

iS5 Communications



RAPTOR iMX950-Web User Interface,
iMX950

Document Version: 1.12.05-1-EN
April 12, 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: i55 Communications Inc. ("**i55Com**") licenses the i55Com 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 i55Com or, if applicable, a reseller for i55Com, 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 i55Com, including i55Com Materials, trade secrets, technology and records to which access is obtained hereunder by the Customer, and any materials provided by i55Com 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 i55Com; (c) is already known to the Customer at the time of its disclosure to the Customer by i55Com 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 i55Com; or (f) is disclosed pursuant to court order or other legal compulsion.*

- "**Customer**" means the licensee of the i55Com Software pursuant to the Contract.
- "**i55Com Documentation**" means Documentation supplied by or on behalf of i55Com under the Contract relating to the development, use, installation, implementation, integration, configuration, operation, modification, maintenance or support of i55Com Software, or i55Com Firmware.
- "**i55Com Firmware**" means i55Com Software in object code format that is embedded in i55Com Hardware.
- "**i55Com Hardware**" means Hardware supplied by or on behalf of i55Com under the Contract.
- "**i55Com Materials**" means, collectively, the i55Com Software and the i55Com Documentation.

- **“i5Com Software”** means Software supplied by or on behalf of i5Com under the Contract. For greater certainty, i5Com Software shall include all operating Software for i5Com Hardware, and i5Com 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 i5Com and sublicensed to the Customer.
- **“Update”** means a supplemented or revised version of i5Com Software which rectifies bugs or makes minor changes or additions to the functionality of i5Com Software and is designated by i5Com 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 i5Com hereby grants to the Customer, subject to any Third Party License Terms, a non-exclusive, non-transferable, non-sublicensable right and licence to use i5Com 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 i5Com Documentation, and, in the case of i5Com Firmware, solely on i5Com Hardware on which i5Com Firmware was installed, provided that Customer may only install i5Com 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 i55Com Materials for any purpose, except for the sole purpose of making an archival or back-up copy; (b) modify, translate or adapt the i55Com Materials, or create derivative works based upon all or part of such i55Com Materials; (c) assign, transfer, loan, lease, distribute, export, transmit, or sublicense i55Com Materials to any other party; (d) use i55Com Materials for service bureau, rent, timeshare or similar purposes; (e) decompile, disassemble, decrypt, extract, or otherwise reverse engineer, as applicable, i55Com Software or i55Com Hardware; (f) use i55Com Materials in a manner that uses or discloses the Confidential Information of i55Com or a third party without the authorization of such person; (g) permit third parties to use i55Com Materials in any way that would constitute breach of this EULA; or (h) otherwise use i55Com Materials except as expressly authorized herein.

– **2.3 Updates and Upgrades**

The license granted hereunder shall apply to the latest version of i55Com 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 i55Com 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 i55Com 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, i55Com and the Customer agree that i55Com is and shall be the owner of all Intellectual Property Rights in i55Com Materials and all related modifications, enhancements, improvements and upgrades thereto, and that no proprietary interests or title in or to the intellectual property in i55Com Materials is transferred to the Customer by this EULA. i55Com reserves all rights not expressly granted to the Customer under Section 2.1.

– **3.2 Firmware**

i55Com and the Customer agree that any and all i55Com Firmware in or forming a part of i55Com 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 i55Com Firmware.

– **3.3 Third Party Software**

Certain of i55Com Software provided by i55Com 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 i55Com Materials contain Confidential Information of i55Com and that disclosure of such Confidential Information to any third party could cause great loss to i55Com. The Customer agrees to limit access to i55Com Materials to those employees or officers of the Customer who require access to use i55Com 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 i55Com.

– **4.2 Irreparable Harm**

Without limiting any other rights or remedies available to i55Com 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 i55Com 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 i55Com 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 ADVISED 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 i55Com 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 i55Com Materials) the entire agreement between the Customer and i55Com pertaining to the Customer’s right to access and use i55Com 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

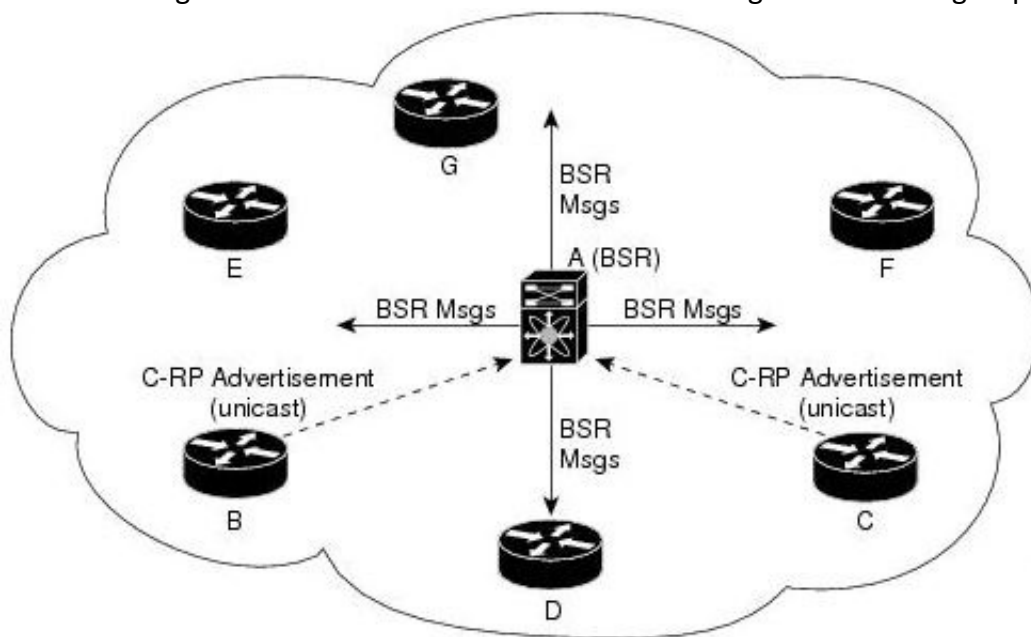
Berkeley Software Distribution (BSD)

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 average 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

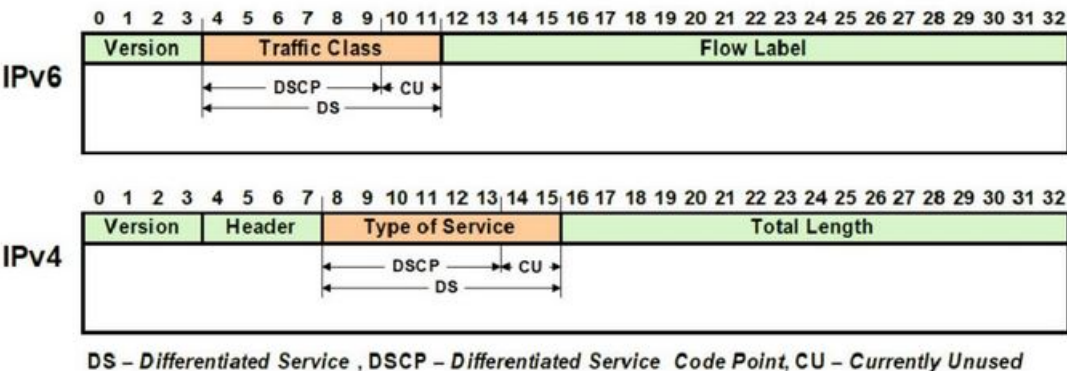
Dot1x Authentication is enabled when dot1x system-auth-control is enabled, and aaa authentication dot1x default is local. If you enable authentication on a port by using the default setting of dot1x port-control, which is force-authorized, it disables 802.1X authentication and causes the port to transition 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).

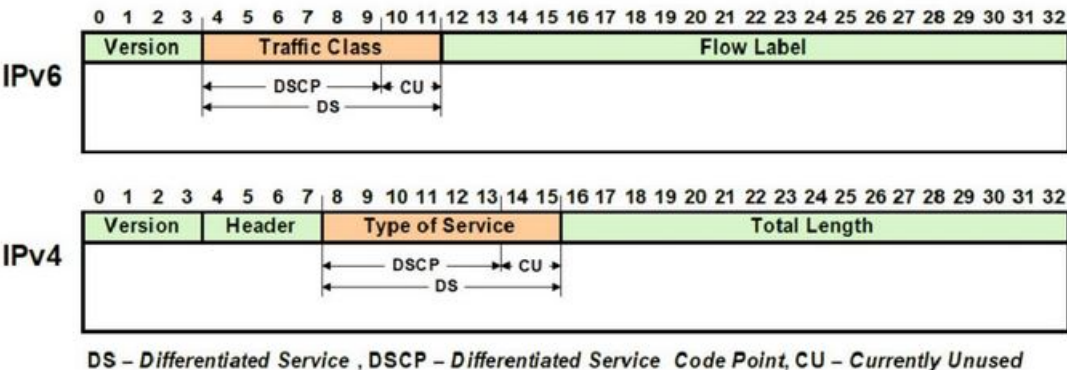
DS

Differentiated Services (DS).



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.



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 frames 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 neighborhood 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 4.29×10^9 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 hexadecimal digits. An example of IPv6 address is as follows

3001:0da8:75a3:0000:0000:8a2e:0370:7334

there are different types 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 represent 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

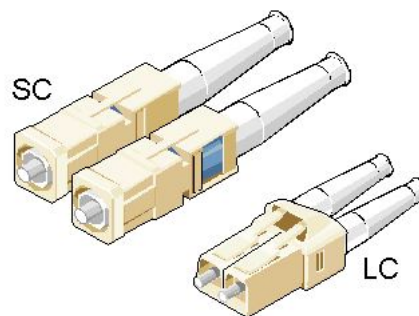
Link Aggregation Group

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, a device 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 μm .

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

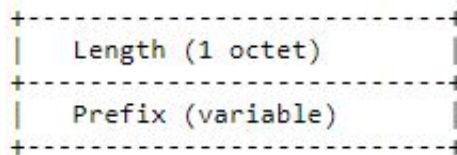
Network Basic Input / Output System (NETBIOS)

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 detecting network 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 by all 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 by all 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 ("cached 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 BPDUs.

