to be filtered
 IP address Type                  : IPV4
 Source IP address                : 0.0.0.0
 Source IP address mask           : 0.0.0.0
 Source IP Prefix Length          : 0
 Destination IP address           : 0.0.0.0
 Destination IP address mask      : 0.0.0.0
 Destination IP Prefix Length     : 0
 Flow Identifier                  : 0
 In Port List                     : NIL
 Out Port List                    : NIL
 Service Vlan                     : 0
 Service Vlan Priority            : 0
 Customer Vlan                    : 0
 Customer Vlan Priority           : None
 Packet Tag Type                  : Single-tag
 Filter Action                    : Deny
 Redirect Port List               : NIL
 TrafficDistField                 : Unknown
 Sub Action                       : NONE
 Sub Action Id                    : 0
```

```
 Status                          : InActive

MAC ACCESS LISTS
-----------------
Extended MAC Access List 2
------------------------------
 Filter Priority                 : 1
 Ether Type                      : 0
 Protocol Type                   : 0
 VLAN ID                         : 0
 Destination MAC Address         : 00:00:00:00:00:00
 Source MAC Address              : 00:00:00:00:00:00
 In Port List                    : NIL
 Out Port List                   : NIL
 Outer EtherType                 : 0
 Service Vlan                    : 0
 Service Vlan Priority           : None
 Customer Vlan Priority          : None
 Packet Tag Type                 : Single-tag
 Drop precedence value           : 3
 Filter Action                   : Permit
 Redirect Port List              : NIL
 TrafficDistField                : Unknown
 Sub Action                      : MODIFY
 CFI/DEI Sub Action Id                  : 1
 Status                          : InActive

Extended MAC Access List 5
------------------------------
 Filter Priority                 : 1
 Ether Type                      : 0
 Protocol Type                   : 0
 VLAN ID                         : 0
 Destination MAC Address         : 00:00:00:00:00:00
 Source MAC Address              : 00:00:00:00:00:00
 In Port List                    : Gi0/10
 Out Port List                   : NIL
 Outer EtherType                 : 0
 Service Vlan                    : 0
 Service Vlan Priority           : None
```

```
 Customer Vlan Priority           : None
 Packet Tag Type                  : Single-tag
 Filter Action                    : Permit
 Redirect Port List               : NIL
 TrafficDistField                 : Unknown
 Sub Action                       : NONE
 Sub Action Id                    : 0
 Status                           : Active

 USER DEFINED LISTS
----------------------
 User Defined Access List 2
----------------------------
Priority                         : 1
 Packet Type                      : User-Defined
 Offset Base                      : L2
 OffSet Position                  :
 OffSet Value                     :
 Filter Action                    : Permit
 In Port List                     : NIL
 Filter One Type                  : None
 Filter Id                        : 0
 Filter Two Type                  : None
 Filter Id                        : 0
 Redirect Port List               : NIL
 TrafficDistField                 : Unknown
 Sub Action                       : NONE
 Sub Action Id                    : 0
 Status                           : InActive
```

30.20. show egress access-list mode

To display the egress filter mode configuration, use the command **show egress access-list mode** in Privileged EXEC Mode.

show egress access-list mode

```
show egress access-list mode
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show egress access-list mode

```
    Egress Filter Mode                : IP
```

30.21. show interfaces rate-limit

To display the interface status and configuration, use the command **show interfaces rate-limit** in Privileged EXEC Mode.

show interfaces rate-limit

```
show interfaces rate-limit
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show interfaces rate-limit

```
    Gi0/1
    Port Control Rate Limit : 64 kbps
    Port Control Burst Size : 32 kbits

    Gi0/2
    Port Control Rate Limit : 0 kbps
    Port Control Burst Size : 0 kbits

    Gi0/3
    Port Control Rate Limit : 0 kbps
    Port Control Burst Size : 0 kbits
```

30.22. show interfaces storm-control

To display interface status and configuration, use the command **show interfaces storm-control** in Privileged EXEC Mode.

show interfaces storm-control

```
show interfaces storm-control
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show interfaces storm-control

```
    Gi0/1
    DLF Storm Control           : Disabled
    Broadcast Storm Control     : Enabled
    Broadcast Storm Control Limit : 1000

    Multicast Storm Control     : Disabled

    Gi0/2
    DLF Storm Control           : Disabled
    Broadcast Storm Control     : Disabled
    Multicast Storm Control     : Disabled
```

30.23. storm-control

To set the storm control rate for broadcast, multicast, and DLF packets, use the command **storm-control** in Interface Configuration Mode. The no form of this command deletes the configured storm control rate for broadcast, multicast, and DLF packets to the default value.

storm-control

```
storm-control {broadcast |multicast | dlf} level <rate-value (1-262143)>
```

no storm-control

```
no storm-control <access-list-number (1-65535)> {in | out}
```

Parameters

Parameter	Type	Description
broadcast		Enter to set the storm control rate for Broadcast packets.
multicast		Enter to set the storm control rate for Multicast packets.
dlf		Enter to set the storm control rate for Destination lookup failure (dlf) packets. **NOTE:** Redirect Filter is not applicable for out bound packets.
level		Enter to configure the storm control suppression level.
<rate-value (1-262143)>	Integer	Enter a value for the storm control rate for Destination lookup failure (dlf) packets. This value ranges from 1 to 262143 packets per second.

Mode

Interface Configuration Mode

Default

Broadcast, multicast, and DLF storm control are disabled.

Prerequisites

Storm control is supported only on physical interfaces.

The above configurations are applicable per port level in ingress direction, not per device level. The value configured in level, should be applicable to the type (broadcast/multicast/dlf) whichever is configured.

Examples

```
iS5comm(config)# interface gigabit 0/1
is5comm (config-if)# storm-control broadcast level 1000
iS5comm (config-if)# end
iS5comm (config-if)# show interfaces storm-control
show interfaces storm-control
```

VRRP

31. VRRP

The Virtual Router Redundancy Protocol (VRRP) is a standard First Hop Redundancy Protocol (FHRP) that specifies an election protocol that dynamically assigns responsibility for a virtual router (VR) to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the Master and it forwards packets sent to these IP addresses. The election process provides dynamic failover in the forwarding responsibility, when the Master becomes unavailable. This will allow any virtual router (Master) IP addresses on the LAN to be used as the default gate for the hosts. The advantage of using VRRP is to provide a redundancy for the default gateways which used by endpoints.

In the VRRP, the Master router is responsible for forwarding the data packets received for VRRP MAC address. Backup routers listen for advertisement packets from the Master. In the case that Backup routers do not receive advertisement packets for a certain period of time from the Master, an election will start between backup routers to elect the new Master for VRRP interface.

31.1. VRRP Definitions

The following table gives definitions for some of the features used in this document.

Definitions

Acronym		Definitions
Accept Mode		Controls whether a virtual router in Master state will accept packets addressed to the virtual IP address (VRRP IP address). The default is False. Deployments that rely on, for example, pinging the address owner's IPvX address may wish to configure Accept Mode to True.
Preempt Mode		Controls whether a (starting or restarting) higher-priority Backup router preempts a lower-priority Master router.
Primary IP Address		An IPv4 address is selected from the set of real interface addresses. In IPv4 mode, VRRP advertisements are always sent using the primary IPv4 address as the source of the IPv4 packet. For adding a secondary IP address, the use the secondary one should be explicitly specified.
Priority		Priority value to be used by this VRRP router in Master election for this virtual router. The value of 255 (decimal) is reserved for the router that owns the IP address associated with the virtual router. The value of 0 (zero) is reserved for the Master router to indicate it is releasing responsibly for the virtual router. The range 1-254 (decimal) is available for VRRP routers backing up the virtual router. Higher values indicate higher priorities. The default value is 100 (decimal).
Router Advertisement		This is an ICMP packet used by routers to advertise their presence together with various link and Internet parameters either periodically. Router Advertisements contain prefixes that are used for determining whether another address shares the same link (on-link determination) and/or address configuration, a suggested hop limit value, etc.
VRRP Router		A router running VRRP. It may participate as one or more virtual routers.
Virtual Router (VR)		An abstract object managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a Virtual Router Identifier and either a set of associated IPv4 addresses or a set of associated addresses across a common LAN. A VRRP Router may back up one or more virtual routers. The scope of each virtual router is restricted to a single LAN.
Virtual Router Master		The VRRP router that is assuming responsibility of forwarding packets sent to the IP address(es) associated with the virtual router answering ARP requests.
Virtual Router Identifier (VRID)		This is the VRRP group number. It is configurable item in the range 1-255 (decimal). There is no default.

Reference

These definitions have been taken from

1) Network Working Group, RFC 3768 Virtual Router Redundancy Protocol (VRRP)

https://tools.ietf.org/html/rfc3768

31.2. auth-deprecate

To configure the interface related information, use the command **auth-deprecate** in VRRP Configuration Mode.

auth-deprecate

```
auth-deprecate {disable | enable}
```

Parameters

Parameter	Type	Description
disable		Enter to disable the Authentication Deprecation flag.
enable		Enter to enable the Authentication Deprecation flag

Mode

VRRP Configuration Mode

Examples

iS5comm(config)# router vrrp

iS5comm (config-vrrp)# vrrp version v3

31.3. interface

To configure the interface related information, use the command **interface** in VRRP Configuration Mode.

interface

```
interface {<ipiftype> | Extreme-Ethernet <0>/<1-28> | Gigabitethernet
<0>/<1-28> | vlan <vlan_vfi_id>}
```

no interface

```
no interface
```

Parameters

Parameter	Type	Description
ipiftype		Enter to set IP interface type.
Extreme-Ethernet		Enter to enable extreme Ethernet interface. This is a version of Ethernet that supports data transfer up to 10 Gbits per second. This Ethernet supports only full duplex links.
<0>/<1-28>		Enter to set slot number/port number.
Gigabitethernet		Enter to enable Gigabit Ethernet interface. This is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
vlan	Integer	Enter for VLAN related configuration.
<vlan_vfi_id>		Enter a value for the range. the range for VLAN ID is from 1 to 4094 and from 4096 to 65535 for VFI.

Mode

VRRP Configuration Mode

Examples

iS5comm(config)# router vrrp

iS5comm (config-vrrp)# interface vlan 55

31.4. router vrrp

To enable VRRP in the router and enter the VRRP Configuration Mode, use the command **router vrrp** in Global Configuration Mode. The no form of the command disables the VRRP.

router vrrp

```
router vrrp
```

no router vrrp

```
no router vrrp
```

Mode

Global Configuration Mode

Examples

iS5comm (config)# router vrrp

iS5comm (config-vrrp)#

31.5. track

To enables Link Track or IP track feature, use the command **track** in Global Configuration Mode. The no form of the command resets the number of links tracked if number of links is configured or disables the IP track feature.

track

```
track <group-index> {IPv4 address <IpAddress> | {interface {Extreme-Ethernet
<0>/<1-28> | Gigabitethernet <0>/<1-28> | vlan <vlan_vfi_id>} | links
<1-255>}
```

no track

```
no track <group-index> {IPv4 address <IpAddress> | {interface
{Extreme-Ethernet <0>/<1-28> | Gigabitethernet <0>/<1-28> | vlan
<vlan_vfi_id>} | links}
```

Link-track and IP-track

In a Link-track, if uplink of the Master fails, the forwarding capability of the router will be affected. In this case, Link-track feature is used. When an uplink of Master VRRP router goes down, a trigger is given to decrement Master router's priority, and after that, election process begins. Thus, Backup becomes Master Router and forwarding capability is carried by Backup router.

If any one of the uplinks comes up, the Master will send VRRP advertisement with its original priority and becomes Master. For example, in the current scenario, the number of links tracked can be 2. This means, that the number of links tracked is 2, and when any two uplinks of the Master go down, then, a trigger will be sent to the Master. Then, the Master will send the VRRP advertisement with the decreased priority, which is configured in VRRP instance as decrement priority.

In IP-track, if the tracked destination fails, the forwarding capability will be affected. In case, IP-tracking feature is used. When tracked IP address of Master VRRP router goes down, a trigger is given to decrement Master router's priority, and after that, election process begins. Thus, Backup becomes Master Router and forwarding capability is carried by Backup router.

When the uplink on the Master router changes its status to online, the reverse process occurs. The previous Master router advertises with original Priority, and after election, the previous Master becomes Master again.

Parameters

Parameter	Type	Description
ipiftype		Enter to set IP interface type.
IPv4		Enter to enable IPv4 related configuration
address		Enter to set the IP address of the node to be pinged.
<IpAddress>		Enter a value to specify the IP address of the node to be pinged
interface		Enter for interface related configuration.
Extreme-Ethernet		Enter to enable extreme Ethernet interface. This is a version of Ethernet that supports data transfer up to 10 Gbits per second. This Ethernet supports only full duplex links.
<0>/<1-28>		Enter to set slot number/port number.
Gigabitethernet		Enter to enable Gigabit Ethernet interface. This is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
vlan	Integer	Enter for VLAN related configuration.
<vlan_vfi_id>		Enter a value for the range. the range for VLAN ID is from 1 to 4094 and from 4096 to 65535 for VFI.
links		Enter the number of links to be tracked for the VRRP instance. By default, the number of links tracked is All (i.e. when all three uplinks of the Master go down, the Master will send the VRRP advertisement with decreased priority).
<1-255>		Enter to set tracked links value.

Mode

Global Configuration Mode

Examples

iS5comm(config)# track 30 interface vlan 1

31.6. vrrp

For the VRRP deployment on an interface, use the command **vrrp** in VRRP Interface Configuration Mode. The no form of the command resets all configured parameters.

vrrp

```
vrrp {<vrid (1-255>

 {accept-mode {disable | enable}

 | authentication {none | text <password>}

 | ip {<ip_addr> [secondary] | A.B.C.D <ip_addr>} | AAAA::BBBB <ipv6_addr>}
| accept-mode {disable | enable} | preempt [delay minimum <value(0-30)>] |
priority <priority (1-254)> | timer {advertise [msec] <interval(1-255secs) /
(10-255000msecs)> | msec <interval(1-255secs) /(10-255000msecs)> | track
<group-index (1-4294967295)> decrement <1-254>}

 | preempt [delay minimum <value (0-30)>]

 | priority <priority (1-254)>

 | text-authentication <password>}

 | timer {advertise [msec] <interval(1-255secs)/(10-255000msecs)> | msec
<interval(1-255secs)/(10-255000msecs)>

 | timers {advertise [msec] <interval(1-255secs)/(10-255000msecs)> | msec
<interval(1-255secs)/(10-255000msecs)>

 | track <group-index (1-4294967295)> decrement <1-254>}

 | group shutdown}
```

no vrrp

```
no vrrp {<vrid (1-255> [ipv4] {preempt | priority | timer | track} | ip
{<ip_addr> [secondary] | text-authentication}
```

Parameters

Parameter	Type	Description
<vrid(1-255)>	Integer	Enter to set the virtual router's (VR)'s ID.
accept-mode		Enter to configure Accept mode. Enabling Accept mode allows the Master VRRP device to respond to ping, traceroute, and Telnet/ SSH packets.
disable		Enter to disable Accept mode. This is the default option.
enable		Enter to enable Accept mode.
authentication		Enter to set authentication-related configuration. VRRP uses the authentication type associated with the interfaces on which the virtual router is defined. VRRP text authentication can be configured to authenticate VRRP packets. An advertisement packet will get discarded if the authentication key in the packet does not match the locally configured value.
none		Enter for no authentication.
text		Enter to set clear text authentication. A simple text password can be used.
<password>		Enter a value for authentication password used to validate the incoming VRRP packets.
ip		Enter to specify the IP address of a virtual router (VR). A VR can be associated with more than one IP address. When a router becomes the Master for an instance, it replies to the ARP request(s) for all associated with the VRRP instance IP addresses.
<ip_addr>		Enter a value for the IP address. The format is A.B.C.D
secondary		Enter to specify secondary IP Address.
A.B.C.D <ip_addr>		Enter a value for the IP address. The format is A.B.C.D
AAAA::BBBB <ipv6_addr>		Enter a value for IPv6 address.
preempt		Enter to specify which router becomes the master router and enable Preempt mode. Preemption of a backup VRRP device acting as a master device is allowed when another backup device has a higher priority. By default, preemption is enabled for VRRP. In VRRP, preemption allows a backup device with the highest priority to become the master device when the master device goes offline.

Parameter	Type	Description
delay		Enter to specify the number of seconds the router delays before issuing an advertisement claiming virtual IP address ownership to be the master router. By default preempt is Enabled and the delay value is 0 seconds (no delay).
minimum		Enter to specify the minimum number of seconds.
<value (0-30>	Integer	Enter a value for minimum number of seconds the router delays before issuing an advertisement claiming virtual IP address ownership to be the master router.
priority		Enter to establish a priority for a VR. A VR can be configured with a priority so that the router with higher priority will become the Master for that instance.
<priority (1-254)>	Integer	Enter a value for the priority for a VR. Priority can be configured from 1 to 254, with 1 being the lowest priority. A priority of 255 is used for the router that owns the associated IP address associated with the virtual router. The default is 110.
timer / timers		Enter to configure the interval between successive advertisements by the Master Router. The VRRP Master router sends a router advertisement at regular intervals to convey to the backup routers that the Master is alive. By default, the advertisement interval value is 1 second.
advertise		Enter to set the advertisement timer.
msec		Enter to specify that the unit is changed to milli-seconds.
<interval(1-255secs)/(10-255000msecs)>	Integer	Enter a value for the he interval between successive advertisements by the Master Router acceptable range for version 2 is (1-255 secs)/(100-255000 msecs) / acceptable range for version 2-3 and version 3 is (1-40 secs)/(10-40950 msecs). For example, timer 5 will configure the advertisement timer interval as 5 seconds.
track		Enter to configure tracking of the priority for a VR based on an interface.
<group-index (1-429496729)>	Integer	Enter a value for group Index Value.
decrement		Enter to configure the decrement.
<1-254>	Integer	Enter a value for the decrement with a default of 10.
text-authentication		Enter to set authentication password to be used to validate the incoming VRRP packet.

Parameter	Type	Description
<random_str>		Enter a value for authentication password used to validate the incoming VRRP packets.
group		Enter to set group related configuration.
shutdown		Enter to shut down the VRRP feature.

Mode

VRRP Interface Configuration Mode

Examples

iS5comm(config)# router vrrp

iS5comm (config-vrrp)# interface vlan 1

iS5comm(config-vrrp-if)# vrrp 1 accept-mode enable

iS5comm(config-vrrp-if)# vrrp 1 authentication text 1234

iS5comm(config-vrrp-if)# vrrp 1 ipv4 192.168.10.3

iS5comm(config-vrrp-if)# vrrp 1 ipv4 192.168.10.4

iS5comm(config-vrrp-if)# vrrp 1 preempt

iS5comm(config-vrrp-if)# vrrp 1 priority 200

iS5comm(config-vrrp-if)# vrrp 1 vrrp 1 text-authentication 1234

iS5comm(config-vrrp-if)# vrrp 1 timer 5

iS5comm(config-vrrp-if)# vrrp 1 timer msec 5000

iS5comm(config-vrrp-if)# vrrp 1 timers advertise 5

iS5comm(config-vrrp-if)# vrrp 1 track 30 decrement 150

iS5comm(config-vrrp-if)# vrrp group shutdown

31.7. vrrp version

To configure the VRRP version, use the command **vrrp version** in VRRP Configuration Mode.

vrrp version

```
vrrp version {v2 | v2-v3 | v3}
```

Parameters

Parameter	Type	Description
v2		Enter to enable VRRP Version 2. VRRP version 2 is intended for use with IPv4 routers only. For VRRPv2, no authentication methods are supported; these are deprecated in the VRRPv2 specification as they do not provide any additional security over the base protocol. For details, see RFC 3768 Virtual Router Redundancy Protocol (VRRP) https://tools.ietf.org/html/rfc3768
v2-v3		Enter to enable both VRRP Version 2 and Version 3. Use this mode to switch between both versions.
v3		Enter to enable VRRP Version 3. VRRP version 3 (VRRPv3) introduces IPv6 address support. For details, see RFC 5798 Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6, https://tools.ietf.org/html/rfc5798

Mode

VRRP Configuration Mode

Default

v2

Examples

iS5comm(config)# router vrrp

iS5comm (config-vrrp)# vrrp version v3

31.8. ip-tracking

To set the VRRP IP tracking feature, use the command **ip-tracking** in VRRP Configuration Mode. The VRRP object tracking describes how to track an IP object using a VRRPv3 group. Each VRRP group can track multiple objects that may affect the priority of the VRRP device. VRRP is notified of any changes to a specified object to be tracked. VRRP increments (or decrements) the priority of the virtual device based on the state of the object being tracked. The no form of the disables the IP tracking configuration.

ip-tracking

```
ip-tracking {query-delay <short(2-60)> | query-success <short(1-10)> |
ping-frequency <short(1-5)> | pings-per-query <short(1-10)> | connec-
tivity-success <short(1-10)> | connectivity-failure <short(1-10)>}
```

no ip-tracking

```
no ip-tracking {query-delay | query-success | ping-frequency |
pings-per-query | connectivity-success | connectivity-failure}
```

Parameters

Parameter	Type	Description
query-delay		Enter to configure delay between consecutive tracking queries
<short(2-60)>	Integer	Enter a value for the delay between consecutive tracking queries; default is 5.
query-success		Enter to configure the number of successful pings per tracking query for it to be a success.
<short(1-10)>	Integer	Enter a value for the number of successful pings per tracking query for it to be a success; default is 4
ping-frequency		Enter to configure frequency of pings within a tracking query (pings per second).
<short(1-5)>	Integer	Enter a value for the frequency of pings within a tracking query (pings per second); default is 2/sec
pings-per-query		Enter to configure number of pings per tracking query.
<short(1-10)>	Integer	Enter a value for the number of pings / tracking query; default is 5.
connectivity-success		Enter to configure number of consecutive successful tracking queries for raising the priority.
<short(1-10)>	Integer	Enter a value for number of consecutive successful tracking queries for raising the priority; default is 5.
connectivity-failure		Enter to configure number of failed tracking queries for lowering the priority.
<short(1-10)>	Integer	Enter a value for the number of failed tracking queries for lowering the priority; default is 2

Mode

VRRP Configuration Mode

Prerequisites

The VRRP IP Tracking Feature only works for VRRP Version 3. Include as follows:

iS5comm(config-vrrp)# vrrp version v3

Create a track group in Global Configuration Mode before setting the VRRP tracking feature.

Examples

iS5comm(config)# router vrrp

iS5comm (config-vrrp)# vrrp version v3

iS5comm(config-vrrp)# ip-tracking query-delay 2

iS5comm(config-vrrp)# ip-tracking query-success 1

iS5comm(config-vrrp)# ip-tracking pings-per-query 2

iS5comm(config-vrrp)# ip-tracking ping-frequency 2iS5comm(config-vrrp)# ip-tracking connectivity-success 1

iS5comm(config-vrrp)# ip-tracking connectivity-failure 1

31.9. show running vrrp

To display the current operating VRRP configuration in the system, use the command **show running vrrp** in Privileged EXEC Mode.

show running vrrp

```
show running vrrp
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show running vrrp

```
    #Building configuration...
    !
    !
    track 30 interface vlan 1
    router vrrp
    vrrp version v3
    interface vlan 1
```

```
vrrp 1 ipv4 192.168.10.4
vrrp 1 priority 200
vrrp 1 timer 5
vrrp 1 accept-mode enable
vrrp 1 track 30 decrement 150
end
!
end
```

31.10. show track

To display the VRRP track group Information., use the command **show track** in Privileged EXEC Mode.

show track

```
show track
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show track

```
Track Group Information for Group 30
-----------------------------------
Number of Links Required to go down for state transition: 0
Interfaces Tracked are
----------------------
vlan 1
```

31.11. show vrrp

To display the VRRP status, use the command **show vrrp** in Privileged EXEC Mode. The options are brief, detail, interface, and statistics.

show vrrp

```
show vrrp {brief | detail | interface <ipiftype> {Extreme-Ethernet
<0>/<1-28> | Gigabitethernet <0>/<1-28>} | statistics}
```

Parameters

Parameter	Type	Description
brief		Enter to display brief information.
detail		Enter to display detailed information.
interface		Enter to display interface related configuration.
<ipiftype>		Enter to identify IP interface type to be displayed.
Extreme-Ethernet		Enter to identify extreme Ethernet interface to be displayed. This is a version of Ethernet that supports data transfer up to 10 Gbits per second. This Ethernet supports only full duplex links.
<0>/<1-28>		Enter to identify slot number/port number to be displayed.
Gigabitethernet		Enter to identify Gigabit Ethernet interface to be displayed. This is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
statistics		Enter to display statistics related information.

Mode

Privileged EXEC Mode

Examples

iS5comm# show vrrp

```
    P indicates configured to preempt

    Interface vrID Prio P State  Master Address    VRouter Address

    --------- ---- ---- - -----  -------------- ------------------

    vlan1      1    200  P Master 192.168.10.1       192.168.10.3
```

iS5comm(config)# show vrrp brief

```
    P indicates configured to preempt

    Interface vrID Prio P State  Master Address    VRouter Address

    --------- ---- ---- - -----  -------------- ------------------
```

```
    vlan1      1    200  P Master 192.168.10.1       192.168.10.3
```

iS5comm(config)# show vrrp detail

```
    lan1  - vrID 1
    ------------------
    State is Master
    Virtual IP address is 192.168.10.3
    Virtual MAC address is 00:00:5e:00:01:01
    Master router is 192.168.10.1
    Associated IpAddresses :
    ----------------------
    192.168.10.3
    Advertise time is 5000 milli secs
    Current priority is 200
    Configured priority is 200, may preempt
    Tracked Group is 30, Decrement Priority is 150
    Tracked Group is UP
    Accept Mode is Enabled
    Time Since Virtual Router is UP is 00:08:57
```

iS5comm(config)# show vrrp interface

```
    P indicates configured to preempt

    Interface vrID Prio P State  Master Address    VRouter Address
    --------- ---- ---- - -----  -------------- ------------------

    vlan1      1    200  P Master 192.168.10.1       192.168.10.3
```

iS5comm(config)# show vrrp interface gi 0/1 1

```
    P indicates configured to preempt

    Interface vrID Prio P State  Master Address            VRouter Address

    --------- ---- ---- - -----  -------------------------
    -------------------------
```

iS5comm(config)# show vrrp statistics

```
    RRP Statistics
    ---------------
    Router Checksum Errors          : 0
    Router Version Errors           : 0
    Router VrId Errors              : 0
```

```
vlan1  - vrID 1
------------------
Transitions to Master          : 13
Advertisements Received        : 0
Advertise Interval Errors      : 0
TTL Errors                     : 0
Zero Priority Packets Received : 0
Zero Priority Packets Sent     : 12
Invalid Type Packets Received  : 0
Address List Errors            : 0
Packet Length Errors           : 0
V3 Advertisements Sent         : 1419
V2 Advertisements Sent         : 8730
V2 Advertisements Ignored      : 0
New Master Reason              : Master No Response
Last Protocol Error            : No Error
```

Alarms

32. Alarms

The software monitors the conditions of all its ports, per switch, for its chassis, or if they are Alarms security, services, and protocol -related.

The software monitors the conditions of all its ports, per switch, for its chassis, or if they are Alarms security, services, and protocol -related.

If a condition which is present on the switch or a port does not match predetermined parameters, an alarm or a system message appear. By default, the switch software sends the system messages to a syslog facility. The switch can be configured to send Simple Network Management Protocol (SNMP) traps to an SNMP server.

All alarms which are related to power supply failure; CPU/RAM/Flash/Temperature/Line Module mismatch or a chassis type are referred as global alarms. The switch can also monitor the status of the Ethernet ports and generate alarm messages which are categorized as Port Status Monitoring Alarms.

There are eight different categories of alarms as depicted in the below table. GPS and cell alarms are not currently defined as the base feature is not available yet.

No. & Type	ID Range	Events
1 - Admin	1000 - 1999	Administrative aspect of the device, such as license key problems, etc.
2 - Chassis	2000 - 2999	Alarms related to power supply failure; CPU / RAM / Flash / Temperature / Line Module mismatch.
3 - Switch	3000 - 3999	Port link up/down; SFP not compatible, etc
4 - Security	4000 - 4999	Invalid login; SNMP authentication failure
5 - Services	5000 - 5999	Alarms related to software download failure/syslog buffer overflow/ login failures
6 - Protocol	6000 - 6999	All protocol-related alarms like STP root change, VRRP role change, etc
7 - Cell	Not defined yet	-
8 - GPS	Not defined yet	-

32.1. Example

For interface-specific alarms such as link up/down, the alarm ID is the sum of the base alarm ID plus the port no. For example, the port 11 link up / down alarm is denoted by ID 3011 (i.e. 3000 +11).

```
ID    TYPE      TIMESTAMP      STATE DESCRIPTION              SEVERITY
-------------------------------------------------------------------------
3011 SWITCH Sep/10/19:43:28  SET   Gi0/11 Interface Link State DOWN
Critical
```

32.2. Alarm events covered – First phase

All critical alarms will have the Relay feature and red LED enabled by default.

No. & Type	Description	Threshold & Severity
1 - Switch	Link UP / DOWN event	N/A - Critical
2 - Chassis	Main board temperature threshold	10 to +40 - Alert
3 - Chassis	CPU over usage	80% - Alert
4 - Chassis	Flash over usage threshold	80% - Alert
5 - Chassis	RAM over usage threshold	80% - Alert
6 - Security	Invalid log-in	N/A - Alert
7 - Services	Firmware upgrade fail	N/A - Error
8 - Protocol	VRRP master change	N/A - Info
9 - Protocol	RSTP root bridge node	N/A - Info

NOTE: The most essential alarms are to be installed during the first phase; later, we will increase the number of alarms. Request QA to help on identifying the alarms.