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

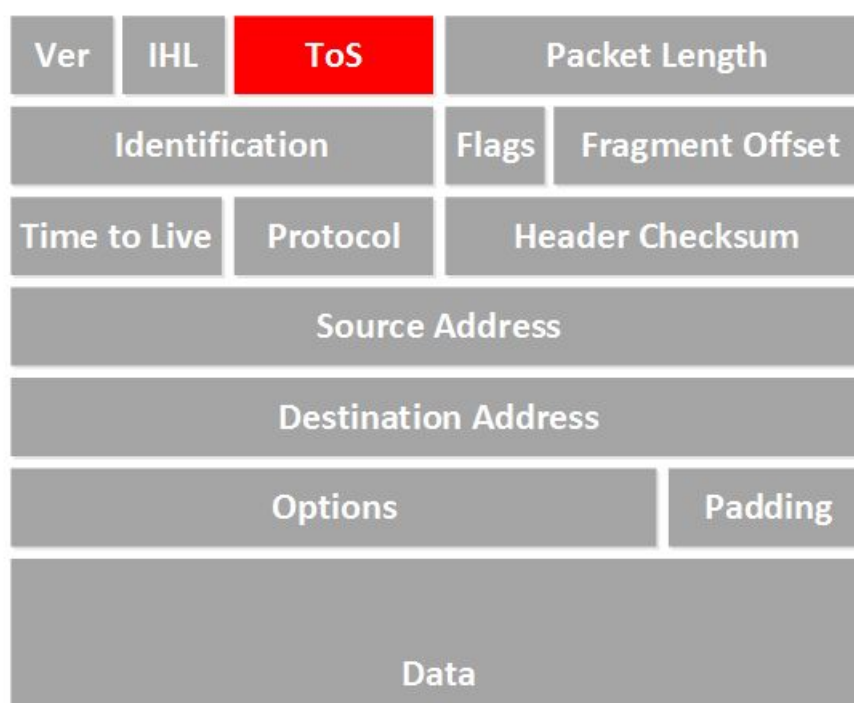
type, length, and value (TLV) traces

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 to the WebUI	1
	Introduction	1
	Purpose	1
	Scope	1
	Web Interface Conventions	1
	Browser Settings	3
	Document Conventions	5
	Web Interface: Logging into the RAPTOR	6
	Home Page	7
	System Acknowledgment	8
	Introduction to Left Navigation Pane Structure	9
	System	10
	Layer 2 Management	10
	Layer 3 Management	11
	Layer 4 Management	12
	Multicast	12
	RMON	13
	Clock	13
	Statistics	13
	Context-Specific Configuration	15
Chapter: 2	System Settings	16
	System Information	16
	System Settings	18
	Line Modules Information	22
	SFP Information	23
	Power Supply Information	24
	Clear Counters	25

System Alarms	.25
System Alarms	.26
System Alarms History	.27
System Alarms Supported	.29
System Resources	.29
System Resources	.29
NVRAM Settings	.32
NVRAM Settings	.32
Peripheral Settings	.36
Peripheral Settings	.36
System Users	.37
CPU Settings	.37
Protecting Against CPU Overloading Settings	.38
Audit Log	.39
System Upgrade	.41
Save and Restore	.42
Save Configuration	.43
Restore Configuration	.45
Factory Reset	.46
Reboot	.47
Syslog Transfer	.47
File Transfer	.49
File Upload	.49
File Download	.51
Diagnostic File Transfer	.52
Audit Log	.52
ACL	.54
MAC ACL Configuration	.54
IP Standard ACL Configuration	.58
IP Extended ACL Configuration	.61
IP Authorized Manager	.65
Port Isolation	.68

Chapter: 3

QoS	70
QoS Ingress	.70
Basic Settings	.71
Data Path	.72
Classifier	.75
Classifier Element	.76
Meter	.78
Token Bucket Meter	.80
Action	.83
Priority Map Settings	.85
Class Map Settings	.87
Class to Priority Settings	.89
Policy Map Settings	.90

	Def UserPri Settings	.94
	QoS Egress	.95
	Queue Template Settings	.95
	Red Conf Settings	.99
	Scheduler Table Settings	103
	Queue Table Settings	105
	Min Rate	106
	Max Rate	108
	Queue Map Settings	110
	Scheduler	112
	Queue	114
Chapter: 4	Authentication Protocols	.116
	802.1x	116
	802.1X Basic Settings	116
	PNAC Traces	119
	802.1X Port Settings	121
	802.1X Timer Configuration	126
	Local Authentication Server Configuration	128
	RADIUS Global Configuration	129
	RADIUS Server Configuration	129
	RADIUS Traces	131
	MAC Session Info	132
	TACACS	133
	TACACS Server Configuration	134
	TACACS Traces	136
	TACACS Active Server Configuration	137
Chapter: 5	Timing Protocols	.138
	Clock	138
		138
	PTP	138
	PTP Global Configurations	139
	Clock Configuration Page	140
	PTP Interfaces	142
	Clock IWF	143
	Clock Interworking Settings	143
	SNTP	145
	SNTP Settings	145
	SNTP Unicast Table	148
	SNTP Broadcast Configuration	150
	SNTP Multicast Configuration	151
	SNTP Manycast Configuration	152
Chapter: 6	Interfaces to the RAPTOR	.154

	SSH	154
	SSH Global Settings	154
	SSL	155
	SSL Global Settings	156
	SSL Digital Certificate	158
	Notes on Digital Certificates	159
	HTTP	160
	HTTP Settings	160
	Web Session	161
	SNMP	162
	SNMP Agent Control Settings	162
	AGENT	163
	SNMP Community Settings	164
	SNMP Group Settings	166
	SNMP Group Access Settings	167
	SNMP View Tree Settings	169
	SNMP Target Address Settings	170
	SNMP Target Parameter Settings	171
	SNMP Filter Profile Settings	173
	User SNMP Security Settings	174
	SNMP Trap Manager	176
	SNMP Filter Settings	177
	SNMP Proxy Settings	179
	SNMP Settings	181
	Telnet	182
	Telnet Settings	182
Chapter: 7	Syslog	183
	BSD Syslog	183
	BSD Syslog Settings	184
	BSD Logging Settings	187
	BSD Syslog File Table	190
	BSD Syslog Mail Table	191
	BSD Syslog Forward Table	192
Chapter: 8	Port Manager	193
	Welcome to Layer 2 Management Page	193
	Port Basic Settings	195
	VLAN Traffic Class Mapping	201
	Port Control	203
	Storm Control	207
	Port Role	210
Chapter: 9	VLAN Section	212
	VLAN	212

	VLAN Basic Settings	213
	VLAN Port Settings	219
	Static VLAN Configuration	223
	VLAN Protocol Group Settings	225
	Port VLAN Protocol Settings	228
	VLAN Port Mac Map	229
	FDB Flush	230
GARP	GARP Configuration	231
	GARP Traces	232
Dynamic VLAN	Dynamic VLAN Global Configuration	234
	Dynamic VLAN Port Configuration	236
	GARP Timers Configuration	238
	GARP Clear Statistics	240
Chapter: 10	Spanning Tree Protocols	241
	RSTP	241
	Global Information	241
	RSTP Traces	245
	RSTP Configuration	247
	Port Status Configuration	248
	RSTP Port Status	253
	MSTP	255
	Global Information	255
	MSTP Traces	259
	MSTP Timers	261
	Port Configuration - CIST Settings	262
	VLAN Mapping	266
	Port Settings	267
	MSTP CIST Port Status	268
	Bridge Priority	270
	PVRST	271
	Global Configuration	271
	Port Configurations	273
	Instance Bridge Configurations	276
	Instance Port Configurations	277
	Instance Port Status	278
Chapter: 11	MRP WebUI Interface	280
	Global Settings	280
	MRP Configuration	281
	MRP Status	283
Chapter: 12	Link Aggregation	284

	Basic Settings	284
	Port Channel Interface Basic Settings	287
	Port Channel Settings	288
	Link Aggregation Port Settings	291
	Link Aggregation Port State Machine Information	293
	Link Aggregation Load Balancing Policy	294
	DLAG Remote Port Channel Information	296
	DLAG Remote Ports Information	297
Chapter: 13	LLDP	298
	LLDP Global Configurations	298
	Configured Traces	300
	LLDP Basic Settings	303
	Interface Settings	305
	Neighbor Information	307
	LLDP Agent Information	307
	LLDP Agent Details	308
Chapter: 14	Serial Communication	311
	Comparison of Serial Communication Standards	311
	RS-232	311
	RS-232 Connectivity	312
	3-wire Mode	312
	Simple Null Modem Cable Route	312
	Simple Straight Through Cable Route - 5-wire Mode	313
	RS-422	313
	Direct Connect Mode	314
	Multi Listener Mode	314
	RS-485	315
	4-Wire Full-duplex Mode	315
	2-wire Half-duplex Mode	316
	Serial Port Configuration	316
	Serial Port Configuration	316
	Serial Profile Configuration	319
	Serial Profile Configuration	320
	Serial Port Statistics	330
Chapter: 15	Filters	332
	L2 Unicast Filter Configuration	332
	L2 Multicast Filter Configuration	334
	Forward Ports Configuration	335
Chapter: 16	Mirroring	337
	ISS Mirroring Control Settings	337

Chapter: 17	Split-Horizon	.339
	Split-Horizon Configuration Settings	339
Chapter: 18	UFD	.340
	UFD Global Configuration Settings	340
	UFD Group Configuration	341
Chapter: 19	DHCP	.343
	DHCP Server	343
	DHCP Basic Settings	344
	DHCP Pool Settings	345
	DHCP Pool Option Settings	347
	DHCP Server IP Exclude Settings	348
	DHCP Host IP Settings	349
	DHCP Host Options Settings	350
	DHCP Bootfile Configuration	351
	DHCP Relay	351
	DHCP Relay Configuration	352
	DHCP Relay Interface Configuration	353
	DHCP Client	354
	Enabling DHCP Client	355
	DHCP Option Type Settings	355
	DHCP Client Identifier Setting	358
Chapter: 20	Routing	.359
	RIP	359
	RIP VRF Creation	359
	RIP Basic Settings	360
	RIP Interface	363
	RIP Neighbour List	365
	RIP Security Settings	366
	RIP Interface Specific Address Summarization	368
	Route Map	369
	Route Map Creation	369
	Route Map Match	371
	Route Map Set	375
	IP Prefix List	378
	OSPF	379
	OSPF VRF Creation	380
	Debug Trace Settings	381
	OSPF Basic Settings	383
	OSPF Area Configuration	386
	OSPF Interface Configuration	388
	OSPF Virtual Interface Configuration	391

OSPF Neighbor Configuration	393
OSPF RRD Route Configuration	394
OSPF Area Aggregation	395
OSPF AS External Area Aggregation	396
Graceful Restart Settings	398
Route Redistribution	400
Redistribution BGP Configuration	401
Redistribution RIP Configuration	403
Redistribution OSPF Configuration	405
VRRP	406
VRRP Global Settings	407
IF Track Settings	408
IP Track Settings	410
VRRP Virtual Router Settings	411
Associated IP Table	414
BGP (Beta Version)	415
BGP Creation	416
BGP Basic Settings	417
BGP Settings	422
Neighbor Configuration	424
BGP MED Configuration	431
BGP Local Preference Configuration	434
BGP Filter Configuration	437
BGP Route Aggregation Configuration	440
BGP Timer Configuration	442
BGP GR Settings	444
TCP-AO MKT Configuration	446
Peer Group Configuration	448
Neighbor Configuration—Peer Group 2	452
Peer Addition	456
Clear BGP	458
BGP Route Map Settings	460
Peer Orf Config	461
ORF Filters	462
Filtering	463
BGP4 (Beta Version)	464
Confederation Settings	464
BGP RFD Settings	465
Community Filter Configuration	467
Routes Community Set Status Table	469
Community Routes	470
Extended Community Filter Configuration	471
Extended Community Set Status Table	473
Routes Extended Community Table	474

Chapter: 22	Multicast Protocols	.478
	IGMP Snooping	478
	IGMP Snooping Configuration - Basic Settings	478
	IGMP Snooping Timer Configuration	483
	IGMP Snooping VLAN Configuration	485
	IGMP Snooping Interface Configuration	488
	IGMP Snooping VLAN Router Port Configuration	489
	IGMP Snooping VLAN Router Ports	491
	IGMP Snooping Static Configuration	491
	MAC Based Multicast Forwarding Table	492
	Multicast Receiver Table	492
	IGMP	493
	IGMP Configuration	494
	IGMP Interface Configuration	495
	IGMP Group Configuration	497
	IGMP Membership Information	498
	IGMP Group List Configuration	498
	IGMP Proxy	499
	IGMP Proxy Configuration	499
	IGMP Upstream Interface Configuration	500
	IGMP Proxy MRoute Configuration	501
	IGMP Proxy Next Hop Configuration	502
	PIM	502
	PIM Basic Settings	503
	PIM Component Configuration	505
	PIM Interface Configuration	506
	PIM Candidate RP Configuration	507
	PIM Static RP Configuration	509
	PIM Global Configuration	510
	PIM DM Global Configuration	511
	PIM Route Configuration	512
	PIM RP Configuration	513
	PIM High Availability	514
	PIM Elected RP Information	515
	PIM DF Information	515
	IPv4 Multicasting	516
	Basic Settings	516
	Interface Settings	517
	TAC	517
	TAC Profile Configuration	518
Chapter: 23	RMON	.519
	RMON Basic Settings	519
	RMON Alarm Configuration	520
	Ethernet Statistics Configuration	522

Event Configuration	524
History	525

Chapter: 24

Statistics	527
Interface	528
Interface Clear	528
Interface Statistics	528
Ethernet Statistics	529
TCP/UDP	530
TCP Statistics	531
TCP Listeners	531
TCP Connections	532
UDP Statistics	533
UDP Connections	533
VLAN	534
Current Database	535
Port Statistics	535
Multicast Table	536
Counter Statistics	537
Capabilities	538
FDB Entries	538
MSTP	539
Information	540
CIST Port Statistics	540
MSTI Port Statistics	541
RSTP	541
Information	542
Port Statistics	542
PVRST	544
Information	544
Instance Information	545
Port Statistics	545
Instance Port Statistics	546
MRP	546
MRP Statistics	547
Link Aggregation	547
Link Aggregation Port Statistics	547
Link Aggregation Neighbour Statistics Information	548
LLDP	550
Traffic Information	550
Statistics Information	552
Error Information	553
802.1x	553
802.1x Session Statistics	553
802.1x Supplicant Statistics Information	555
MAC Session Statistics	555

	RADIUS	556
	QoS	556
	QoS Policer Statistics	556
	QoS CoS Statistics	557
	IGMP Snooping	557
	IGMP Snooping Clear Statistics	558
	IGMP Snooping V1/V2 Statistics	558
	IGMP Snooping V3 Statistics	559
	IP	559
	ARP Cache	559
	ICMP Statistics	560
	IPv4 Interface Specific Statistics	561
	IPv4 System Specific Statistics	561
	RIP	562
	OSPF	562
	OSPF Route Information	563
	Link State Database	563
	Redundancy Information	564
	VRRP	564
	IGMP	565
	IGMP Proxy	566
	IPv4 Multicasting	566
	Route Statistics	566
	Next Hop Statistics	567
	RMON	567
	PTP	568
	SNMP Agent	569
	Serial	570
Chapter: 25	Power over Ethernet (PoE)	572
	Power Over Ethernet	572
	PoE Global Configuration	572
	PoE Global Configuration	572
	PoE Port Settings	573
	PoE Port Settings	573
Chapter: 26	Security	575
	NAT	575
	NAT Global Configuration	576
	Static SNAT Configuration	576
	Dynamic SNAT Configuration	577
	NAPT Configuration	578
	Destination NAT Configuration	580
	All NAT Configurations	581
	Active Connections	582

VPN	582
VPN Global Configuration	583
ACK Packets	587
VPN Policy Configuration	587
VPN Status	593
Firewall	594
Firewall Global Configuration	594
Firewall Rule Configuration	595
Access Group Configuration	598
Firewall Status	600
Security IPv4 Interface Settings	600
Security IP Route Configuration	601
 Index	 i

Introduction

1. Introduction to the WebUI

Introduction to the RAPTOR Web User Interface reference.

RAPTOR™ iMX Series (“RAPTOR” or “the Switch”) is an Intelligent Cyber Secure Platform that supports switching and routing on a single platform. It has a simplified user interface which allows easy configuration and monitoring with a Web-based user interface (*Web UI*). Web-based UI or Web user UI that accept input and provide output by generating web pages viewed by the user using a web browser.

This section introduces the reader to navigation through the Web User Interface.

1.1. Introduction

Introduction to the RAPTOR Web User Interface reference.

RAPTOR™ iMX Series (“RAPTOR” or “the Switch”) is an Intelligent Cyber Secure Platform that supports switching and routing on a single platform. It has a simplified user interface which allows easy configuration and monitoring with a Web-based user interface (*Web UI*). Web-based UI or Web User UI accepts input and provides output by generating web pages viewed by the user using a web browser.

Purpose

This chapter states the purpose and scope of the user manual and lists acronyms and conventions used in all volumes of the user manual. For more information or support, email support@is5com.com.

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

Scope

This document explains in detail all web screens and fields for the Web UI. It does not include the details of the *HTTP* (Hyper Text Transfer Protocol) server architecture, backend processing of web screens, or the protocol details.

Web Interface Conventions

RAPTOR's WEB interface is composed of different screen elements which are used to get input from user and/or to display output. These screen elements are Text Fields, Option Buttons, Check Boxes, Combo Boxes, Buttons, Text Areas, and Lists.

- Web User Interface facilitates new and inexperienced users to create the basic routing and security functions, quickly and effectively. Advanced configuration options can be set only through the CLI.
- A field entry with a * symbol displayed in a Web screen, denotes that it is a mandatory field.
- A drop-down list (as shown below) specifies that the selected LED slot is displayed in all Web screens.



The following sample screens depict the IS5Com Web interface with the standard screen elements named, as it is used in this document.