Relay and LED for Alarms

By default, all critical severity alarms are enabled with Relay and RED LED indication . The LED and relay are triggered during the first occurrence of fault and cleared during the next occurrence of fault clearance. Some examples are as follows.

iS5comm# show alarm history all

```
ID    TYPE      TIMESTAMP      STATE          DESCRIPTION
SEVERITY
-------------------------------------------------------------------------
-------
```

```
3024  SWITCH   May/2/07:48:01   SET   Gi0/24 Interface link state DOWN
Critical
3024  SWITCH   May/2/07:48:03   CLR   Gi0/24 Interface link state UP
Critical
3037  SWITCH   May/2/07:48:03   CLR   vlan1 Interface link state UP
Critical
3037  SWITCH   May/2/07:48:04   SET   vlan1 Interface link state DOWN
Critical
3024  SWITCH   May/2/07:48:07   CLR   Gi0/24 Interface link state UP
Critical
3037  SWITCH   May/2/07:48:07   CLR   vlan1 Interface link state UP
Critical
3037  SWITCH   May/2/07:48:08   SET   vlan1 Interface link state DOWN
Critical
3024  SWITCH   May/2/07:48:08   SET   Gi0/24 Interface link state DOWN
Critical
3024  SWITCH   May/2/07:48:13   CLR   Gi0/24 Interface link state UP
Critical
3037  SWITCH   May/2/07:48:13   CLR   vlan1 Interface link state UP
Critical
3037  SWITCH   May/2/10:32:29   SET   vlan1 Interface link state DOWN
Critical
4000  SECURITY May/6/01:50:17   SET   Invalid login
Alert
4000  SECURITY May/6/01:50:29   CLR   Invalid login
Alert
```

show alarm history switch

```
ID    TYPE      TIMESTAMP      STATE          DESCRIPTION
SEVERITY
-------------------------------------------------------------------------
-------
3024  SWITCH   May/2/07:48:01   SET   Gi0/24 Interface link state DOWN
Critical
3024  SWITCH   May/2/07:48:03   CLR   Gi0/24 Interface link state UP
Critical
3037  SWITCH   May/2/07:48:03   CLR   vlan1 Interface link state UP
Critical
3037  SWITCH   May/2/07:48:04   SET   vlan1 Interface link state DOWN
Critical
```

32.3. set alarm

To enable or disable globally the alarm module, use the command **set alarm** in Global Configuration Mode. When the module is disabled, the alarms are not captured.

set alarm

```
set alarm {disable | enable}
```

Parameters

Parameter	Type	Description
disable		Enter to disable the alarm module.
enable		Enter to enable the alarm module. This is default.

Mode

Global Configuration Mode

Default

enable

Examples

iS5comm(config)# set alarm enable

32.4. alarm buffered

To configure the number of alarm messages to be hold in RAM, use the command **alarm buffered** in Global Configuration Mode. The no form of the command resets the alarm level to its default value.

alarm buffered

```
alarm buffered <100-2048>
```

no alarm buffered

```
no alarm buffered
```

Parameters

Parameter	Type	Description
<100-2048>	Integer	Enter a value for the number of alarm messages to be hold in RAM. The configurable numbers are between 100 to 2048 entries. 512 is default.

Mode

Global Configuration Mode

Default

512 (entries)

Examples

iS5comm(config)# alarm buffered 1024

32.5. alarm config-type

To enable / disable alarm's administrative state, relay feature, or LED feature based on its type, use the command **alarm config-type** in Global Configuration Mode.

alarm config-type

```
alarm config-type
 {{switch | admin | chassis | security | protocol | service}
 {admin | relay | LED} {enable | disable}}
```

Parameters

Parameter	Type	Description
switch		Enter to enable switch type alarm.
admin		Enter to enable admin type alarm.
chassis		Enter to enable chassis type alarm.
security		Enter to enable security type alarm.
protocol		Enter to enable protocol type alarm.
service		Enter to enable service type alarm.
admin		Enter to enable / disable alarm's administrative state based on its type.
relay		Enter to enable / disable alarm's relay feature based on its type.
LED		Enter to enable / disable alarm's LED feature based on its type
enable		Enter to enable alarm's administrative state, relay feature, or LED feature based on its type
disable		Enter to disable alarm's administrative state, relay feature, or LED feature based on its type

Mode

Global Configuration Mode

Default

All alarms are disabled

Examples

iS5comm(config)# alarm config-type admin admin enable

iS5comm(config)# alarm config-type admin relay enable

iS5comm(config)# alarm config-type admin LED enable

32.6. show active alarms

To display all active [SET] alarms, use the command **show active alarms** in Privileged EXEC Mode.

show active alarms

```
show active alarms
```

Mode

Privileged EXEC Mode

Examples

iS5comm# show active alarms

```
ID    TYPE      TIMESTAMP      STATE DESCRIPTION              SEVERITY
------------------------------------------------------------------------
2000  CHASSIS  Sep/10/17:47:18  SET   Power supply limit exceeded
Alert
6000  PROTOCOL Sep/10/17:47:08  SET   RSTP root bridge node
Info
3011  SWITCH   Sep/10/19:43:28  SET   Gi0/11 Interface Link State DOWN
Critical
3025  SWITCH   Sep/10/17:47:08  SET   Ex0/1 Interface Link State DOWN
Critical
3026  SWITCH   Sep/10/17:47:08  SET   Ex0/2 Interface Link State DOWN
Critical
3027  SWITCH   Sep/10/17:47:08  SET   Ex0/3 Interface Link State DOWN
Critical
3028  SWITCH   Sep/10/17:47:08  SET   Ex0/4 Interface Link State DOWN
Critical
3037  SWITCH   Sep/22/17:59:50  SET   vlan1 Interface Link State DOWN
Critical
```

32.7. show alarm history

To display alarms for all alarm types—both SET and CLEARED, use the command **show alarm history** in Privileged Exec Mode.

show alarm history

```
show alarm history
 {all |switch | admin | chassis | security | protocol | service}
```

Parameters

Parameter	Type	Description
all		Enter to specify all alarms to be displayed.
switch		Enter to specify switch type alarm to be displayed.
admin		Enter to specify admin type alarm to be displayed.
chassis		Enter to specify chassis type alarm to be displayed.
security		Enter to specify security type alarm to be displayed.
protocol		Enter to specify protocol type alarm to be displayed.
service		Enter to specify service type alarm to be displayed.

Mode

Privileged Exec Mode

Default

All alarms are disabled

Examples

iS5comm# show alarm history all

```
ID    TYPE      TIMESTAMP      STATE          DESCRIPTION
SEVERITY
-------------------------------------------------------------------------
-------
3024  SWITCH   May/2/07:48:01   SET   Gi0/24 Interface link state DOWN
Critical
3024  SWITCH   May/2/07:48:03   CLR   Gi0/24 Interface link state UP
Critical
3037  SWITCH   May/2/07:48:03   CLR   vlan1 Interface link state UP
Critical
3037  SWITCH   May/2/07:48:04   SET   vlan1 Interface link state DOWN
Critical
3024  SWITCH   May/2/07:48:07   CLR   Gi0/24 Interface link state UP
Critical
3037  SWITCH   May/2/07:48:07   CLR   vlan1 Interface link state UP
Critical
```

```
3037  SWITCH   May/2/07:48:08   SET   vlan1 Interface link state DOWN
Critical
3024  SWITCH   May/2/07:48:08   SET   Gi0/24 Interface link state DOWN
Critical
3024  SWITCH   May/2/07:48:13   CLR   Gi0/24 Interface link state UP
Critical
4000  SECURITY May/6/01:50:17   SET   Invalid login
Alert
4000  SECURITY May/6/01:50:29   CLR   Invalid login
Alert
```

show alarm history switch

```
ID    TYPE      TIMESTAMP      STATE          DESCRIPTION
SEVERITY
-------------------------------------------------------------------------
-------
3024  SWITCH   May/2/07:48:01   SET   Gi0/24 Interface link state DOWN
Critical
3024  SWITCH   May/2/07:48:03   CLR   Gi0/24 Interface link state UP
Critical
3037  SWITCH   May/2/07:48:03   CLR   vlan1 Interface link state UP
Critical
3037  SWITCH   May/2/07:48:04   SET   vlan1 Interface link state DOWN
Critical
```

32.8. show alarm supported

To display all supported alarms, use the command **show alarm supported** in Privileged Exec Mode.

show alarm supported

```
show alarm supported
 {all |switch | admin | chassis | security | protocol | service}
```

Parameters

Parameter	Type	Description
all		Enter to specify all alarms to be displayed.
switch		Enter to specify switch-related alarms to be displayed.
admin		Enter to specify admin-related alarms to be displayed.
chassis		Enter to specify chassis-related alarms to be displayed.
security		Enter to specify security-related alarms to be displayed.
protocol		Enter to specify protocol-related alarms to be displayed.
service		Enter to specify service-related alarms to be displayed.

Mode

Privileged Exec Mode

Examples

show alarm supported all

```
ALARM-ID    ALARM-SUPPORTED
---------  ------------------

2000        Power supply limit exceeded
2001        Main Board Temperature overheat
2002        CPU usage over-threshold
2003        Flash usage over-threshold
2004        RAM usage over-threshold
2005        Power supply not operational
2006        Line card state

3000        Interface link state
3001        Cyber-security link
3002        Line module temperature threshold reached

4000        Invalid login

5000        Firmware upgrade failed
```

```
6000        RSTP root bridge node
6001        VRRP master - VRID
6002        MRP Ring status changed
6003        MRP Multiple MRM condition
```

PoE

33. PoE

The RAPTOR may be ordered from the factory with support for Power over Ethernet, PoE, in which case it requires an external power supply to provide the PoE power to the line modules. The RAPTOR supports IEEE 802.3af (15.4W), IEEE 802.3at PoE+ (30W), and IEEE 802.3bt Type 3 (60W).

The RAPTOR chassis supports up to 720W of PoE, where slots 1-3 each may deliver up to a maximum of 240W each.

This section describes the CLI commands available to monitor and configure the PoE capabilities.

33.1. set poe

The **set poe** command is used enable or disable PoE services in Global Configuration Mode.

set poe

```
set poe {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enables Power over Ethernet module in the switch
disable		Disables Power over Ethernet module in the switch

Mode

Global Configuration Mode

Examples

iS5comm# configure terminal

iS5comm(config)# set poe enable

33.2. show power

To view the current internal state of the PoE feature on the device, use the **show power** command in Privileged EXEC Mode.

show power

```
show power { counters
 [ Extreme-Ethernet <0>/<1-28> | Gigabitethernet <0>/<1-28> ] | detail |
inline
 [ Extreme-Ethernet <0>/<1-28> | Gigabitethernet <0>/<1-28> ] }
```

Parameters

Parameter	Type	Description
counters		PoE counter related Information
detail		PoE related information
inline		PoE inline configuration
Extreme-Ethernet		This option is not supported and will be removed from iBiome in a future release.
Gigabitethernet		Gigabit Ethernet Interface <Chassis Number>/<Port Number>

Mode

Privileged EXEC Mode

Examples - Power Counters

iS5comm# show power counters

```
iS5comm# show power counters

PoE Port Counters
-----------------

PoeInterface          MPSAbsent  InvalidSign  PowerDenied  OverLoad   Short
--------------------  ---------  -----------  -----------  ---------  ---------
gigabitethernet 0/1           0            0            0          0          0
gigabitethernet 0/2           0            0            0          0          0
gigabitethernet 0/3           0            0            0          0          0
gigabitethernet 0/4           0            0            0          0          0
gigabitethernet 0/5           0            0            0          0          0
gigabitethernet 0/6           0            0            0          0          0
gigabitethernet 0/7           0            0            0          0          0
gigabitethernet 0/8           0            0            0          0          0
gigabitethernet 0/9           0            0            0          0          0
gigabitethernet 0/10          0            0            0          0          0
gigabitethernet 0/11          0            0            0          0          0
gigabitethernet 0/12          0            0            0          0          0
gigabitethernet 0/13          0            0            0          0          0
gigabitethernet 0/14          0            0            0          0          0
gigabitethernet 0/15          0            0            0          0          0
gigabitethernet 0/16          0            0            0          0          0
gigabitethernet 0/17          0            0            0          0          0
--More--
```

Example - Power Counters, single interface

iS5comm# show power counters gigabitethernet 0/1

```
iS5comm# show power counters gigabitethernet  0/1

PoE Port Counters Info
----------------------
PoeInterface            : gigabitethernet 0/1
MPSAbsentCounter        : 0
InvalidSignatureCounter : 0
PowerDeniedCounter      : 0
OverLoadCounter         : 0
ShortCounter            : 0

iS5comm#
```

Example - Power Detail

iS5comm# show power detail

```
iS5comm# show power detail

PSE Status
----------
PoE Global Admin State     : Disabled
PSE Operational Status     : Off
Max Power Supplies         : 0
Total Power Available (W)  : 720
Total Power Consumed (W)   : 0
Voltage Supplied (V)       : 0.00
PSE Detection Mode         : Legacy

iS5comm#
```

Example - Power Inline

iS5comm# show power inline

```
iS5comm# show power inline

PoE Port Info
-------------

PoeInterface          AdminState  DetectionStatus   Class  Priority  Power(W)
--------------------  ----------  ----------------  -----  --------  --------
gigabitethernet 0/1   Down        OtherFault        0      Low        0.00
gigabitethernet 0/2   Down        OtherFault        0      Low        0.00
gigabitethernet 0/3   Down        OtherFault        0      Low        0.00
gigabitethernet 0/4   Down        OtherFault        0      Low        0.00
gigabitethernet 0/5   Down        OtherFault        0      Low        0.00
gigabitethernet 0/6   Down        OtherFault        0      Low        0.00
```

Example - Power Inline, single interface

iS5comm# show power inline gigabitethernet 0/1

```
iS5comm# show power inline gigabitethernet 0/1

PoE Port Info
-------------
PoeInterface        : gigabitethernet 0/1
PoeAdminStatus      : Down
PoeDetectionState   : Other Fault
Class               : 0
Priority            : Low
PowerPairsMax       : Two
Power Consumed (W)  : 0.00

iS5comm#
```

33.3. show poe state

To view the current internal state of the PoE feature on the device, use the **show poe** command in Privileged EXEC Mode. This is a debug level command, and it is meant to be used by iS5 support staff. End users are free to use this command, however, it may not be interpretable by all users.

show poe

```
show poe {state}
```

Parameters

Parameter	Type	Description
state		Current PoE internal state

Mode

Privileged EXEC Mode

Examples

iS5comm# show poe state

```
PoE State Info
-------------
PoE Conf MIB: En=0, Pwr=720, Detect=Strict (Chassis-support=1)
Port-En: 00000000 00000000 00000000
Port-Pri: 33333333 33333333 33333333
Port-Pairs: 22222222 22222222 22222222
PoE Drag: En=0, ErrState=OK, Starts=0, Slots-HW:0=OK-OK-OK
Dropped messages[819]:
PoeGetPseStatus
PoE Logs: Mon Jan 14 19:02:58 2019
```

33.4. power inline

The **power inline** command is used to set the detection method of the PoE links. To define the maximum power that can be delivered by the external PoE Power Supply, use the **power inline** command in Global Configuration Mode.

power inline