Figure 1: Web Interface – Different Screen Elements – Part 1

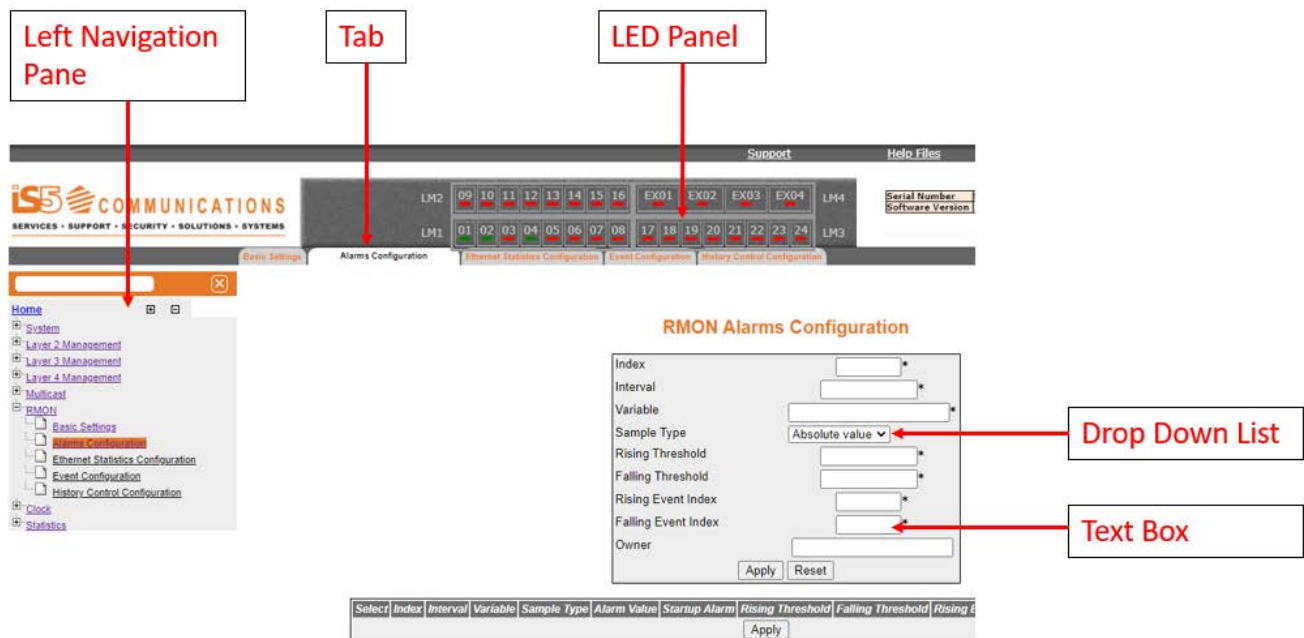
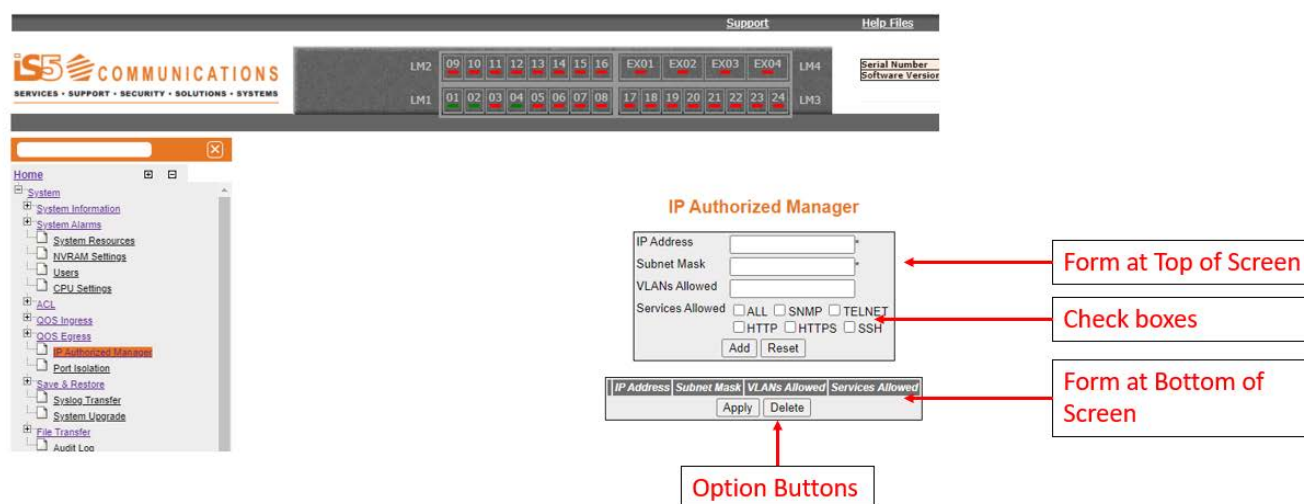
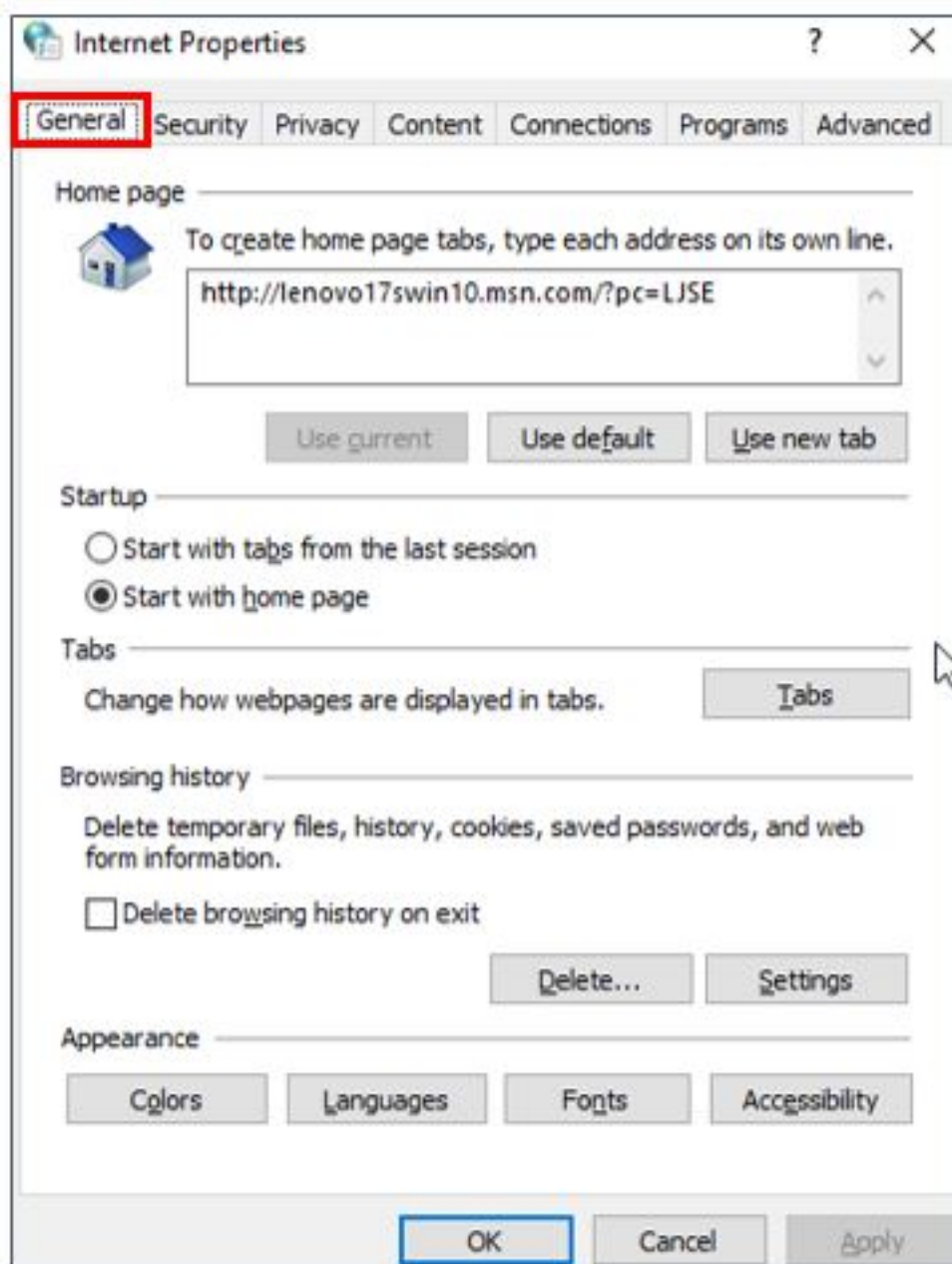


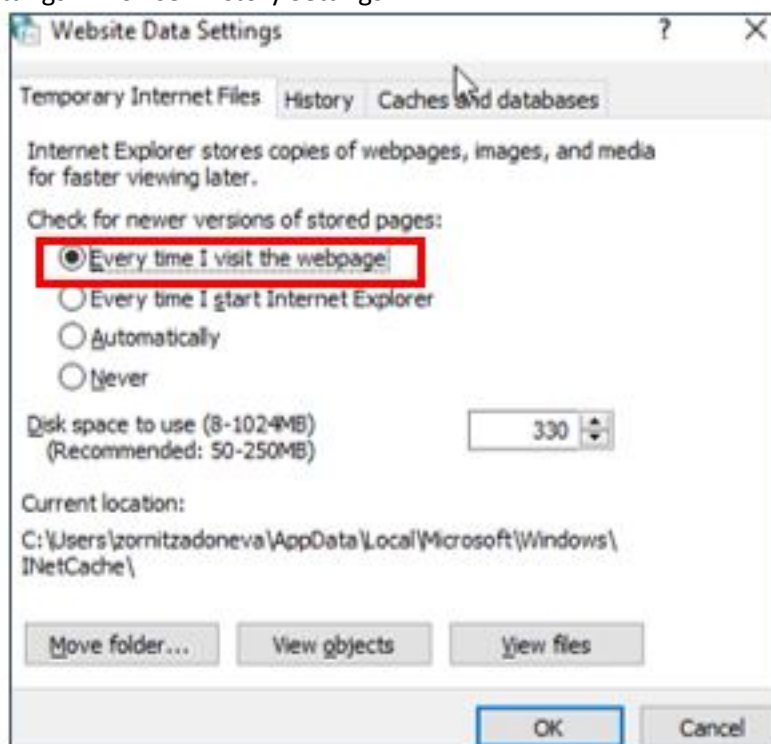
Figure 2: Web Interface – Different Screen Elements – Part 2

Browser Settings

For product screens viewed in Internet Explorer, ensure that the browser settings are follows.

Figure 3: Browser Settings—General Tab

Go to **General**, then **Browsing History**, and click **Settings**.

Figure 4: Browser Settings—Browser History Settings

Select **Every time I visit the webpage** as shown. Click **OK**.

Document Conventions

[Table 1](#) lists the terms and typographical conventions used in this document.

Table 1: Conventions Used in this Document

Convention	Usage	Example
Arial Bold 10	Navigation path to each screen. Includes tab name as well.	Layer 3 Management > IP > VLAN Interface
	Any references to screen elements like action Buttons, option Buttons, check boxes, screens names.	There are two options to save the configuration data namely, Flash Save and Remote Save
<i>Arial 10 Italics</i>	User Inputs to Fields.	Specify the name of the configuration file available in the remote system. The default file name is iS5Com.conf.
Note	Denotes any additional information on an associated topic.	NOTE: All configurations are active only when the SNTP module is enabled.

1.2. Web Interface: Logging into the RAPTOR

This section describes how to login to the RAPTOR via the *Web UI*.

PREREQUISITE:

Figure 5: Ethernet/IP Connectivity



CONTEXT:

RAPTOR can be configured through Web User Interface from Web browsers. The Web User Interface (*Web UI*) allows the user to control various parameters at the System and Protocol level.

Before configuring the RAPTOR from a PC, confirm accessibility of RAPTOR's firmware by pinging it from the PC.

1. An Ethernet cable must connect the switch and a computer. The computer interface should be assigned an IP address on the 192.168.10.0/24 network. This is summarized in [Figure 5](#).

FOR EXAMPLE: An address of 192.168.10.100 with a subnet mask of 255.255.255.0 is one such suitable combination of an IP address and submask to be assigned for the computer to be used in the connection.

- Launch a web browser to enter the RAPTOR's default IP address. The IP address of the RAPTOR's interface is 192.168.10.1.

STEP RESULT: The **Login** page appears.

Welcome to the Raptor device.

- Enter the **User Name** “admin” and **Password** “admin” and click **Login**.

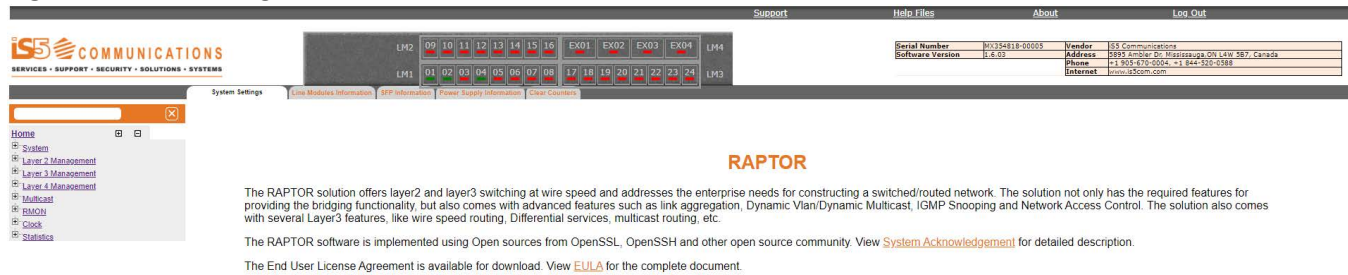
STEP RESULT: The home page will appear.

RESULT:

You have logged into the RAPTOR via the Web User Interface (*Web UI*).

1.3. Home Page

This section describes the Home Page of the *Web UI*.

Figure 6: Home Page

Screen Objective	This screen provides the user with basic information about i55Com and provides links to configure the system and protocol parameters
Navigation	On successful Login from the Login screen
Fields	• System Acknowledgment—to access the i55Com’s System Acknowledgment screen. • Left Navigation Pane—it shows links for accessing system and protocol configuration screens. All links are categorized based on a protocol and functionality. • Right Top Corner Links—the following standard set of links is displayed on the right-hand side top corner of the all Web screens: – Support: To get high-quality and prompt technical support. – Help: To access the User Documentation / Help Files – About: To get additional information about Web management. – Log Out: To Log out the Web session through which the user is connected.
Buttons	• Login—logins to i55Com and views the i55Com home screen.

System Acknowledgment

To go to **System Acknowledgment** page, click **System Acknowledgment**.

Figure 7: System Acknowledgment

Open Source Software References

Packet Name	License	Description
U-Boot 2016.09	GNU GPLv2	U-Boot Boot Loader
NXP SDK v2.0-1703	GNU GPLv2	Linux Drivers Linux Kernel-4.1.30
OpenSSL v1.1.1	Double license: OpenSSL License and the original SSLeay license	OpenSSL is a toolkit for the Transport Layer Security and Secure Sockets Layer protocols.
libssh v0.8.90	LGPL	Multiplatform C library implementing the SSHv2 protocol on client and server side.
Marvell CPSS v4.1.622 Components	GPLv2	Buildroot and Patches Linux cross compilation tool.
Marvell CPSS v4.1.622 Components	Apache 2.0	FPA h-files

1.4. Introduction to Left Navigation Pane Structure

This chapter describes the organization of several modules and features under respective links in the Home page.

Figure 8: iS5 Home Page

System Settings | **Link Modules Information** | **STP Information** | **Power Supply Information** | **Clear Cookies**

Home | **System** | **Layer 2 Management** | **Layer 3 Management** | **Layer 4 Management** | **Multicast** | **BMON** | **Clock** | **Statistics**

RAPTOR

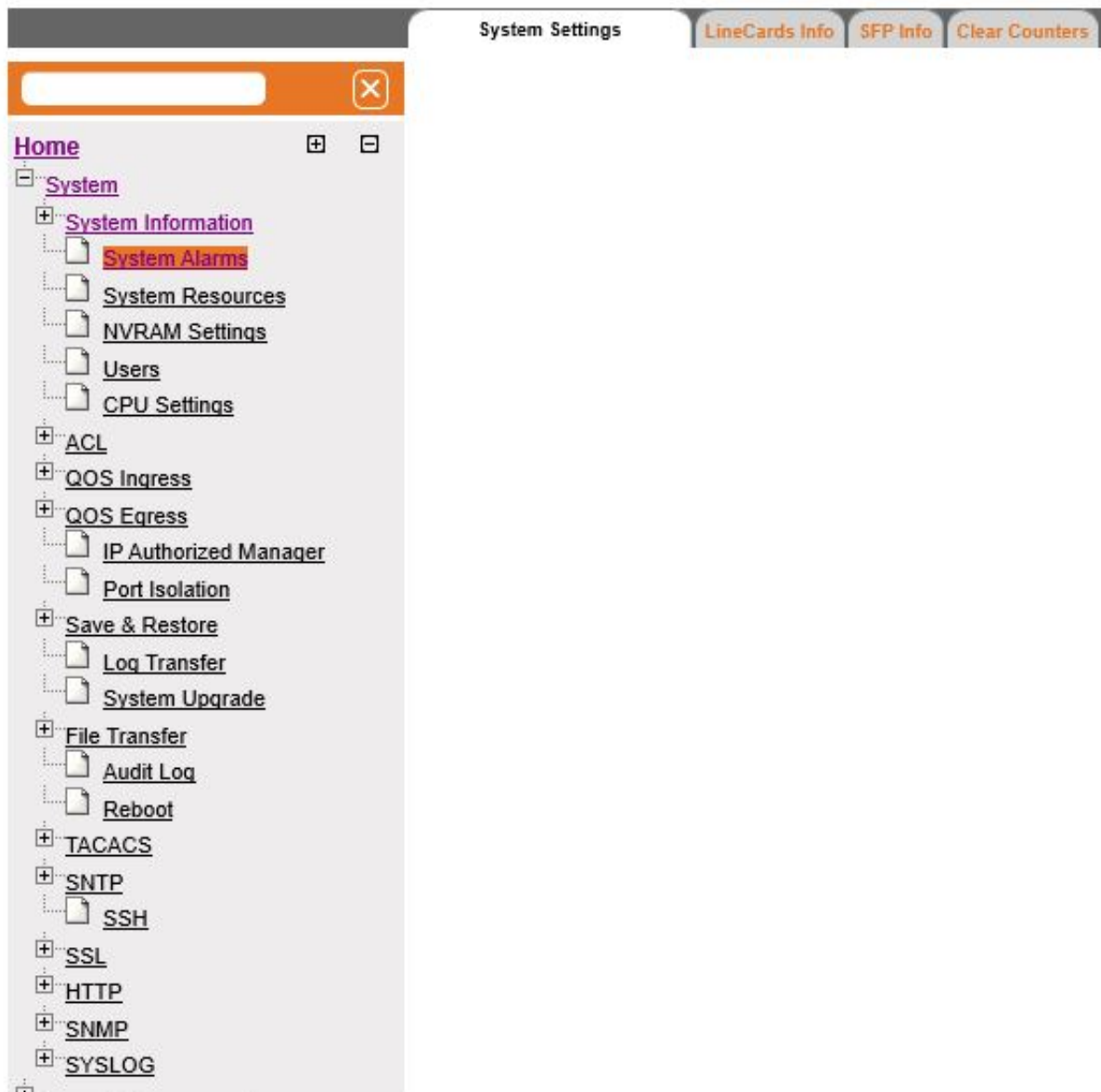
The RAPTOR solution offers layer2 and layer3 switching at wire speed and addresses the enterprise needs for constructing a switched/routed network. The solution not only has the required features for providing the bridging functionality, but also comes with advanced features such as link aggregation, Dynamic Vlan/Dynamic Multicast, IGMP Snooping and Network Access Control. The solution also comes with several Layer3 features, like wire speed routing, Differential services, multicast routing, etc.

The RAPTOR software is implemented using Open sources from OpenSSL, OpenSSH and other open source community. View [System Acknowledgement](#) for detailed description.

The End User License Agreement is available for download. View [EULA](#) for the complete document.

System

Figure 9: System Information Home Page

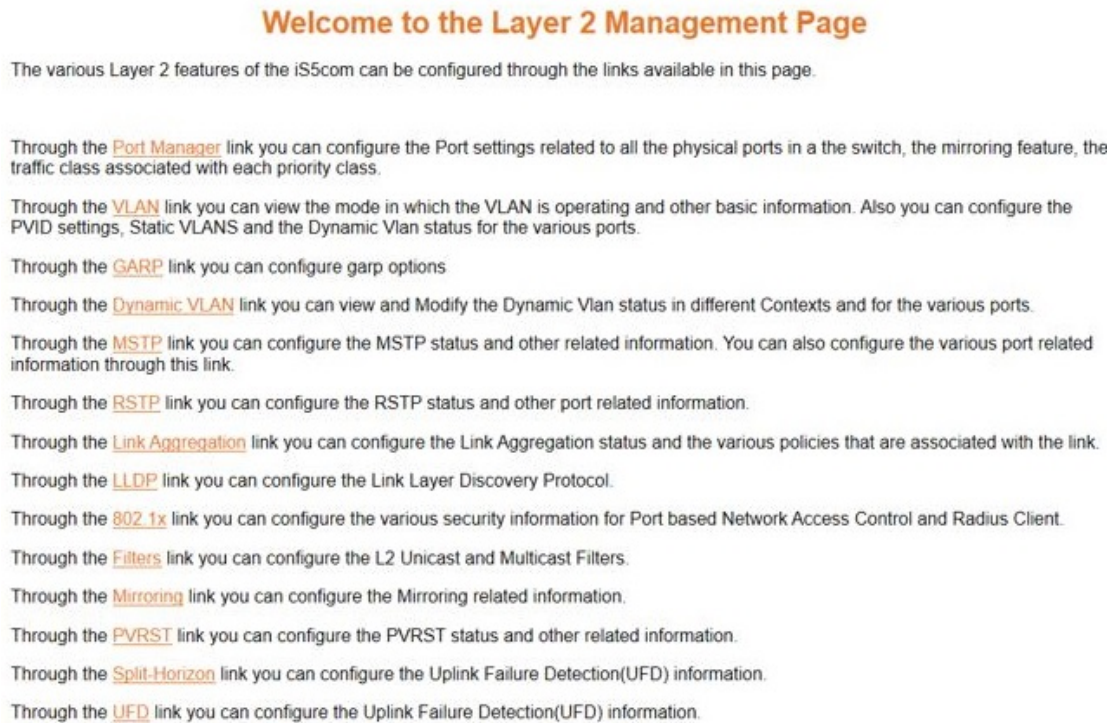


This link has sub-links in the left navigation pane for all system-specific configuration and system specific modules. System-specific configuration can be performed through the screens displayed by these links.