```
power inline { detect [ legacy | strict ] | max-power-supply < 100 - 6000 > }
```

Parameters

Parameter	Type	Description
`detect legacy`		Sets the Power Over Ethernet to legacy detect mode. Legacy mode is for old PoE devices, which are not IEEE compliant.
`detect strict`		Sets the Power Over Ethernet to strict detect mode. This is meant for IEEE supported devices.
`max-power-supply`		Max-power-supply is followed by an integer value with a range of 100 - 6000. This value denotes the maximum wattage the external PoE power supply or supplies can provide to the switch. External Power Supplies may be wired in parallel. This value is used as follows: The switch will only provide power to PoE devices up to this value. The max-power-supply, if set too high, might cause devices to be oversubscribed, and all devices will become starved for power. If the calculated power consumption exceeds the max-power-supply and when too much power is drawn, PoE devices will be shut down. The order is determined by PoE Port Priority and Numbering. The lower the port number, the higher the priority.

Mode

Global Configuration Mode

Examples

iS5comm (config)# power inline detect legacy

iS5comm (config)# power inline detect strict

iS5comm (config)# power inline max-power-supply 720

33.5. power inline (interface)

To set the configure interface specific PoE settings, use the **power inline** command in Interface Configuration Mode.

power inline

```
power inline { auto | maxpairs < two | four > | never | priority < critical | high | low > }
```

Parameters

Parameter	Type	Description
auto		Enable and apply Power Over Ethernet if the device requires power.
maxpairs		Use this command to specify if PoE power is to provided on up to two or four pairs of wires. It is followed by the value **two** or **four**. IEEE 802.3af (up to 15.4 Watts) and IEEE 802.3at (up to 30 Watts) use two pairs of wires to supply PoE power. IEEE 802.3bt can uses four pairs to supply up to 60W of PoE power, however to ensure power consumption limits the adjacent port (odd/even combination) needs to be disabled before this can be set.
never		Disables PoE on the port and disables power to the port.
priority		Priority related configuration. The PoE port priority may be set as critical, high or low. The priority and port numbering are used to determine which ports are shut down in the event that there is not sufficient power for all PoE ports. The ports are grouped by their priority levels where critical is the last group to get shut down and low would be the first to lose power. Within those groupings preference is determined by port numbering. Example: Port 24 - critical would be shut down after Port 1 - low, but before Port 23 - critical.

Mode

Interface Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# interface gigabitethernet 0/1

iS5comm (config-if)# power inline auto

iS5comm (config-if)# power inline maxpairs two

iS5comm (config-if)# power inline priority high

iS5comm (config-if)# power inline never

HSR

34. HSR-PRP

High-availability Seamless Redundancy (*HSR*) is a redundancy protocol that:

- provides short switchover time in case of failure,
- provides seamless failover against failure of any single network component
- allows to chain nodes for cost effective networking,
- allows complex ring topology,
- is easily implemented in hardware,
- supports deterministic transmission of highest priority frames, and
- is standardized as per IEC 62439-3 Clause 5

The following *CLI* commands outline how to configure redundancy interface, redundancy / bypass mode, different types of *HSR* operational modes, *LRE* parameters, and how to verify the configuration.

34.1. redundancy

To configure interface redundancy, use the command **redundancy** in Global Configuration Mode.

redundancy

```
redundancy  {<integer (1-8)>} [name <string(64)>]
```

Parameters

Parameter	Type	Description
`integer (1-8)`		Enter to configure interface redundancy and enter specific *LRE* Redundant Interface Configuration Mode. Up to 8 interfaces can be defined.
`name <string(64)>`		Enter to a assign a name with up to 64 characters a redundant interface. This is an optional parameter.

Mode

Global Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# redundancy 1

iS5comm(config-if-red1)#

34.2. redundancy

To configure redundancy or bypass mode, use the command **redundancy** in *LRE* Redundant Interface Configuration Mode.

redundancy

```
redundancy {enable | disable}
```

Parameters

Parameter	Type	Description
enable		Enter to configure redundancy mode. By default, redundancy is enabled.
disable		Enter to configure bypass mode.

Mode

LRE Redundant Interface Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# redundancy 1

iS5comm(config-if-red1)# redundancy disable

34.3. mode

To configure the redundancy mode, use the command **mode** in *LRE* Redundant Interface Configuration Mode.

mode

```
mode {hsr | prp | hsr-hsr | hsr-prp-a netid <integer (1-7)> | hsr-prp-b
netid <integer (1-7)>}
```

Parameters

Parameter	Type	Description
`hsr`		Enter for *HSR* mode.
`prp`		Enter for *PRP* mode. This is the default mode.
`hsr-hsr`		Enter for HSR - HSR mode (QuadBox mode). In this mode, two redundant switches are connected to each other via PONCAT a.k.a. Gigabit / Extreme Ethernet) ports using PCL Rules.
`hsr-prp-a`		Enter for HSR-PRP A mode (Dual RedBox mode). In this mode, two different RedBoxes connect to LAN A and LAN B of the PRP network.
`netid <integer (1-7>`		Enter the net ID for the HSR-PRP mode. The net ID defines a *PRP* network and the two RedBoxes that connect the *PRP* network to an *HSR* ring. Netid values are from 1 to 7 and are follow: • 0 for regular HSR frames • 1 to 6 for frames originating from a PRP network • 7 is reserved When a *PRP* frame from LAN A or LAN B of a PRP network with a given netid is inserted to the *HSR* ring, the RedBox inserts its own netid into the PathId field of the *HSR* tag (header).
`hsr-prp-b`		Enter for HSR-PRP B mode (Dual RedBox mode). In this mode, two different RedBoxes connect to LAN A and LAN B of the PRP network.

Mode

LRE Redundant Interface Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# interface redundant 1

iS5comm(config-if-red1)# mode hsr-prp-a netid 5

34.4. hsr-operational-mode

To configure the *LRE HSR* Operational Mode, use the command **hsr-operational-mode** in *LRE* Redundant Interface Configuration Mode.

hsr-operational-mode

```
hsr-operational-mode {modeh | moden | modet |modeu}
```

Parameters

Parameter	Type	Description
modeh		Enter for Mode H—the HSR-tagged forwarding mode. This is the default normal and mandatory mode.
moden		Enter for Mode N—the optional No Forwarding mode. Select if the HSR network is built in the same way as PRP networks—with double star topology
modet		Enter for Mode T—the optional Transparent Forwarding mode.
modeu		Enter for Mode U—the optional Unicast Forwarding mode. Here, the ring port will send unicast traffic unaltered to the other ring port as well as to Interlink without HSR header.

Mode

LRE Redundant Interface Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# redundancy 1

iS5comm(config-if-red1)# hsr-operational-mode moden

iS5commconfig-if-red1)# mode hsr

34.5. default

To go back to the default interface redundancy configuration, use the command **default** in *LRE* Redundant Interface Configuration Mode. When a switch is back to the default interface redundancy configuration, we have LRE disabled (shut down), PRP mode, port A and B being active as well as “supervisory-expiry-time” and “proxy-expiry-time” of 60 seconds.

default

```
default
```

Mode

LRE Redundant Interface Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# redundancy 1

iS5comm(config-if-red1# default

34.6. no shutdown

To enable the *LRE*, (active redundant mode), use the command **no shutdown** in *LRE* Redundant Interface Configuration Mode. By default, *LRE* is enabled.

no shutdown

```
no shutdown
```

Mode

LRE Redundant Interface Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# redundancy 1

iS5comm(config-if-red1)# no shutdown

34.7. shutdown

To disable the *LRE*, use the command **shutdown** in *LRE* Redundant Interface Configuration Mode. Weh the *LRE* is shut down, the *RED* in the Configuration Redundant mode and it is not active. Any protocol related modifications should be done when the *RED* is in Configuration Redundant mode.

shutdown

```
shutdown
```

Mode

LRE Redundant Interface Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# redundancy 1

iS5comm(config-if-red1)# shutdown

34.8. proxy-expire-time

To configure the *LRE* proxy node expire time, use the command **proxy-expire-time** in *LRE* Redundant Interface Configuration Mode.

proxy-expire-time

```
proxy-expire-time <integer (0-1023)>
```

Parameters

Parameter	Type	Description
<integer (0-1023)>	Integer	Enter a value (in seconds) for proxy node expire time. The default is 60 seconds.

Mode

LRE Redundant Interface Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# redundancy 1

iS5comm(config-if-red1)# proxy-expire-time 55

34.9. supervisory-expire-time

To configure the *LRE* supervisory node expire time, use the command **supervisory -expire-time** in *LRE* Redundant Interface Configuration Mode.

supervisory -expire-time

```
supervisory -expire-time <integer (0-1023)>
```

Parameters

Parameter	Type	Description
<integer (0-1023)>	Integer	Enter a value (in seconds) for supervisory node expire time. The default is 60 seconds.

Mode

LRE Redundant Interface Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# interface redundant 1

iS5comm(config-if-red1)# supervisory-expire-time 60

34.10. port

For port speed configuration, use the command port in *LRE* Redundant Interface Configuration Mode. Ports a and b can be enabled / disabled even during the “active” state.

port

```
port {A | B} speed <integer>
```

Parameters

Parameter	Type	Description
A		Enter for Port-A.
B		Enter for Port-B.
speed		Enter to define the speed of the selected port.
<integer>	Integer	Enter the speed of the selected port.

Mode

LRE Redundant Interface Configuration Mode

Examples

S5comm# configure terminaliS5comm(config)# redundancy 1iS5comm(config-if-red1)# port A down

34.11. debug hst-prp

To enable the trace levels for HSR-PRP, use the command **debug hst-prp** in Privileged EXEC Mode.

debug hst-prp

```
debug hst-prp {all | trace | data | info | critical | none}
```

Parameters

Parameter	Type	Description
`all`		Enter to specify generating of debug messages for all possible traces.
`trace`		Enter to specify generating of debug messages on trace level.
`data`		Enter to specify generating of debug statements for data path traces.
`info`		Enter to specify generating of debug statements on info level.
`critical`		Enter to specify generating debug statements on critical level.
`none`		Enter to specify not generating debug statements.

Mode

Privileged EXEC Mode

Examples

iS5comm # debug hst-prp all

34.12. clear counters redundant

To clear the counters of the node table, use the command **clear counters redundant** in *LRE* Redundant Interface Configuration Mode.

clear

```
clear counters redundant [<integer (1-8)>] {node-table | proxy-node-table}
```

Parameters

Parameter	Type	Description
<integer (1-8)>		Enter the number of redundant interface to have counters cleared.
node-table		Enter to clear the counters of the node table.
proxy-node-table		Enter to clear the counters of the proxy node table.

Mode

LRE Redundant Interface Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# redundancy 1

iS5comm(config-if-red1)# clear counters redundant 1 node-table

34.13. clear interfaces redundant

To clear the counters of the redundant interface, use the command **clear interfaces redundant** in Global Configuration Mode.

clear

```
clear interface redundant <red-id (1-8)> counters
```

Parameters

Parameter	Type	Description
red-id (1-8)		Enter the number of redundant interface to be cleared.
counters		Enter to clear the counters of the redundant interface.

Mode

Global Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# clear interfaces redundant 1 counters

34.14. show interfaces counters redundant

To display the redundant interface counters, use the command **show interfaces counters redundant** in Privileged EXEC Mode.

show

```
interfaces counters redundant [<integer (1-8)>]
```

Parameters

Parameter	Type	Description
integer (1-8)	Integer	Enter a number for a specific redundant interface to be displayed.

Mode

Privileged EXEC Mode

Examples

iS5comm# show interfaces counters redundant

34.15. show redundancy

To display the *LRE*-specific or for all *LRE* node table, proxy node table, configuration, or map, use the command **show redundancy** in Privileged EXEC Mode.

show

```
redundancy [<integer (1-8)>] {node-table | proxy-node-table | config | map}
```

Parameters

Parameter	Type	Description
`integer (1-8)`	Integer	Enter a number for a specific redundant interface to be displayed.
`node-table`		Enter to display an LRE-specific or for all LREs node table.
`proxy-node-table`		Enter to display an LRE-specific or for all LREs proxy-node table.
`config`		Enter to display an LRE-specific or for all LREs configuration.
`map`		Enter to display an LRE-specific or for all LREs map.

Mode

Privileged EXEC Mode

Examples

iS5comm# show redundancy node-table

NAT Map

35. NAT

Network Address Translation (NAT) is a method by which IP addresses are mapped from one realm to another, in an attempt to provide transparent routing to hosts. Reference, RFC 2663

The need for IP Address translation arises when a network's internal IP addresses cannot be used outside the network either because they are invalid for use outside, or because the internal addressing must be kept private from the external network. RFC 2663 Address translation allows hosts in a private network to communicate transparently with destinations on an external network and vice versa.

To provide transparent routing for the datagrams traversing between address realms, NAT binds addresses in private network with addresses in global network and vice versa. The binding in some cases may extend to transport level identifiers, such as TCP/UDP ports. Address binding is done at the start of a session. There are two types of address assignments: static and dynamic. In the case of static address assignment, there is one-to-one address mapping for hosts between a private network address and an external network address for the lifetime of NAT operation.

Network Address Port Translation (NAPT) is a variation of the traditional NAT. NAPT extends the notion of translation one step further by also translating transport identifiers (e.g., TCP and UDP port numbers, ICMP query identifiers).

- For packets outbound from the private network, NAPT would translate the source IP address, source transport identifier and related fields such as IP, TCP, UDP and ICMP header checksums. Transport identifier can be one of TCP/UDP port or ICMP query ID.
- For inbound packets, the destination IP address, destination transport identifier and the IP and transport header checksums are translated.

Destination network address translation (DNAT) is a technique for transparently changing the destination IP address of an end route packet and performing the inverse function for any replies.

35.1. set ip nat

To enable or disable NAT feature, or define NAT entries number, use the **set ip nat** command in Global Configuration Mode.

set ip nat

```
set ip nat {enable | disable | entries_typical_num <short (0-5000)>}
```

Parameters

Parameter	Type	Description
enable		Enter to enable NAT.
disable		Enter to disable NAT.
entries_typical_num		Enter to define NAT debug level.
<short (0-5000)>		Configures NAT debug to trace level

Mode

Global Configuration Mode

Examples

iS5comm (config)# set ip nat enable

iS5comm (config)# set ip nat disable

iS5comm (config)# set ip nat entries_typical_num 100

iS5comm (config)# set nat entries_typical_num 300

35.2. ip nat

To configure Destination NAT, enable and configures Network Address Port Translation (NAPT) for all networks or a specific network, add a global address pool and enable a global static NAT for a subnet or all networks, and configure Static SNAT, use the **ip nat** command in Interface Configuration Mode. Depending on the option selected, the no form of the command disables Destination NAT, NAPT for specific network or removes specific NAPT configuration, deletes the global address pool, or deletes Static SNAT rule.

ip nat

```
ip nat
 {dest {<ucast_addr - public ip> <ucast_addr - local ip>} | tcp port
<Port-No(1-65535)> | udp port <Port-No(1-65535)>}
 | napt enable | {<ucast_addr - local ip> <ip_mask - local subnet mask> |
tcp port <Port-No(1-65535)> | udp port <Port-No(1-65535)>}
 | pool <ucast_addr - local subnet> <ip_mask - local subnet mask>
<ucast_addr - first public ip> <ucast_addr - last public ip>
 | static <ucast_addr - local ip> <ucast_addr - public ip> [bidirectional]}
```

no ip nat