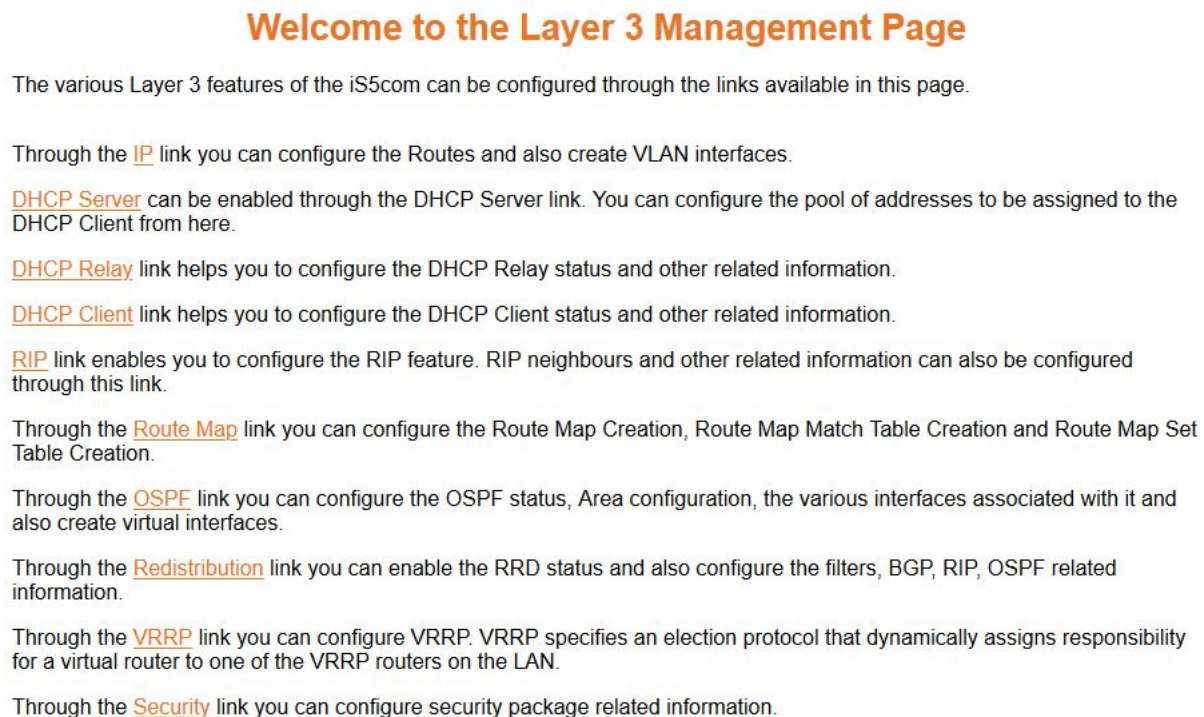
The **System Information** link provides access to all shown above links.

Layer 2 Management

This link has sub-links for all Layer 2 related features and modules. Layer 2 configuration can be performed through the screens displayed by these links.

Figure 10: Layer 2 Management Home Page

Layer 3 Management

Figure 11: Layer 3 Management Home Page

The **Layer 3 Management** link on the left pane provides access to the following links. There are also individual chapters with these titles in this WebUI User Manual.

Layer 4 Management

Figure 12: Layer 4 Management

Layer 4 Switching Filter

Filter Number *

Protocol

Port Number

Copy-To-Port

Select	Filter Number	Protocol	Port Number	Copy-To-Port
Delete				

This link has sub-link for Layer 4 switching filter. Layer 4 switching filter enhances the ability of the Layer 3 switches to control and forward network traffic based on the information that can be derived from protocols operating at Layer 4.

The **Layer 4 Management** link on the left pane provides access to the **Switch Filter**. There is also an individual chapter with such title in this user manual.

Multicast

Figure 13: Multicast Home Page

Welcome to the Multicast Page

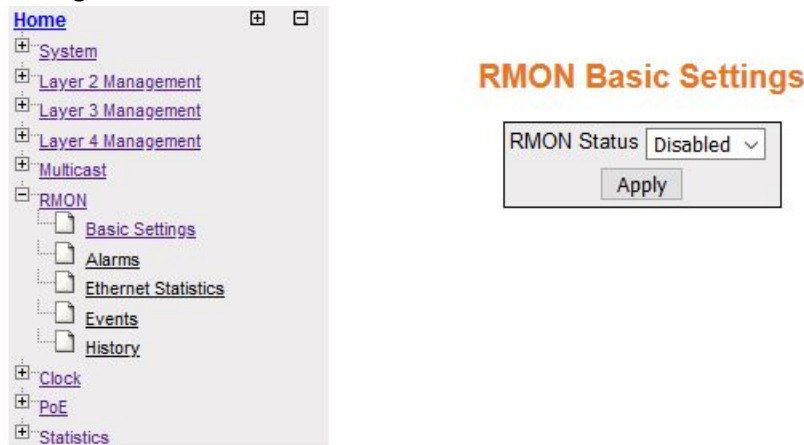
The various Multicast features of the iS5com can be configured through the links available in this page.

- Through the [IGMP Snooping](#) link you can configure the IGMP Snooping status and other related information.
- Through the [IGMP](#) link you can configure the IGMP status and other related information.
- Through the [IGMP Proxy](#) link you can configure the IGMP Proxy related information.
- Through the [PIM](#) link you can configure the interfaces that are to be associated with PIM and also the candidate RP information.
- Through the [IPv4 Multicasting](#) link you can configure Multicasting Routing status and other related information.
- Through the [TAC](#) link you can configure filter rules for particular profile and internet address type that can be used by multicast protocols.

The link **Multicast** shows sub-links for multicast protocols. Multicast protocols are involved in transmitting a message to a set of selected multiple recipients.

RMON

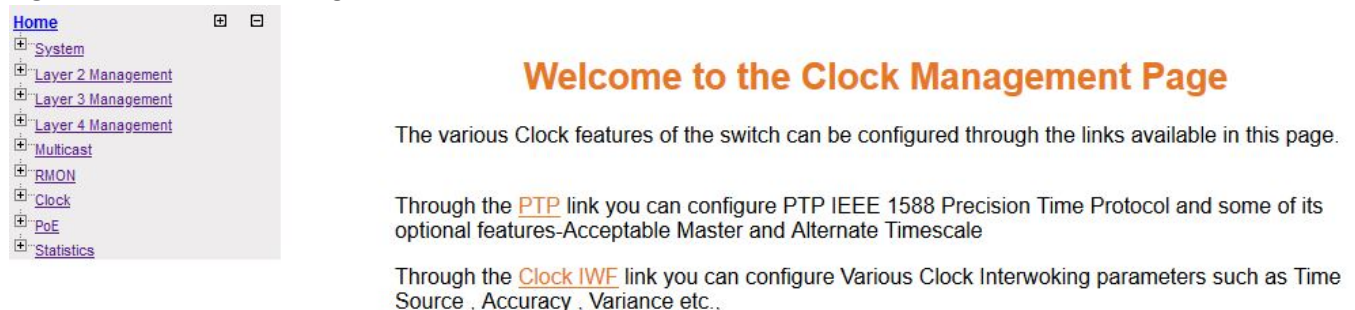
Figure 14: RMON Home Page



This link allows the user to perform RMON-related configuration. All screens are explained in the **RMON** chapter.

Clock

Figure 15: Clock Home Page



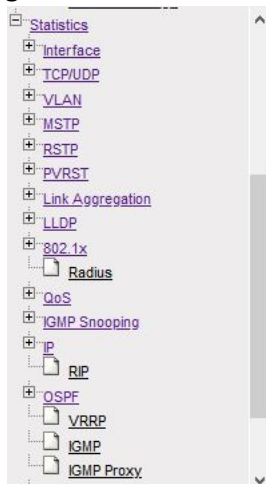
This link has sub-links for clock-related features and modules. Clock-related configuration can be performed.

The **Clock** link on the left pane provides access to the following links:

- PTP
- Clock *IWF* (InterWorking Function)

Statistics

This link has sub-links for statistics of several modules and features.

Figure 16: Statistics Home Page

Welcome to the Statistics Page

The Statistics of the various layer2, layer3 protocols and other information of the iS5com can be viewed through the links available in this page.

The **Statistics** link provides access to the links as shown in the figure below.

Figure 17: Statistics Links

1.5. Context-Specific Configuration

Configuring VLAN settings using the Context ID.

There is a global configuration with context ID of 0 as shown in the following figure.

Figure 18: RSTP Configuration Screen

Global Configuration

Select	Context Id	System Control	Status	Dynamic Path Cost Calculation	Speed Change Path Cost Calculation	Flush Interval	Flush Indication Threshold	BPDU Guard
☒	0	Start ▼	Enabled ▼	False ▼	False ▼	0	0	Disable ▼

Note : To enable RSTP Functionality, **MSTP** and **PVRST** should be disabled.

Figure 19: RSTP Configuration Screen with Context id Shown

RSTP Configuration

Select	Context Id	Priority	Version	Tx Hold Count	Max Age	Hello Time	Forward Delay
☒	0	32768	RSTP Compatible ▼	6	20	2	15

To view the VLAN Port settings for a default context, go to **Layer 2 Management > VLAN > Port Settings**. The **VLAN Port Settings** page appears.