```
no ip nat {dest | napt | pool | static}
 no ip nat napt enable
```

Parameters

Parameter	Type	Description
dest		Enter this option for Destination NAT.
<ucast_addr - public ip>	A.B.C.D	Enter a global IP address for the public IP to be remapped to a local one. It is the IP address network number obtained from the IANA which can be used by NAT for translating the local IP addresses.
<ucast_addr - local ip>	A.B.C.D	Enter a global IP address for the local IP to which the public IP is to be remapped.
tcp		Enter to configure the protocol as TCP for transport identifier of the packets.
port		Enter to configure the port.
<Port-No(1-65535)>	Integer	Enter a value for the TCP for transport identifier of the packets; enter a local port number in a range from 1 to 65535.
udp		Enter to configure the UDP for transport identifier of the packets.
port		Enter to configure the port.
<Port-No(1-65535)>	Integer	Enter a value for the UDP for transport identifier of the packets; enter a local port number in a range from 1 to 65535.
napt		Enter this option for Network Address Port Translation (NAPT) .
enable		Enter to create a port remaping SNAT rule: Source IP and port will be remapped with the interface IP and port.
<ucast_addr - local ip>	A.B.C.D	Enter a global IP address for the local IP to be remapped to public IP.
<ip_mask - local subnet mask>	A.B.C.D	Enter a local subnet mask.
tcp		Enter to configure the protocol as TCP for transport identifier of the packets.
port		Enter to configure the port.
<Port-No(1-65535)>	Integer	Enter a value for the TCP for transport identifier of the packets; enter a local port number in a range from 1 to 65535.
udp		Enter to configure the UDP for transport identifier of the packets.
port		Enter to configure the port.

Parameter	Type	Description
<Port-No(1-65535)>	Integer	Enter a value for the UDP for transport identifier of the packets; enter a local port number in a range from 1 to 65535.
pool		Enter this option to add a global address pool and enable a global static NAT for a subnet or all networks
<ucast_addr - local subnet>	A.B.C.D	Enter a global IP address for the local IP to be remapped to public IP (0.0.0.0 if N/A).
<ip_mask - local subnet mask>	A.B.C.D	Enter a local subnet IPP address mask(0.0.0.0 if N/A)
<ucast_addr - first public ip>	A.B.C.D	Enter a global IP address for the public IP dynamic SNAT address pool start.
<ip_mask - last public ip>	A.B.C.D	Enter a global IP address for the public IP dynamic SNAT address pool start.
static		Enter this option for Static SNAT. A Static SNAT rule is created: the original source IP will be mapped to a new IP in ingressing / egressing direction, or bidirectionally if this option had been selected.
<ucast_addr - local ip>	A.B.C.D	Enter a global IP address for the local IP to be remapped to a public one.
<ucast_addr - public ip>	A.B.C.D	Enter a global IP address for the public IP to which the local Ip will be remapped.
bidirectional	A.B.C.D	Enter to configure NAT as bidirectional. The bidirectional option will configure Static SNAT and DNAT under a single command.

Mode

Interface Configuration Mode

Examples

iS5comm # configure terminal

iS5comm (config)# interface gi 0/4

iS5comm (config-if)# dest 80.0.0.10 192.168.20.10

iS5comm (config-if)# ip nat napt 192.168.10.0 255.255.255.0

iS5comm (config-if)# no ip nat napt 192.168.10.0 255.255.255.0

iS5comm (config-if)# ip nat napt enable

iS5comm (config-if)# no ip nat napt enable

For a subnet

iS5comm (config-if)# ip nat pool 192.168.10.0 255.255.255.0 80.0.0.10 80.0.0.20

iS5comm (config-if)# ip nat pool 192.168.10.0 255.255.255.0 80.0.0.10 80.0.0.20

For all networks:

iS5comm (config-if)# ip nat pool 0.0.0.0 0.0.0.0 80.0.0.10 80.0.0.20

iS5comm (config-if)# ip nat pool 0.0.0.0 0.0.0.0 80.0.0.10 80.0.0.20

iS5comm(config-if)# ip nat static 192.168.20.10 80.0.0.10 bidirectional

35.3. clear ip connections

To delete all or NAT connections, use the command **clear ip connections** in Global Configuration Mode.

clear ip connections

```
clear ip connections {all | nat}
```

Parameters

Parameter	Type	Description
`all`		Enter to delete all connections. **NOTE:** This command does not clear the global statistics.
`nat`		Enter to delete NAT connections.

Mode

Global Configuration Mode

Examples

iS5comm(config)# clear ip connections all

35.4. clear ip nat rules

To all NAT rules, use the command **clear ip nat rules** in Global Configuration Mode.

clear ip nat rules

```
clear ip nat rules
```

Mode

Global Configuration Mode

Examples

iS5comm(config)# clear ip nat rules

35.5. show ip nat

To display NAT configuration, use the **show ip nat** command in Privileged EXEC Mode. Different options are available.

show nat

```
show ip nat {connections [{from <short (1-65535)>}] [{max <short (0-65535)>}]
[rule <short (0-65535)>]] [{static | dynamic | napt | destination}] [int
<short (1-24)>] [vlan <short (0-65535)>]]
 | info
 | rules {[destination [int <short (1-24)>]] [vlan <short (0-65535)>]]
[dynamic [int <short (1-24)>] [vlan <short (0-65535)>]] [int <short (1-24)>]
[napt [int <short (1-24)>] [vlan <short (0-65535)>]] [static [int <short
(1-24)>] [vlan <short (0-65535)>]]}
```

Parameters

Parameter	Type	Description
connections		Enter to display NAT active connections including connection IPs, ports, and protocol.
from <short (1-65535)>	Integer	Enter to display from specific number of NAT entry to show.
max <short (0-65535)>	Integer	Enter to display the maximum number of entries
rule		Enter to display connections related to the rule number
<short (0-65535)>	Integer	Enter a value for a rule number. The range of the value is from 0 to 65535.
info		Enter to display NAT global information
rules		Enter to display NAT rules of different NAT types on various interfaces.
destination		Enter to show destination NAT.
int		Enter to show a specific interface type.
<short (1-24)>	Integer	Enter a value for specific interface type. The range of the value is from 1 to 24.
vlan		Enter to show a specific VLAN ID number.
<short (0-65535)>	Integer	Enter a value for a VLAN ID. The range of the value is from 0 to 65535.
dynamic		Enter to show dynamic SNAT.
int		Enter to show a specific interface type.
<short (1-24)>	Integer	Enter a value for specific interface type. The range of the value is from 1 to 24.
vlan		Enter to show a specific VLAN ID number.
<short (0-65535)>	Integer	Enter a value for a VLAN ID. The range of the value is from 0 to 65535.

Parameter	Type	Description
napt		Enter to show source NAPT.
int		Enter to show a specific interface type.
<short (1-24)>	Integer	Enter a value for specific interface type. The range of the value is from 1 to 24.
vlan		Enter to show a specific VLAN ID number.
<short (0-65535)>	Integer	Enter a value for a VLAN ID. The range of the value is from 0 to 65535.
static		Enter to show static SNAT
int		Enter to show a specific interface type.
<short (1-24)>	Integer	Enter a value for specific interface type. The range of the value is from 1 to 24.
vlan		Enter to show a specific VLAN ID number.
<short (0-65535)>	Integer	Enter a value for a VLAN ID. The range of the value is from 0 to 65535.

Mode

Privileged EXEC Mode

Examples

Note that if you have less then 5 connections, there will be empty list in the output:

iS5comm# show ip nat connections from 5

```
States: ET - ESTABLISHED, ASU - ASSURED, UN - UNREPLIED, WAIT -
TIME_WAIT
ID    Ip Ver  Protocol   Timeout                  STATE

ORIGIN: Source IP          Port    Destination IP    Port    Packets
REPLY:  Source IP          Port    Destination IP    Port    Packets
```

Note that if the list is not empty, an example output as shown below appears:

iS5comm# show ip nat connections from 5

```
States: ET - ESTABLISHED, ASU - ASSURED, UN - UNREPLIED, WAIT -
TIME_WAIT
```

```
ID    Ip Ver  Protocol   Timeout                  STATE
ORIGIN: Source IP          Port    Destination IP    Port    Packets
REPLY:  Source IP          Port    Destination IP    Port    Packets

1    48596 ipv4    ---        189                      UN
1.1.1.1            0        2.2.2.2                   0
2.2.2.2            0       1.1.1.2           0       0
```

iS5comm# show ip nat info

iS5comm# show ip nat rules static

iS5comm# show ip nat rules static int 22

iS5comm# show ip nat rules vlan 33

iS5comm# show ip nat rules destination vlan 55

35.6. debug nat

To get debug information from Linux kernel for NAT rules configured, use the **debug nat** command in User Exec Mode. To disable, use the no form of the command.

debug nat

no debug nat

Parameters

N/A

Mode

User Exec Mode

Examples

iS5comm # debug nat

iS5comm # no debug nat

Firewall Map

36. firewall

To enable Firewall Configuration Mode, use the **firewall**command in Global Configuration Mode.

firewall

36.1. Parameters

N/A

36.2. Mode

Global Configuration Mode

36.3. Examples

iS5comm # configure terminal
iS5comm (config)# firewall

36.4. enable

To enable firewall service, use the **enable** command in Firewall Configuration Mode.

enable

Parameters

N/A

Mode

Firewall Configuration Mode

Examples

iS5comm # configure terminal

iS5comm (config)# firewall

iS5comm (config-firewall)# enable

36.5. disable

To disable firewall service, use the **disable** command in Firewall Configuration Mode.

disable

Parameters

N/A

Mode

Firewall Configuration Mode

Examples

iS5comm # configure terminal

iS5comm (config)# firewall

iS5comm (config-firewall)# disable

36.6. access-group

To create a firewall access group, use the **access-group** command in Firewall Configuration Mode. The no form of the command deletes firewall access groups.

access-group

```
access-group <string> {in | out} <string> interface {Gigabitethernet <inter-
face-id>| Extreme-ethernet <interface-id>| vlan <vlan-id/vfi-id>}
```

no access-group

```
no access-group <string> {in | out}
```

Parameters

Parameter	Type	Description
<string>		Assign an access group name
in		Set the direction of the packet as inbound
out		Set the direction of the packet as outbound
<string>		Assign an ACL (filter) name
interface		determine the interface
Extreme-Ethernet <interface-id>		Select for Extreme Ethernet interface. Extreme Ethernet interface is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. Specify the interface ID with a format <0>/<1-28>—slot number/port number
Gigabitethernet <interface-id>		Select for Gigabit Ethernet interface. Gigabit Ethernet interface is a version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. Specify the interface ID with a format <0>/<1-28>—slot number/port number
vlan <vlan-id/vfi-id>		specify the range of the specified VLAN ID This is a unique value that represents the specific VLAN created and activated. The range (1-4094) is for VLAN ID and the range (4096 - 65535) is for VFI. Note that if router ports are used then correspondingly the last set of vlans will not be available. For example, if router ports is 24, then max VLAN number will be 4070 only

Mode

Firewall Configuration Mode

Examples

iS5comm (config)# firewall

iS5comm (config-if)# access-group ag1 in ac1,ac2 interface vlan 555

36.7. ip route

To add a static route, use the **ip route** command in Global Configuration Mode. The route defines the IP address or interface through which the destination can be reached. The no form of this command deletes a static route. If the static route is configured without any metric value, the route will be configured with metric value 1.

ip route

```
ip route <ucast_addr> <ip_mask> <next-hop> [<distance_value (1-255)>]
[cybsec] [private]

 <ucast_addr> <ip_mask> {<next-hop> | vlan <vlan-id/vfi-id> [switch
<switch-name>] [<next-hop>] | {Gigabitethernet <interface-id> |
Extreme-ethernet <interface-id> [<next-hop>] | Linuxvlan <interface-name> |
Cpu0 | tunnel <tunnel-id (0-128)> | <IP-interface-type> <IP-inter-
face-number> | ppp <1-10>} [<distance_value (1-255)>] [private] [permanent]
[name <nexthop-name>]
```

no ip route

```
no ip route <ucast_addr> <ip_mask> <next-hop> [<distance_value (1-255)>]
[cybsec] [private]

 <ucast_addr> <ip_mask> {<next-hop> | vlan <vlan-id/vfi-id> [switch
<switch-name>] [<next-hop>] | {Gigabitethernet <interface-id> |
Extreme-ethernet <interface-id> [<next-hop>] | Linuxvlan <interface-name> |
Cpu0 | tunnel <tunnel-id (0-128)> | <IP-interface-type> <IP-inter-
face-number> | ppp <1-10>} [<distance_value (1-255)>] [private] [permanent]
[name <nexthop-name>]
```

Parameters

Parameter	Type	Description
<ucast_addr>	A.B.C.D	Enter to configure unicast destination IP address; 0.0.0.0 is IP address for a default route
<ip_mask>	A.B.C.D	Enter to configure a subnet mask for the destination; 0.0.0.0 is subnet mask for a default route
<next-hop>		Enter to configure the IP address or IP alias of the next hop that can be used to reach that network
cybsec		Enter for configure security application
<distance_value (1-255)>	Integer	Enter to configure the Administrative distance for the specified next hop address or the interface. This value ranges from 1 to 255. The default is 1.
private		Enter to configure a private route
<ucast_addr>	A.B.C.D	Enter to define unicast destination IP address; 0.0.0.0 is IP address for a default route
<ip_mask>	A.B.C.D	Enter to configure a subnet mask for the destination; 0.0.0.0 is subnet mask for a default route
<next-hop>		Enter to configure the IP address or IP alias of the next hop that can be used to reach that network
vlan		Enter for configure a vlan option.
<vlan-id/vfi-id>		specify the range of the specified VLAN ID This is a unique value that represents the specific VLAN created and activated. The range (1-4094) is for VLAN ID and the range (4096 - 65535) is for VFI. Note that if router ports are used then correspondingly the last set of vlans will not be available. For example, if router ports is 24, then max VLAN number will be 4070 only
switch		Enter to configure name of the switch.
<switch-name>		Enter a name for the switch.
<next-hop>		Enter to configure the IP address or IP alias of the next hop that can be used to reach that network
Gigabitethernet <interface-id>		Enter to select Gigabit Ethernet interface. Gigabit Ethernet interface is a version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. Specify the interface ID with a format <0>/<1-28>—slot number/port number

Parameter	Type	Description
Extreme-Ethernet <interface-id>		Enter to select Extreme Ethernet interface. Extreme Ethernet interface is a version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. Specify the interface ID with a format <0>/<1-28>—slot number/port number
Linuxvlan		Enter to specify Linux VLAN interface related configuration.
<interface-name>		Enter a name for the Linux VLAN Interface.
Cpu0		Enter to set the Out of Band Management Interface for the route.
tunnel		Enter to configure the static route for the specified Tunnel Identifier.
<tunnel-id (0-128)>		Enter a value for tunnel Identifier. This value ranges from 0 to 128.
<IP-interface-type>		Enter to configures the static route for the specified L3 Pseudo wire interface in the system
<IP-interface-number>		Enter a value that represents the specific interface. This value ranges from 1 to 65535 for Pseudowire interface.
ppp		Enter to configure the PPP (point-to-point protocol) interface for the route.
<1-10>		Enter a value for PPP. The value ranges from 1 to 10
<distance_value (1-255)>	Integer	Enter to configure the Administrative distance for the specified next hop address or the interface. This value ranges from 1 to 255. The default is 1.
private		Enter to configure a private route
permanent		Enter to configure a switch name /context name; option default is available now.
name		Enter to configure a next hop name.
<nexthop-name>		Enter a next hop name.

Mode

Global Configuration Mode

Prerequisites

Interface must be a router port.

Examples

iS5comm (config)# ip route 30.0.0.2 255.255.255.255 vlan 1

iS5comm (config)# ip route 30.0.0.2 255.255.255.255 gi 0/2 12.2

36.8. clear screen

To clear the screen, use the **clear screen** command in Firewall Configuration Mode.

firewall

Parameters

N/A

Mode

Firewall Configuration Mode

Examples

iS5comm # configure terminal

iS5comm (config)# firewall

iS5comm (config-firewall)# clear screen

36.9. help

To access help for firewall commands, use the **help** command in Firewall Configuration Mode.

help