Figure 20: VLAN Port Settings—Configuration Screen

VLAN Port Settings

Select	Port	MAC Based VLAN	Port and Protocol Based VLAN	Port Protected	Subnet Based VLAN	PVID	Acceptable Frame Types	Ingress Filtering	Ingress EtherType Prefix Hex values by Itr	Egress EtherType Prefix Hex values by Itr	Egress TPID Type	Allowable TPID1	Allowable TPID2	Allowable TPID3
☐	Gi0/1	Disabled ▼	Enabled ▼	False ▼	Disabled ▼	1	All ▼	Disabled ▼	8100	8100	Portbased ▼	0	0	0
☐	Gi0/2	Disabled ▼	Enabled ▼	False ▼	Disabled ▼	1	All ▼	Disabled ▼	8100	8100	Portbased ▼	0	0	0
☐	Gi0/3	Disabled ▼	Enabled ▼	False ▼	Disabled ▼	1	All ▼	Disabled ▼	8100	8100	Portbased ▼	0	0	0
☐	Gi0/4	Disabled ▼	Enabled ▼	False ▼	Disabled ▼	1	All ▼	Disabled ▼	8100	8100	Portbased ▼	0	0	0
☐	Ex0/3	Disabled ▼	Enabled ▼	False ▼	Disabled ▼	1	All ▼	Disabled ▼	8100	8100	Portbased ▼	0	0	0
☒	Ex0/4	Disabled ▼	Enabled ▼	False ▼	Disabled ▼	1	All ▼	Disabled ▼	8100	8100	Portbased ▼	0	0	0

System Settings

2. System Settings

Brief Introduction to the System Settings

The System section of the Web allows the user to adjust system settings such as the switch name, counters, alarms and non-volatile settings. Items such as system upgrades, reboots, and log settings are also covered.

2.1. System Information

The System Information section allows the user to view and configure various system properties and settings.

To access **System Information** screen, go to **System > System Information**.

The **System Information** link contains the following tabs.

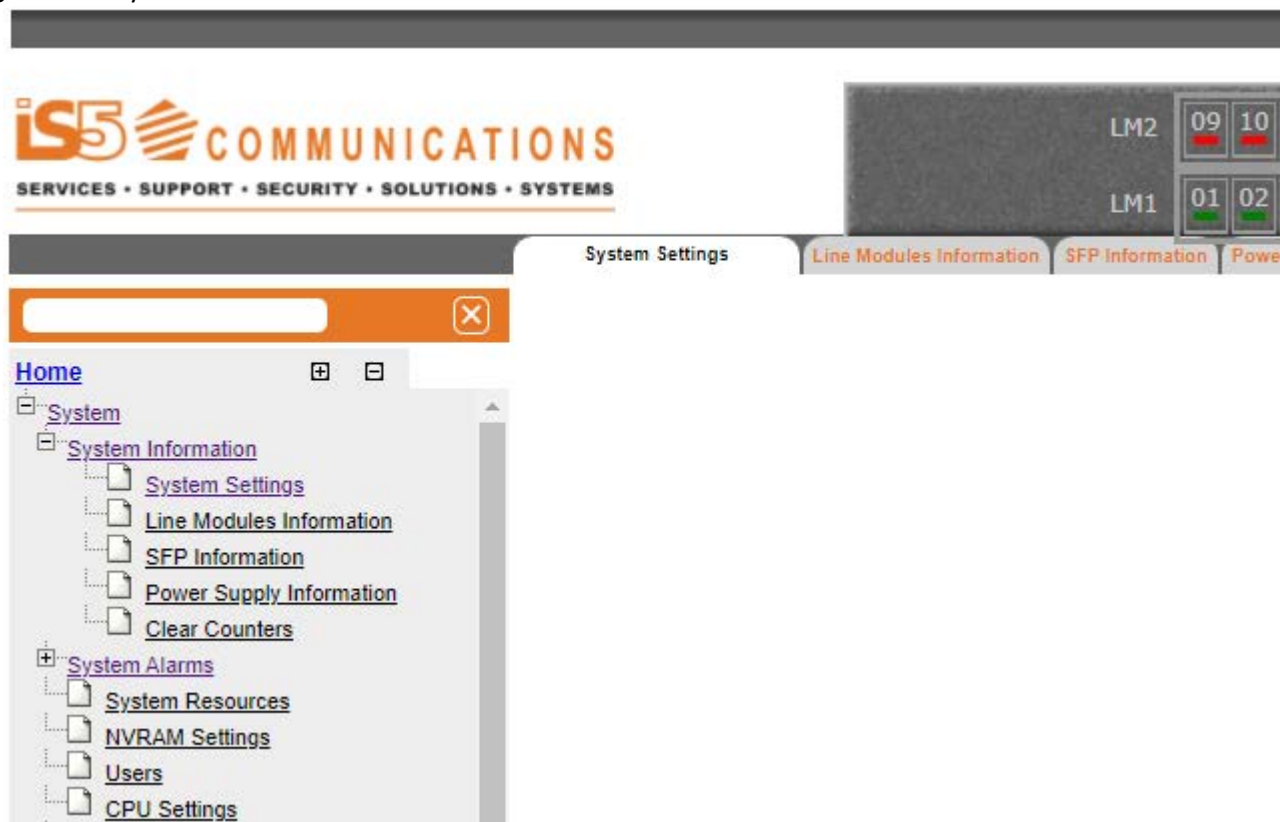
[System Settings](#)

[Line Modules Information](#)

[SFP Information](#)

[Power Supply Information](#)

[Clear Counters](#)

Figure 1: System Information

By default, the tab **System Information** displays the **System Information** screen.

System Settings

Figure 2: System Settings

System Settings

iBiome Software Version	1.12.03
Model Name	iMX950-HV-XX-XX-8GSFP-8GSFP-8GSFP-4TGSFP
Serial Number	MX350119-00003
Factory Name	iMX950
Factory Version	1531-0001-B05
Factory Subrevision	001
Factory Serial Number	1531-0001-B05-27-20-0162
Factory Chassis Part Number	N/A
Primary Software Version	9.2.9
FPGA Firmware Version	4.10
UBoot Software Version	U-Boot 2016.09 ver 1.31
Linux Software Version	Linux iS3000 Local version v1.20
CPLD Version	2.1
PSM Version	1.8
Switch Name	Raptor
Prompt Name	iS5comm
Banner Name	iBiome OS
System Contact	iS5com
System Name	iS5com
System Location	iS5com
Logging Option	CONSOLE ▾
Device Clock	23:59:49 2019-11-26
Device Up Time	0 Days 0 Hrs, 21 Mins, 35 Secs
Login Authentication Mode	Local ▾
Configuration Save Status	Not Initiated
Remote Save Status	Not Initiated
Configuration Restore Status	Not Initiated
Traffic Separation Control	None

Screen Objective	This screen allows the user to configure the system information.
Navigation	System > System Information > System Settings

Fields	• iBiome Software Version—displays the hardware version number. • Model Name—displays the hardware configuration of the system. • Serial Number—displays the serial number of the system. • Factory Name—displays the factory model name. • Factory Version—displays the factory version. • Factory Subrevision—displays the factory subrevision. • Factory Serial Number—displays the mainboard serial number. • Factory Chassis Part Number—displays the factory chassis part number. • Primary Software Version—displays the software version number of the system. • FPGA Firmware Version—displays the <i>FPGA</i> firmware version number. • U-Boot Software Version—displays the U-Boot software version number. • Linux Software Version—displays the Linux software version number. • CPLD Version—displays the <i>CPLD</i> version number. • PSM Version—displays the PSM version number. • Switch Name—enter the name for identifying the device. The default value is iS5. This value range is a string of size 15. • Prompt Name—enter the prompt name to be used. The default value is iS5. • Banner Name—enter the banner name to be used. The default value is RAPTOR iBiome Operation System. • System Contact—enter the contact person details for this managed node. This value range is a string of size 50. The default value is iS5com. • System Name—enter the system name. The default value is iS5com. • System Location—enter the physical location of this node. This value range is a string of size 50. The default value is iS5com. • Logging Option—select the path to log the debug details. The default option is Console. The list contains:— select the current date and time. The format is Day Month Date Year Hours Minutes Seconds Example: Fri May 07 2010 13: 40: 00. – CONSOLE—logs the debug details in a console. – FILE—logs the debug details in a file (system buffer). • Device Clock— select the current date and time. The format is Day Month Date Year Hours Minutes Seconds Example: Fri May 07 2010 13: 40: 00. • Device Up Time—displays the time from which the device is up. The format is Days Hours, Minutes, Seconds Example: 0 Days 1Hrs, 15Mins, 27 Secs.

Fields (cont)	• Login Authentication Mode—select the Login Authentication Mode. The list contains: – Local —sets the Authentication Mode as Local. The user identification, authentication, and authorization method are chosen by the local system administration and does not necessarily comply with any other profiles – Remote—sets the Authentication Mode as Remote. Authentication is done in the remote location through a <i>RADIUS</i> (Remote Authentication Dial-In User Service) or <i>TACACS</i> server. <i>RADIUS</i> is a 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. <i>TACACS</i> (Terminal Access Controller Access-Control System) is a remote authentication protocol that is used to communicate with an authentication server commonly used in networks – tacacs—sets the authentication mode as <i>TACACS</i>. Authentication is done through a <i>TACACS+</i> server. • Configuration Save Status—displays the configuration save status. The default option is Not Initiated. Once the configuration is done, the save status will be displayed as any of the following: – Successful—system information is configured and saved successfully. – Failure—system information configuration Save failed. – In progress—system information configuration save is in-progress. – Not Initiated—system information configuration save is not initiated. • Remote Save Status—displays the remote save status. The default option is Not Initiated. This status represents the status of save operation to the remote location as any of the following: – Successful—remote information is configured and saved successfully. – Failure—remote information configuration Save failed. – In progress—remote information configuration save is in-progress. – Not Initiated—remote information configuration save is not initiated. • Configuration Restore Status—displays the configuration restore status. The default option is Not Initiated. The already configured parameter will be restored and the status will be displayed as any of the following: – Successful—configuration is restored successfully. – Failure—configuration restore failed. – In progress—configuration restore is in-progress. – Not Initiated—configuration restore is not initiated.