```
help <string>
```

Parameters

Parameter	Type	Description
<string>		Enter a privileged command for which help should be displayed

Mode

Firewall Configuration Mode

Examples

iS5comm # configure terminal

iS5comm (config)# firewall

iS5comm (config-firewall)# help

```
 access-group <string> {in | out} <filter_name> interface {vlan
<vlan-id/vfi-id>
| <interface-type> <interface-id> }
clear screen
disable
enable
end
exit
help [ command ]
no access-group <acl name> {in | out}
no rule <filter>
rule <filter name> {permit | deny} {<Source IP range>|any} {<Dest IP
range>|any} {<tcp |udp |icmp |igmp |ggp |ip |egp |igp |nvp |rsvp |igrp
|ospf |any |other <1-255>> } [srcport <range>] [destport <range>]
[priority <1-5000>]
```

36.10. debug firewall

To enable the firewall module debug messages, use the **debug firewall** command in User EXEC Mode.

debug firewall

Parameters

N/A

Mode

User EXEC Mode

Examples

iS5comm # **debug firewall**

36.11. show running-config firewall

To display the currently operating firewall configuration in the system, use the **show running-config firewall** command in Privileged EXEC Mode.

show running-config

```
show running-config firewall
```

Parameters

Parameter	Type	Description
`firewall`		Enter this option for see the current operating firewall configuration.

Mode

Privileged EXEC Mode

Examples

iS5comm # show running-config firewall

```
!
firewall
enable rule ac1 permit 80.0.0.0/8 any any
access-group ag1 in ac1 interface vlan 555
!
end
```

iS5comm #

36.12. Example of Firewall Configuration

An example of Firewall Configuration is as shown below.

Example

```
!
iS5comm # configure terminal
iS5comm (config)#firewall
iS5comm (config-firewall)# enable
iS5comm (config-firewall)#rule ac1 permit 80.0.0.0/8 any any
iS5comm (config-firewall)#rule ac2 deny any any any
iS5comm (config-firewall)#access-group ag1 in ac1,ac2 interface vlan 555
exit
exit
iS5comm# show running-config firewall
#Building configuration...
!
iS5comm # configure terminal
iS5comm (config)#firewall
iS5comm (config-firewall)# enable
iS5comm (config-firewall)#rule ac1 permit 80.0.0.0/8 any any
iS5comm (config-firewall)#rule ac2 deny any any any
iS5comm (config-firewall)#access-group ag1 in ac1,ac2 interface vlan 555
!
end
iS5comm#
```

36.13. Static Route Requirements

Static routing has the following benefits:

- No extra processing and added resources as in the case of dynamic routing protocols
- No extra bandwidth requirement caused by the transmission of excessive packets for the routing table update process
- Extra security by manually admitting or rejecting routing to certain network static route can be configured as follows:

For configuring static routing, use the command ip route

36.14. rule

To create firewall access control list (ACL) by adding a filter based on IP address range, protocol and port, use the **rule** command in Firewall Configuration Mode. The no form of the command deletes all rules.

rule

```
rule <string> {permit | deny} {<Source IP range> | any} {<Dest IP range>|
any} {<Source IP range> | any} {tcp | udp | icmp | igmp | ggp | ip | egp |
igp | nvp | rsvp | igrp | ospf | any | other} {srcport <range> | destport
<range> | priority <1-50>}
```

no rule

```
no rule <string>
```

Parameters

Parameter	Type	Description
<string>	string	Configures a rule name with which filter will be referred in access-group
permit		Permits the access
deny		Denies the access
Source IP range	A.B.C.D/E	Configures a source IP address/mask and /or range and applies Firewall ACL rule on the packets having the specified source IP address/mask
any		Applies Firewall ACL rule for allowed packets to have any source address
Dest IP range	A.B.C.D/E	Configures a destination IP with mask and/or range and applies Firewall ACL rule on the packets having the specified destination address
any		Applies Firewall ACL rule for allowed packets to have any destination address
tcp		Specifies TCP as a protocol for which a filter should be applied.
udp		Specifies UDP as a protocol for which a filter should be applied.
icmp		Specifies ICMP as a protocol for which a filter should be applied.
igmp		Specifies IGMP as a protocol for which a filter should be applied.
ggp		Specifies Gateway to Gateway Protocol (GGP) as a protocol for which a filter should be applied.
ip		Specifies IP as a protocol for which a filter should be applied.
egp		Specifies EGP (Exterior Gateway Protocol) as a protocol for which a filter should be applied.
igp		Specifies IGP as a protocol for which a filter should be applied.
nvp		Specifies NVP (Network Voice Protocol)as a protocol for which a filter should be applied.
rsvp		Specifies RSVP (Resource Reservation Protocol) as a protocol for which a filter should be applied.
igrp		Specifies IGRP (Interior Gateway Routing Protocol) as a protocol for which a filter should be applied.
ospf		Specifies OSPF as a protocol for which a filter should be applied.

Parameter	Type	Description
any		Specifies any protocol for which a filter should be applied.
other <1-255>	integer	Specifies other user defined packets related configuration.
srcport <range>	integer	Configures the source port range and applies the Firewall ACL on the packets having source port within this range
destport <range>	integer	Configures the destination port range and applies the Firewall ACL on the packets having destination port within this range
priority <1-5000>	integer	Configures Firewall ACL priority. The available range of numbers is from 1 to 5000.

Mode

Firewall Configuration Mode

Examples

iS5comm (config)# firewall

iS5comm (config-firewall)# rule ac1 permit 80.0.0.0/8 any any

VPN Map

37. VPN

IPSec (Internet Protocol Security) is a suite of protocols that provides security to Internet communications at the IP layer. The most common current use of *IPSec* is to provide a Virtual Private Network (*VPN*), either between two locations (gateway-to-gateway) or between a remote user and an enterprise network (host-to-gateway); it can also provide end-to-end, or host-to-host, security. Ch. 1, Introduction, RFC 6071

IPSec VPN is designated for simple *PPP* networking where encryption is required. Two modes are supported:

- Transport Mode (Route based)

This mode is a route based, which means that to be encrypted, the interesting traffic is routed via a specific path. A Tunnel interface is created at the routing table. The interesting traffic is routed over the tunnel interface.

- Tunnel Mode (Policy-Based)

This mode is referred to as Policy-based. The interesting traffic is defined at the IPsec policy. Since there is no additional IP interface created specifically for the tunnel source, the IPsec policy must define both the interesting traffic source/ destination and the network interfaces source/ destination.

37.1. How IPSec Works

IPSec involves many component technologies and encryption methods. Yet IPSec's operation can be broken down into five main steps. For details, see Cisco, “IPSec Overview Part Four: Internet Key Exchange (*IKE*)”.

1) "Interesting traffic" initiates the *IPSec* process. Traffic is deemed interesting when the IPSec security policy configured in the *IPSec* peers starts the *IKE* process.

   When a distributed operational network uses public transport links for the inter-site connectivity, the traffic must be encrypted to ensure its confidentiality and its integrity. Such virtual VPN connection is executed over an IPSec encrypted link.

2) *IKE* phase 1— IKE authenticates *IPSec* peers and negotiates IKE *Security Association (SA)*s during this phase, setting up a secure channel for negotiating *IPSec SA*s in phase 2.
3) *IKE* phase 2— *IKE* negotiates *IPSec SA* parameters and sets up matching IPSec *SA*s in the peers.
4) Data transfer—data is transferred between *IPSec* peers based on the *IPSec* parameters and keys stored in the *SA* database.
5) IPSec tunnel termination—IPSec *SA*s terminate through deletion or by timing out.

ACK Packets

This section lists off some details of how acknowledgment (*ACK*) packets work with the implementation of *IPSec*.

- Every 60 seconds the switch sends an *ACK* packet
- If an *ACK* is not received, the DPD packet (R_U_THERE) will be retransmitted every 15 seconds for 5 transmissions (75 seconds in total).
- At the end, the endpoint can identify that the other is down in a time between 75 seconds up to 135 seconds.
- When interesting traffic is seen by the switch on either side, the tunnel will try to go up automatically and then will start sending the interesting traffic.

37.2. VPN Global Configuration

The *VPN* Global Configuration commands are:

- **set vp**
- **crypto map**
- **show crypto map**

37.3. set vpn

To configure *VPN*, use the **set vpn** command in Global Configuration Mode.

set vpn

```
set vpn {enable | disable}
```

Parameters

Parameter	Type	Description
`enable`		Enables Global VPN
`disable`		Disables Global VPN

Mode

Global Configuration Mode

Examples

iS5comm (config)# set vpn enable

iS5comm (config)# set vpn disable

37.4. set tunnel

To configure *VPN* Tunnel, use the **set tunnel** command in Crypto Map Configuration Mode.

set tunnel

```
set tunnel {enable | disable}
```

Parameters

Parameter	Type	Description
`enable`		Enables VPN Tunnel
`disable`		Disables VPN Tunnel

Mode

Crypto Map Configuration Mode

Examples

iS5comm (config-crypto-map)# set tunnel enable

iS5comm (config-crypto-map)# set tunnel disable

37.5. crypto map

To establish a *VPN* policy to be negotiated for *SA* creation, use the **crypto map** command in Global Configuration Mode.

crypto map

```
crypto map <policy name (63)>
```

Parameters

Parameter	Type	Description
<policy name (63)>	String	Enter a policy name. This is a string with not more than 63 characters

Mode

Global Configuration Mode

Examples

iS5comm # configure terminal

iS5comm (config)# crypto map cybsec

iS5comm (config-crypto-map)#

37.6. wizard vpn

To use the *VPN* wizard, use the **wizard vpn** command in Global Configuration Mode.

wizard vpn

```
wizard vpn
```

Parameters

Parameter	Type	Description
vpn		Enter to start the VPN Configuration wizard

Mode

Global Configuration Mode

Examples

Step 1: create VPN Configuration.

iS5comm(config)# wizard

iS5comm(config-wizard)# vpn 2 gi 0/3 172.16.100.1 gi 0/1 51 192.168.101.1 172.16.100.101 10.10.101.1 50 192.168.50.1 t1

NOTE: The configuration will be shown on CLI and stored in a file “t1”.

Step 2: review the VPN Configuration.

iS5comm(config-wizard)# show

```
    Name: t2,  Size: 2215       ,  Updated: Wed Nov 24 14:16:23 2021
    Name: t1,  Size: 2215       ,  Updated: Wed Nov 24 17:21:36 2021
```

To show a specific VPN configuration:

iS5comm(config-wizard)# show t1

```
    end
    # Turn on Security
    configure terminal
    set security enable
    end
```

Step 3: Load the VPN Configuration.

iS5comm(config-wizard)# load t1

```
    Executing: end
    Executing:
    Executing:
    Executing: # Turn on Security
    Executing: configure terminal
```

Step 4: Cleanup.

Delete a particular file.

iS5comm(config-wizard)# show

```
    Name: t2,  Size: 2211       ,  Updated: Tue Dec 18 00:04:38 2018
    Name: t1,  Size: 2215       ,  Updated: Mon Dec 17 20:49:12 2018
```

iS5comm(config-wizard)# clear t1

iS5comm(config-wizard)# show

```
    Name: t2,  Size: 2211       ,  Updated: Tue Dec 18 00:04:38 2018
```

Delete all configurations.

iS5comm(config-wizard)# clear all

iS5comm(config-wizard)# show

37.7. show crypto

To display the policy parameters for all interfaces or for a specific interface or show the status and counters of the active *SA*, use the **show crypto** command in Privileged EXEC Mode.

show crypto

```
show crypto {map [<policy name (string(64))>] | sa [<policy name
(string(64))>]}
```

Parameters

Parameter	Type	Description
map		Enter to display a specific crypto map which defines the VPN policy to be negotiated for Security Association (SA) creation. If not policy name is specified, all VPN Policy parameters will be displayed.
<policy name (string (64))>	String	Enter a specific policy name to display information only for this policy. The maximum length of the string is 64.
sa		Enter to display the status and counters of the active SA. Or specify a policy name.
<policy name (string (64))>	String	Enter a specific policy name to display information only for this SA. The maximum length of the string is 64.

Mode

Privileged EXEC Mode

Examples

iS5comm # show crypto map cybsec

```
 VPN Policy Parameters
-------------------------
Policy Name: cybsec
Policy Status: ACTIVE
Tunnel Status: Phase 1 ready - Phase 2 ready
Local end point: 51.0.0.2
Local Id: 51.0.0.2
Remote end point: 161.0.0.2
Remote Id: 161.0.0.2
```

```
Type: tunnel
Local protected network/s: 192.168.151.0/24
Remote protected network/s: 10.10.151.0/24
Authentication by: secret
PSK: presharedkey
IKE version: ikev2
IKE Phase1 encryption: aes256
IKE Phase1 hash: sha512
IKE Phase1 DH Group: modp1536
IKE Phase1 lifetime: 1500 s
IPSec protocol: ESP
IKE Phase2 encryption: aes256
IKE Phase2 lifetime: 3600 s
IKE Phase2 hash: sha
IKE Phase2 DH Group: modp2048
DPD delay timer :  60
```

iS5comm# show crypto sa m1

```
iS5comm# show crypto sa m1
m1: #1, ESTABLISHED, IKEv2
local  '51.0.0.2' @ 51.0.0.2[500]
remote '51.0.0.3' @ 51.0.0.3[500]
AES_CBC-256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MODP_1536
established 3s ago, reauth in 2482s
m1: #1, reqid 1, INSTALLED, TUNNEL, ESP:AES_CBC-256/HMAC_SHA1_96
installed 3s ago, rekeying in 6326s, expires in 7197s
in  c7462e06,      0 bytes,     0 packets
out c600ee1a,      0 bytes,     0 packets
local  192.168.9.0/24 192.168.51.0/24
remote 10.10.9.0/24 10.10.51.0/24
```

37.8. IKE Phase 1

Protocol (*ISAKMP*) defines procedures and packet formats to establish, negotiate, modify and delete Security Associations (*SA*). A *SA* is a relationship between two or more entities that describes how the entities will utilize security services to communicate securely. (RFC 2408)

In endpoint-to-endpoint Transport Mode, both end points of the IP connection implement *IPSec*.

Internet Key Exchange (*IKE*) protocol is a component of *IPSec* used for performing mutual authentication and establishing and maintaining Security Associations (SA)s .(RFC 7296)

Once an *IKE* negotiation is successfully completed, the peers have established two pairs of one-way (inbound and outbound) *SA*s. Since *IKE* always negotiates pairs of *SA*s, the term " *SA*" is generally used to refer to a pair of *SA*s (e.g., an "IKE SA" or an "IPsec SA" is in reality a pair of one-way SAs). The first *SA*, the IKE *SA*, is used to protect IKE traffic. The second SA provides *IPSec* protection to data traffic between the peers and/or other devices for which the peers are authorized to negotiate. It is called the *IPSec SA* in IKEv1 and, in the IKEv2 RFCs, it is referred to variously as a CHILD_SA, a child SA, and an *IPSec* SA.

In addition, since IKEv1 consists of two sequential negotiations, called phases,

- the *IKE* SA is also referred to as a Phase 1 SA, and
- the *IPSec* SA is referred to as a Phase 2 SA.

For details, refer to Sec 2.3.1.

The basic purpose of *IKE* phase 1 is to authenticate the IPSec peers and to set up a secure channel between the peers to enable IKE exchanges.

IKE Phase 1 performs the following functions:

- Authenticates and protects the identities of the *IPSec* peers
- Negotiates a matching *IKE* SA policy between peers to protect the *IKE* exchange
- Performs an authenticated Diffie-Hellman exchange with the end result of having matching shared secret keys
- Sets up a secure tunnel to negotiate *IKE* phase 2 parameters

IKE Phase 1 occurs in two modes: main mode and aggressive mode.

Encryption Algorithms

To authenticates and protect the identities of the *IPSec* peer, the encryption algorithms are as follows:

- DES-CBC—Data Encryption Standard (*DES*) is a symmetric secret-key block algorithm. It has a block size of 64 bits. Use of ESP DES-CBC in the Internet environment is far greater than sending the datagram as cleartext but is not a good encryption algorithm for the protection of even moderate value information in the face of such equipment. Triple *DES* is better choice for such purposes. RFC 2405
- Triple *DES* (3DES)— this *DES* variant processes each block three times, each time with a different key which makes it more secure than DES-CBS.
- Advanced Encryption Standard (*AES*) is a symmetric content encryption algorithm. AES-128 uses 128 bits key-length to encrypt/decrypt a block of message, whereas AES-192 & AES-256 uses 192 & 256 bits key-length to encrypt/decrypt the message.

Diffie and Hellman Key Exchange

Diffie and Hellman (*DH*) describe a method for two parties to agree upon a shared secret number, called ZZ, in such a way that the secret will be unavailable to eavesdroppers. This method requires that both the sender and recipient of a message have key pairs (private and public). By combining one's private key and the other party's public key, both parties can compute the same shared secret number ZZ.

Generation of ZZ

For example, let's identify the communicating parties as party A and party B. Prior to their communication, the parties agree between them on a large prime number p, and a generator (or base) g (where 0 < g < p).

Party A chooses a secret integer xa (her private key) and then calculates ya = g ^ xa mod p (which is her public key). Party B chooses a private key xb, and calculates his public key in the same way as yb = g ^ xb mod p.

Both parties then send each other their public keys. Both parties know their public keys but not their private keys because calculating them is a hard mathematical problem (known as the discrete logarithm problem). However, they can calculate:

ZZ = g ^ (xb * xa) mod p = (yb ^ xa) mod p = (ya ^ xb) mod p, where ZZ is their shared secret as defined by X9.42.

For more details, refer to RFC 2631.

Any eavesdropper who was listening in on the communication knows p, g, and both parties public keysya and yb. But the eavesdropper will be unable to calculate the shared secret from these values.

This secret number can then be converted into cryptographic keying material. The keying material is typically used as a key-encryption key to encrypt (wrap) a content-encryption key which is in turn used to encrypt the message data (the VPN GRE traffic).This key is kept secret and never exchanged over the insecure channel.

The DH groups are identified by the length of the keys in bits. The larger the key (higher group id) the higher is the security but as well the resources required are higher and the user should consider performance degradation.

Exchange Mode

The Exchange Modes in which *IKE* Phase 1 occurs are 2 types: Main and Aggressive.

Main Mode is a more secure option for Phase1 as it involves the identity protection such as three two-way exchanges between the initiator and the receiver:

- Session begins with the initiator sending a proposal to the responder describing what encryption and authentication protocols are supported, the life time of the keys, and if Phase 2 perfect forward secrecy should be implemented. The proposal may contain several offerings. The responder chooses from the offerings and replies to the initiator.
- The next exchange passes Diffie-Hellman public keys and other data. All further negotiation is encrypted within the *IKE SA*.
- The third exchange authenticates the *ISAKMP* session. Once the *IKE SA* is established, *IPSec* negotiation (Quick Mode) begins.

In Aggressive mode, the negotiation is quicker as the session is completed in only 3 messages. The disadvantage is in that the identity of the peers is not protected.

The first two messages negotiate policy, exchange Diffie-Hellman public values and ancillary data necessary for the exchange, and identities. In addition, the second message authenticates the responder. The third message authenticates the initiator and provides a proof of participation in the exchange.

- The initiator send a request with all required *SA* information.
- The responder replies with authentication and its ID.
- The initiator authenticates the session in the follow-up message

The weakness of using the aggressive mode is that both sides have exchanged information before there is a secure channel.

37.9. IKE Phase 2

The purpose of *IKE* Phase 2 is to negotiate IPSec SAs. *IKE* Phase 2 performs the following functions. For details, see Cisco, “IPSec Overview Part Four: Internet Key Exchange (IKE)”.

- Negotiates *IPSec SA* parameters protected by an existing *IKE SA*
- Establishes *IPSec* security associations
- Periodically renegotiates *IPSec SA*s to ensure security
- Optionally performs an additional Diffie-Hellman exchange

A negotiated shared *IPSec* Phase 2 policy includes:

- *IPSec* Security protocols

  When IKE is not used to establish SAs, a single transform set must be used. Before a transform set can be included in a crypto map entry, it must be defined. A transform set specifies one or two IPSec security protocols (either Encapsulation Security Payload (ESP) Protocol or Authentication Header (AH)

  To select a transform set, consider the following:

  – For data confidentiality, include an *ESP* protocol.
  – For data authentication for the outer IP header as well as the data, include an *AH*.
  – For data authentication (either using *ESP* or *AH*), choose from the *MD5* or *SHA* (HMAC keyed hash variants) authentication algorithms. The *SHA* algorithm is generally considered stronger than *MD5*, but is slower.

- Encryption— *AES* Counter mode (AES-CTR) are used are also used. *AES*-CTR use *ESP* confidentiality mechanism and require the encryptor to generate a unique per-packet value and to communicate this value to the decryptor. *AES*-CTR must be used in conjunction with an authentication function, such as HMAC-SHA.
- Authentication
- *IPSec* Mode—the options are tunnel and transport modes.
- Perfect Forward Secrecy (PFS)— *PFS* means that a piece of an encryption system automatically and frequently changes the keys it uses to encrypt and decrypt information, such that if the latest key is compromised, it exposes only a small portion of the user’s sensitive data.

  If PFS is specified in the IPSec policy, a new Diffie-Hellman exchange is performed with each quick mode, providing keying material that has greater entropy (key material life) and thereby greater resistance to cryptographic attacks. Each Diffie-Hellman exchange requires large exponentiations, thereby increasing CPU use and exacting a performance cost.

For *IKE* Phase 2, see **crypto map ipsec** command.

For *IPSec* Mode, see **crypto ipsec mode** command.

37.10. IPSec Local and Peer End Points Configuration

The following commands elaborate on configuration of both end points: local and remote (peer).

isakmp local identity

To determine the local endpoint configuration by specifying the identity used by the router when participating in the Internet Key Exchange (*IKE*) protocol, use the **isakmp local identity** command in Crypto Map Mode. It configures local identity type and its value to be used in *IKE* Phase 1. The type can be IP address, email, fqdn, dn, or key id.

isakmp local identity

```
isakmp local identity {dn <string>| email <string>| fqdn <string>|
ipv4<string> | ipv6<string> | keyId <string>}
```

Parameters

Parameter	Type	Description
`local identity`		Enter for endpoint configuration
`dn <string>`		Specify domain name for local identity value. Support for X.509 certificates is also available.
`email<string>`		Specify email address for local identity value.
`fqdn<string>`		Specify fully Qualified Domain Name for local identity value.
`ipv4<string>`		Specify IPv4 address related information for local identity value
`ipv6<string>`		Specify IPv6 address related information for local identity value.
`<keyId <string>`		Specify key Identifier related information for local identity value.

Mode

Crypto Map Configuration Mode

Examples

iS5comm # configure terminal

iS5comm (config)# crypto map cybsec

iS5comm (config)# isakmp local identity dn 1

iS5comm (config)# isakmp local identity dn “C=CA, ST=ON, L=Miss, O=iS5, OU=SW, CN=r1”

isakmp peer identity

To determine the remote endpoint configuration or enables an *IPSec* peer for *IKE* use the **isakmp peer identity** command in Crypto Map Mode. It configures peer identity type and its value to be used in *IKE* Phase 1. The type can be IP address, email, fqdn, dn or key id.

isakmp peer identity

```
isakmp peer identity {dn <string>| email <string>| fqdn <string>|
ipv4<string> | ipv6<string> | keyId <string>}
```

Parameters

Parameter	Type	Description
`peer identity`		Enter for remote peer identity / endpoint configuration.
`dn <string>`		Specify domain name for remote peer. Support for X.509 certificates is also available.
`email<string>`		Specify email address for remote peer
`fqdn<string>`		Specify fully Qualified Domain Name for remote peer.
`ipv4<string>`		Specify IPv4 address related information for remote peer identity.
`ipv6<string>`		Specify IPv6 address related information for remote peer identity value.
`keyId <string>`		Specify key Identifier related information for remote peer identity value.

Mode

Crypto Map Configuration Mode

Examples

iS5comm # configure terminal

iS5comm (config)# crypto map cybsec

iS5comm (config)# isakmp peer identity dn 1

iS5comm (config)# isakmp peer identity dn "C=CA, ST=ON, L=Miss, O=iS5, OU=SW, CN=r2"

37.11. IPSec Policy Configuration

The IPSec Policy Configuration commands are:

- **set ike version**
- **isakmp policy**
- **crypto key**
- **crypto map ipsec**
- **crypto ipsec mode**
- **access-list**
- **debug crypto ipsec level**

set ike version

To determine *IKE*'s version, use the **set ike version** command in Crypto Map Configuration Mode.

set ike version

```
set ike version {v1 | v2}
```

Parameters

Parameter	Type	Description
v1		Select IKEv1 if you do not need NAT traversal (not supported by v1)
v2		Select IKE v2 for remote access thanks to its EAP authentication, more secure connection due to its use of encryption keys for both sides, improved resistance to DoS attacks, and less bandwidth use.

Mode

Crypto Map Configuration Mode

Examples

iS5comm # configure terminal

iS5comm (config)# crypto map

iS5comm (config-crypto map)# set ike version v2

crypto policy encryption

To configures Phase 1 encryption for the *IKE* policy, hash, *DH* group, mode and lifetime configuration, use the **isakmp policy** command in Crypto Map Configuration Mode.

isakmp policy

```
isakmp policy encryption {des | triple-des | aes | aes-192 | aes-256} hash
{md5 | sha 1 | sha256 | sha384 | sha 512} dh {group 1| group 2| group 14 |
group 16 | group 17 | group 18} exch {main | aggressive} lifetime <lifetime>
{secs | min | hrs}
```

Parameters

Parameter	Type	Description
encryption		selects encryption algorithm
des		sets the Encapsulating Security Payload (ESP) algorithm type as DES-CBS
triple-des		sets ESP algorithm type as 3DES
aes		sets the AES to 28 bits key-length for encrypting / decrypting a block of message
aes-192		sets the AES to 192 bits key-length for encrypting / decrypting a block of message
aes-256		sets the AES to 256 bits key-length for encrypting / decrypting a block of message
blowfish		sets the symmetric-key block cipher algorithm
hash		selects authentication hash algorithm
md5		selects md5 algorithm. The message-digest (md5) algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption
sha1		sets the hash to Secure Hash Algorithm SHA-1 (160 bit)
sha256		sets the hash to Secure Hash Algorithm SHA-2 (256 bit)
sha384		sets the hash to Secure Hash Algorithm SHA-3 (384 bit)
sha512		sets the hash to Secure Hash Algorithm SHA-1 (512 bit)
dh		selects the Diffie-Helman group for the IKE policy
group1		specifies use of 768-bit Diffie-Hellman Group 1 cryptography
group14		specifies use of 2048-bit Diffie-Hellman Group 14 cryptography. This is the minimum acceptable encryption for protection of sensitive information
group15		specifies use of 3072-bit Diffie-Hellman Group 14 cryptography
group16		specifies use of 4096-bit Diffie-Hellman Group 14 cryptography
group17		specifies use of 6144-bit Diffie-Hellman Group 14 cryptography
group18		specifies use of 8192-bit Diffie-Hellman Group 14 cryptography
group2		specifies use of 1024-bit Diffie-Hellman Group 2 cryptography
group5		specifies use of 1536-bit Diffie-Hellman Group 5 cryptography

Parameter	Type	Description
exch		selects the main exchange mode type
main		specifies use of 768-bit Diffie-Hellman Group 1 cryptography
aggressive		selects the aggressive exchange mode type
lifetime <lifetime>		selects the exchange mode type
hrs		specifies lifetime in hours
mins		specifies lifetime in mins
secs		specifies lifetime in secs

Mode

Crypto Map Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# crypto map cybsec

iS5comm (config-crypto map)# isakmp policy encryption blowfish hash sha1 dh group1 exch main life-time min 20

crypto key

To specify the type of algorithm to be used for decryption / encryption or define *VPN* mode-related configuration, use the **crypto key** command in Crypto Map Configuration Mode.

crypto key

```
crypto key decrypt {dsa | rsa} | encrypt {dsa | rsa} | mode {cert |
ipsec-manual | preshared-key | ra-cert | ravpn-preshared-key | xauth |
xauth-cert} [psk <preshared-key> [encrypted]] [Certificate-File <File-name>]
[PrivateKey-File <File-name>]
```

Parameters

Parameter	Type	Description
decrypt		Specify the type of algorithm to be used for decryption TLS profile support related configuration
dsa		Specify Digital Signature Algorithm (DSA) related configuration
rsa		Specify Ron Rivest, Adi Shamir and Len Adleman Algorithm (RSA) related configuration
encrypt		Specify the type of algorithm to be used for decryption TLS profile support related configuration
dsa		Specify Digital Signature Algorithm (DSA) related configuration
rsa		Specify Ron Rivest, Adi Shamir and Len Adleman Algorithm (RSA) related configuration
mode		Specify VPN mode related configuration
cert		Specify certificate information about the security router. The options are: • <CR>—specify the type of VPN used. • psk <preshared-key>—specify pre shared key and its value
ipsec-manual		Specify IPSec manual security association. The options are: • <CR>—specify the type of VPN used. • psk <preshared-key>—specify preshared key and its value
preshared-key		Specify pre-shared key related information. The options are: • <CR>—specify the type of VPN used. • psk <preshared-key>—specify pre shared key and its value
ravpn-preshared-key		Specify remote access VPN related information. The options are: • <CR>—specify the type of VPN used. • psk <preshared-key>—specify preshared key and its value
xauth		Specify extended authentication related information. The options are: • <CR>—specify the type of VPN used. • psk <preshared-key>—specify preshared key and its value
xauth-cert		Specify extended authentication certificate related information. The options are: • <CR>—specify the type of VPN used. • psk <preshared-key>—specify preshared key and its value

Parameter	Type	Description
psk		Enter for preshared key.
preshared-key		Enter a value for the preshared key.
encrypted		Enter for encrypted option.
Certificate-File		Enter for File Certificate file.
File-name		Enter a value for File Certificate file.
PrivateKey-File		Enter for Private key file.
File-name		Enter a value for Private key file.

Mode

Crypto Map Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# crypto map cybsec

iS5comm (config-crypto map)# crypto key decrypt dsa

iS5comm (config-crypto map)# crypto key mode cert Certificate-File r1Cert.pem PrivateKey-File r1Key.pem

crypto map ipsec

To define *IKE* Phase 2 Proposal providing encryption and determining authentication algorithm, mode of transaction, and lifetime as parameters, use the **crypto map ipsec** command in Crypto Map Configuration Mode.

crypto map ipsec

```
crypto map ipsec {authentication ( ah | esp | encryption) | lifetime ( hrs | mins | secs) | pfs (group1 | group14 | group2 | group5) | lifetime ( hrs | mins | secs)}
```

Parameters

Parameter	Type	Description
authentication		Select an IPSec security protocol
ah		Specify authentication header (AH) algorithm related information
esp		Specify encapsulating security payload (ESP) algorithm related information
encryption		Specify encryption related configuration
lifetime		Specify specifies lifetime related configuration
hrs		Specify lifetime in hrs
mins		Specify lifetime in mins
secs		Specify lifetime in secs
pfs		Enables Perfect Forward Secrecy (PFS) related configuration
group1		Specifies IKE group1 related information.
group14		Specifies IKE group14 related information.
group2		Specifies IKE group2 related information.
group5		Specifies IKE group5 related information.
lifetime		Specify specifies lifetime related configuration
hrs		Specify lifetime in hrs
mins		Specify lifetime in mins
secs		Specify lifetime in secs

Mode

Crypto Map Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# crypto map cybsec

iS5comm (config-crypto map)# crypto map ipsec lifetime secs 2

crypto ipsec mode

To determine the type of encryption mode, use the **crypto ipsec mode** command in Crypto Map Configuration Mode. *IPSec* supports two encryption modes: transport and tunnel.

crypto ipsec mode

```
crypto ipsec mode {tunnel | transport}
```

Parameters

Parameter	Type	Description
`tunnel`		Enables the tunnel mode. Tunnel mode encrypts both the header and the payload, which makes it more secure
`transport`		Enables transport mode. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched

Mode

Crypto Map Configuration Mode

Examples

iS5comm# configure terminal

iS5comm (config)# crypto map cybsec

iS5comm (config-crypto map)# crypto ipsec mode tunnel

access-list

To create an access list which determines source and destination IP networks for which security services need to be applied or to specify protocol, use the **access-list** command in Crypto Map Configuration Mode.

access-list

```
access-list source <subnet [proto / port],...> destination < ip/subnet >
```

Parameters

Parameter	Type	Description
source		Enter for source related configuration.
<subnet [proto / port] ,...>		Enter to specify port range of 0-65535, a single port, or %any
destination		Enter for destination related configuration.

Mode

Crypto Map Configuration Mode

Examples

iS5comm# configure terminal

iS5comm(config)# set security enable

iS5comm (config)# crypto map cybsec

iS5comm (config-crypto map)# access-list source 192.168.9.0/24[tcp/%any],192.168.51.0/24 destination 10.10.9.0/24,192.168.61.0/24

iS5comm (config-crypto map)# access-list source 192.168.101.0/24 destination 10.10.101.0/24

iS5comm (config-crypto map)# access-list source gre destination gre

NOTE: If only protocol is to be specified, then no brackets are required.

debug crypto ipsec level

To debug the *VPN*, use the **debug crypto ipsec level** command in User Exec. The no form of the command disables the debugging changing default logging level to 1. and changes default logging level to 1.

debug crypto ipsec level

```
debug crypto ipsec level <sev_level> { 1 | 2 | 3 | 4 | 5} {all | app | asn | cfg | chd | dmn | enc | esp | ike | imc | imv | job | knl | lib | mgr | net | pts | tls | tnc}
```

no debug crypto ipsec

```
no debug crypto ipsec { 1 | 2 | 3 | 4 | 5} {all | app | asn | cfg | chd | dmn | enc | esp | ike | imc | imv | job | knl | lib | mgr | net | pts | tls | tnc}
```

Parameters

Parameter	Type	Description
<sev_level>		Select a debugging level. The levels are as follows:
1	Integer	Very basic auditing logs, (e.g. SA up/SA down)
2	Integer	Generic control flow with errors, a good default to see what's going on
3	Integer	More detailed debugging control flow
4	Integer	Including RAW data dumps in hex
5	Integer	Also include sensitive material in dumps, e.g. keys
all	Integer	Select for all debug messages
app	Integer	Select for applications other than daemons
asn	Integer	Select for low-level encoding/decoding (ASN.1, X.509, etc.)
cfg	Integer	Select for configuration management and plugins
chd	Integer	Select for CHILD_SA/IPsec SA
dmn	Integer	Select for Main daemon setup/cleanup/signal handling
enc	Integer	Select for Packet encoding/decoding encryption/decryption operations
esp	Integer	Select for libipsec library messages
ike	Integer	Select for IKE_SA/ISAKMP SA
imc	Integer	Select for Integrity Measurement Collector
imv	Integer	Select for Integrity Measurement Verifier
job	Integer	Select for Jobs queuing/processing and thread pool management
knl	Integer	Select for IPsec/Networking kernel interface
lib	Integer	Select for libstrongwan library messages
mgr	Integer	Select for IKE_SA manager, handling synchronization for IKE_SA access
net	Integer	Select for IKE network communication
pts	Integer	Select for Platform Trust Service
tls	Integer	Select for libtls library messages
tnc	Integer	Select for Trusted Network Connect

Mode

User Exec Mode

Examples

iS5comm# debug crypto ipsec level 1 knl

iS5comm# no debug crypto ipsec all

set ipv6 peer

To peer related configuration, use the **set ipv6 peer** command in Crypto Map Configuration Mode.

set ipv6 peer

```
set ipv6 peer <ip6_addr>
```

Parameters

Parameter	Type	Description
<ip6_addr>	AAAA::BBBB	Enter IPv6 address related information

Mode

Crypto Map Configuration Mode

Examples

iS5comm (config-crypto-map)#

set local

To local end point configuration, use the **set local** command in Crypto Map Configuration Mode.

set local

```
set local <ucast_addr>
```

Parameters

Parameter	Type	Description
<ucast_addr>	A.B.C.D	Enter the IP address of the local interface

Mode

Crypto Map Configuration Mode

Examples

iS5comm (config-crypto-map)#

set peer

To determine local end point configuration, use the **set peer** command in Crypto Map Configuration Mode.

set peer

```
set peer <ucast_addr>
```

Parameters

Parameter	Type	Description
<ucast_addr>	A.B.C.D	Enter the IP address of the local interface

Mode

Crypto Map Configuration Mode

Examples

iS5comm (config-crypto-map)#

copy crypto-pki

To back up certificates and private keys over SFTP, TFTP and USB, use the **copy crypto-pki** command in Privileged EXEC Mode. Private keys and entire configuration backups are encrypted using a user supplied password.

Device to media (SFTP/TFTP/USB)

copy crypto-pki

```
copy crypto-pki {file <name> | all} {tftp://server/filename |
sftp://<user-nam>e>:<pass-word>@server/filename | usb} [filename <filename>]
[password <string (32)>]
```

media (SFTP/TFTP/USB) to Device

```
copy crypto-pki {<tftp_url> | <sftp_url> | {usb <string(32)>}} {private |
public | CA | all } [ { filename <string(32)>}] [{password <string(32)>}]
```

Parameters

Parameter	Type	Description
file		Enter a Private Key or Certificate file.
name	string (32)	Enter a name to specify a Private Key or Certificate to be backed up.
all		Enter to back up all certificates.
tftp://server/filename	tftp_url	Enter a TFTP URL.
sftp://user:pwd@<ip>/filename	sftp_url	Enter a SFTP URL.
usb		Enter to copy to USB media.
filename		Enter a filename identifier.
<filename>	string (32)	Enter to specify a name of destination file. Used only for USB.
password		Enter for a password identifier.

Mode

Privileged EXEC Mode

Examples

USB

iS5comm # copy crypto-pki file r1Key.pem usb filename r1key password pass

iS5comm # copy crypto-pki usb r1Key private filename r1Key.pem password pas

iS5comm # copy crypto-pki usb r1Key private password pass

iS5comm # copy crypto-pki file r1Cert.pem usb filename r1C

iS5comm # copy crypto-pki usb r1Cert.pem public filename r1Cert.pem

iS5comm # copy crypto-pki usb r1Cert.pem public

iS5comm # copy crypto-pki all usb filename certificates.conf password pass

iS5comm # copy crypto-pki usb certificates.conf all password pass

iS5comm # copy crypto-pki usb certificates.conf all password pass

iS5comm # copy crypto-pki all usb filename cybsec.conf password pass

SFTP

iS5comm # copy crypto-pki file r1Key.pem sftp://pi:raspberry@192.168.101.3/r1key password pass

iS5comm # copy crypto-pki sftp://pi:raspberry@192.168.101.3/r1key private filename r1Key.pem password pass

iS5comm # copy crypto-pki sftp://pi:raspberry@192.168.101.3/r1key private password pass

iS5comm # copy crypto-pki file r1Cert.pem sftp://pi:raspberry@192.168.101.3/r1Cert.pem

iS5comm # copy crypto-pki sftp://pi:raspberry@192.168.101.3/r1Cert.pem public

iS5comm # copy crypto-pki sftp://pi:raspberry@192.168.101.3/r1Cert.pem public filename r1CertCopy.pem

iS5comm # copy crypto-pki all sftp://pi:raspberry@192.168.101.3/cybsec.conf password pass

iS5comm # copy crypto-pki sftp://pi:raspberry@192.168.101.3/cybsec.conf all password pass

TFTP

iS5comm # copy crypto-pki file r2Key.pem tftp://10.10.101.3/r2key password pass

iS5comm # copy crypto-pki tftp://10.10.101.3/r2key private filename r2Key.pem password pass

iS5comm # copy crypto-pki tftp://10.10.101.3/r2key private password pass

iS5comm # copy crypto-pki file r2Cert.pem tftp://10.10.101.3/r2Cert.pem

iS5comm # copy crypto-pki tftp://10.10.101.3/r2Cert.pem public

iS5comm # copy crypto-pki tftp://10.10.101.3/r2Cert.pem public filename r2CertCopy.pem

iS5comm # copy crypto-pki all tftp://10.10.101.3/cybsec.conf password pass

iS5comm # copy crypto-pki tftp://10.10.101.3/cybsec.conf all password pass

show crypto ipsec secrets

To display the local ID, the remote ID and the key type, use the command **show crypto ipsec secrets** in Privileged Exec Mode. Either local ID or peer ID should be configured for a policy to configure key mode (PSK or Certificate); the key mode should be configured after configuring local ID and peer ID. If the peer id or local id is modified, the "key mode" may require to be configured again.

show crypto

```
show crypto ipsec secrets
```

Parameters

Parameter	Type	Description
ipsec		Enter to have the *MRP* interconnection statistics/counter information displayed.
secrets		Enter for displaying the interconnection ID of the *MRP* interconnection instance for which information will be shown.

Mode

Privileged Exec Mode

Examples

```
# show crypto ipsec secrets
Local Id:  172.16.100.1
Remote Id: 172.16.100.101
Type:      Pre-shared key
```

37.12. GRE

Generic routing encapsulation (*GRE*) is an *IP* encapsulation protocol which is used to transport *IP* packets over a network. In *GRE*, an *IP* datagram is tunnelled (encapsulated) within another *IP* datagram.

One great advantage of *GRE* is that it allows routing of *IP* packets between private IPv4 networks which are separated over public IPv4 Internet. *GRE* also supports encapsulating IPv4 broadcast and multicast traffic.

When a system has a packet that needs to be encapsulated and delivered to some destination, this is called a payload packet. The payload is first encapsulated in a *GRE* packet. The resulting *GRE* packet can then be encapsulated in some other protocol and then forwarded.

tunnel mode

To define the tunnel mode an interface, use the **tunnel mode** command in Interface Configuration Mode.

tunnel mode

```
tunnel mode {gre | sixToFour |isatap |compat |ipv6ip |openflow} [config-id
<ConfId(1-2147483647)>] source <TnlSrcIP/IfName> [dest <TnlDestIP>]
```

Parameters

Parameter	Type	Description
gre		Enter to select *GRE*.
sixToFour		Enter to select Six to four encapsulation mode.
isatap		Enter to select ISATAP encapsulation mode.
compat		Enter to select IPv6 auto compatible encapsulation mode mode.
ipv6ip		Enter to select IPv6 over IPv6 configured encapsulation mode.
openflow		Enter to select Openflow tunnel for hybrid communication.
config-id		Enter to define config-id.
ConfId(1-2147483647)		Enter to a value for conig-id
source		Enter to select a source.
<TnlSrcIP/IfName		Enter an identification of the source (e.g. 172.16.100.1).
dest		Enter to select a destination.
<TnlDestIP>		Enter an identification of the destination (e.g. 172.16.100.101)

Mode

Interface Configuration Mode

Examples

iS5comm(config)# interface tunnel 1

iS5comm (config-if)# tunnel mode gre source 172.16.100.1 dest 172.16.100.101

iS5comm (config-if)# ip address 10.10.1.1 255.255.255.0 cybsec

iS5comm (config-if)# no shutdown

37.13. CLI for Displaying Logs

The CLI commands for displaying logs are:

- **show file /var/log/syslog**
- **copy flash log file_name**

show file

To show the contents of different files, use the **show file** command in Privileged EXEC Mode.

show file

```
show file {<CR> | last (bytes (2-8192)}
```

Parameters

Parameter	Type	Description
file		enter the file name to be shown
<CR>		Show the contents of a file
last		enter for last number of bytes to display
(2-8192)	Integer	Enter bytes to display

Mode

Privileged EXEC Mode

Examples

iS5comm # show file /var/log/syslog

```
Feb  3 15:26:03 received netlink error: Address family not supported by
protocol (97)
Feb  3 15:26:03 unable to create IPv6 routing table rule
```

copy flash log file_name

To copy the flash log, use the **copy flash log file_name** command in User Exec Mode.

copy flash log file_name

```
copy flash log file_name {<sftp_url> | <tftp_url>| usb | SD-Card}
```

Parameters

Parameter	Type	Description
<tftp_url>		Copies to a TFTP server; the format is tftp://server/filename
<sftp_url>		Copies to a SFTP server; the format is sftp://<user-name>:<pass-word>@server/filename
usb		Copies to usb; the format is <file_name (string(128))>
SD-Card		Copies to SD-co; the format is <file_name (string(128))>

Mode

User Exec Mode

Examples

iS5comm # copy flash log SD-Card myfile23

Index