Fields (cont)	• Traffic Separation Control—displays the traffic separation control status. This implies the method for receiving control packets to <i>CPU</i>. The default option is None. The options can be: – System_default—specifies the method for receiving control packets to <i>CPU</i> as system default. This implies that the software can automatically install <i>ACL</i> and <i>QoS</i> rules for all control packets. If the configuration is changed from 'system_default' to 'user_defined' option, then all default <i>ACL/QoS</i> rules for carrying protocol control packets to <i>CPU</i> are removed. Then user has to install the specific <i>ACL/QoS</i> rules, to carry the intended control packets to <i>CPU</i> for the processing. – User_defined—specifies the method for receiving control packets to <i>CPU</i> as user defined. This implies that the software cannot automatically install the <i>ACL</i> and <i>QoS</i> rules for all control packets. Only the administrator can install the required rules for receiving control packets to <i>CPU</i>. If the configuration is changed from 'user-defined' to system-default or none, all default <i>ACL</i> filters are installed. Already existing (if any) user configured <i>ACL</i> rules in the system will be not removed. – None—specifies the method for receiving control packets to <i>CPU</i> as none. – If the configuration is changed from 'none' to 'system_default' option, then all default <i>ACL</i> filters for carrying protocol control packets to <i>CPU</i> are removed and new set of filters will be installed. Each filter will be associated with <i>QoS</i> rules. If the configuration is changed from 'none' to 'user_defined' option, then all default <i>ACL</i> filters for carrying protocol control packets to <i>CPU</i> are removed. Then user has to install the specific <i>ACL/QoS</i> rules, to carry the intended control packets to <i>CPU</i> for the processing.
Buttons	• Apply—logs to IS5Com and views the Home screen.

Line Modules Information

Figure 3: Line Modules Information

Line Modules Information

Card #	Part #	Module	Sub Revision	Serial #	Minimum Operating Temperature (°C)	Maximum Operating Temperature (°C)	Current Operating Temperature (°C)
1	1531-0001-A01	IRM-8GSFP	001	s4217-00001	-40	105	37
2	1531-0009-A01	IRM-8GRJ45	001	R8RJ450219-0003	-40	105	39
3	1031-0017-A02	IRM-8GRJ45	001	R8PGRJ450419-0062	-40	105	35
4	1531-0003-B01	IRM-TGSFP	001	R4TGSFP0119-0002	-40	105	32

Screen Objective	This screen allows the user to find information about the line modules.
Navigation	System > System Information > Line Modules Information

Fields	• Card #—displays card#. • Part#—displays part number (e.g. 1531-0004-A02) • Module—displays part number (e.g. iRM-8PGRJ45) • Sub Revision—displays part number (e.g. 001) • Serial #—displays the part number (e.g. R8PGRJ450419-0049) • Minimum Operating Temperature (C)—displays minimum temperature (e.g. -40) • Maximum Operating Temperature (C)—displays maximum temperature (e.g. 105) • Current Operating Temperature (C)—displays current temperature (shown 37)
Buttons	• Apply—modifies attributes and saves the changes.

SFP Information

Figure 4: SFP Info

SFP Info									
Port #	Type	Vendor	Serial #	Part #	Temp. (C)	Voltage (V)	Current (mA)	TxPower (dBm)	RxPower (dBm)
1	NOT PRESENT								
2	NOT PRESENT								
3	NOT PRESENT								
4	NOT PRESENT								
5	1000BASE_LX	FS	C1807117597 180801	CW61-1G-20-1610	60	3	24	-1	-50
6	NOT PRESENT								
7	1000BASE_LX	FS	C1807030621 180711	CW61-1G-20-1610	58	3	26	-3	-50
8	NOT PRESENT								
9	NOT PRESENT								
10	NOT PRESENT								
11	NOT PRESENT								
12	NOT PRESENT								
13	NOT PRESENT								
14	NOT PRESENT								
15	NOT PRESENT								
16	NOT PRESENT								
17	NOT PRESENT								
18	NOT PRESENT								
19	NOT PRESENT								
20	NOT PRESENT								
21	NOT PRESENT								
22	NOT PRESENT								
23	NOT PRESENT								
24	NOT PRESENT								
25	NOT PRESENT								
26	NOT PRESENT								

Screen Objective	This screen allows the user to find information about the <i>SFPs</i> .
Navigation	System > System Information > SFP Information

Fields	• Port #—displays port#. • Type#—displays <i>SFP</i>'s type number. • Vendor—displays <i>SFP</i>'s vendor number. • Serial #—displays <i>SFP</i>'s serial number. • Part #—displays <i>SFP</i>'s part number.
Fields	• Temp (C)—displays <i>SFP</i>'s temperature. • Voltage (V)—displays <i>SFP</i>'s voltage. • Current (mA)—displays <i>SFP</i>'s current. • TxPower (dBm)—displays <i>SFP</i>'s TxPower. • RxPower (dBm)—displays <i>SFP</i>'s RxPower.
Buttons	• Apply—modifies attributes and saves the changes.

Power Supply Information

Figure 5: Power Supply Info

Power Supply Information

#	Presence	Module	Version	Serial #	Current Operating Temperature (°C)	Min Voltage	Max Voltage
1	Unknown	Unknown					
2	Unknown	Unknown					

Screen Objective	This screen allows the user to find information about the power supplies.
Navigation	System > System Information > Power Supply Information
Fields	• Presence—displays the power supply. • Module—displays module type. • Version—displays version. • Serial #—displays serial number. • Current Operating Temperature (C)—displays current temperature • Min Voltage—displays the minimum voltage. • Max Voltage—displays the minimum voltage.

Clear Counters

Figure 6: Clear counters

Clear counters

Protocols

- ☐ BGP
- ☐ OSPF
- ☐ RIP
- ☐ IPv4
- ☐ ALL

Apply

Screen Objective	This screen allows the user to clear all or specific health counters.
Navigation	System > System Information > Clear Counters
Fields	• Protocols—select the protocols for which health check counters is to be cleared. The options are: – BGP—clears health check counters for <i>BGP</i>. – OSPF—clears health check counters for <i>OSPF</i>. – RIP—clears health check counters for <i>RIP</i>. – IPv4—clears health check counters for <i>IPv4</i>. – All—clears all health check counters.
Buttons	• Apply—modifies attributes and saves the changes.

2.2. System Alarms

This section describes events and alarms supported by RAPTOR.

An **event** is a distinct incident that occurs at a specific point in time, such as a port status change. Events can indicate errors, failures, or exceptional conditions in the network. Events can also indicate the clearing of those errors, failures, or conditions.

An **alarm** is a response to one or more related events. Only certain events generate alarms. Alarms have a state (cleared or not cleared) and a severity. An alarm inherits the severity of its most recent event. Alarms remain open until a clearing event is generated (or if the alarm is manually cleared).

To access **System Information** screen, go to **System > System Information**.

The **System Information** link contains the following tabs.

- [System Alarms](#)
- [System Alarms History](#)

- *System Alarms Supported*

By default, the tab **System Alarms** displays the **System Resources** screen.

System Alarms

Figure 7: System Alarms

System Alarms

Global Settings

Setting	Value
Status	Enabled ▾
No. of Logs	512 ▴ ▾

Apply

Individual Settings

Type	Enabled	Relay	LED Ind.
Admin	Enabled ▾	Disabled ▾	Disabled ▾
Chassis	Enabled ▾	Disabled ▾	Disabled ▾
Switch	Enabled ▾	Disabled ▾	Disabled ▾
Security	Enabled ▾	Disabled ▾	Disabled ▾
Services	Enabled ▾	Disabled ▾	Disabled ▾
Protocol	Enabled ▾	Disabled ▾	Disabled ▾

Apply

Screen Objective	This screen allows the user to configure type, status, relay, and LED Indicator.
Navigation	System > System Alarms

Fields	• Type—choose the type of alarm. – Admin – Chassis – Module – Switch – Security – Services – Protocol • Enabled • Relay displays the status of the relay. Two options are available: Disabled and Enabled. • LED Ind. displays the status of the <i>LED</i>. Two options are available: Disabled and Enabled.
Buttons	• Apply—modifies attributes and saves the changes.

System Alarms History

Figure 8: System Alarms History

System Alarms History

ID	Type	Severity	Timestamp	State	Description
3037	SWITCH	Critical	May/14/21:47:36	SET	vlan1 Interface Link State DOWN
6000	PROTOCOL	Info	May/14/21:47:36	SET	RSTP root bridge node
3025	SWITCH	Critical	May/14/21:47:36	SET	Ex0/1 Interface Link State DOWN
3026	SWITCH	Critical	May/14/21:47:36	SET	Ex0/2 Interface Link State DOWN
3027	SWITCH	Critical	May/14/21:47:36	SET	Ex0/3 Interface Link State DOWN
3028	SWITCH	Critical	May/14/21:47:36	SET	Ex0/4 Interface Link State DOWN
3009	SWITCH	Critical	May/14/21:47:39	CLR	Gi0/9 Interface Link State UP
3009	SWITCH	Critical	May/14/21:47:41	SET	Gi0/9 Interface Link State DOWN
3009	SWITCH	Critical	May/14/21:47:44	CLR	Gi0/9 Interface Link State UP
3037	SWITCH	Critical	May/14/21:47:44	CLR	vlan1 Interface Link State UP
2000	CHASSIS	Alert	May/14/21:47:46	SET	Power supply limit exceeded
3009	SWITCH	Critical	May/20/15:06:04	SET	Gi0/9 Interface Link State DOWN
3037	SWITCH	Critical	May/20/15:06:04	SET	vlan1 Interface Link State DOWN
3009	SWITCH	Critical	May/20/15:06:07	CLR	Gi0/9 Interface Link State UP
3037	SWITCH	Critical	May/20/15:06:07	CLR	vlan1 Interface Link State UP
3009	SWITCH	Critical	May/20/15:06:08	SET	Gi0/9 Interface Link State DOWN
3037	SWITCH	Critical	May/20/15:06:08	SET	vlan1 Interface Link State DOWN
3009	SWITCH	Critical	May/20/15:06:11	CLR	Gi0/9 Interface Link State UP
3037	SWITCH	Critical	May/20/15:06:11	CLR	vlan1 Interface Link State UP

Clear

Screen Objective	This screen allows the user to configure the type, severity, status, relay, <i>LED</i> Indicator, <i>LED</i> Display, and Auto Clear status.
Navigation	System > System Alarms > Alarms History
Fields	• ID • Type—choose the type of alarm. – Admin – Chassis – Module – Switch – Security – Services – Protocol
Fields (cont.)	• Severity—choose the severity of alarm. – Debug – Info – Event – Warning – Error – Critical – Alert – Emergency • Timestamp shows the time of the alarm occurrence. • State displays the status of the alarm. Two options are available: SET and CLR. • Description—displays the status of the alarm
Buttons	• Clear—modifies attributes and saves the changes.

System Alarms Supported

Figure 9: System Alarms Supported

System Alarms Supported

ID	Description
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
3000	Interface Link State
3001	Line module temperature threshold reac
4000	Invalid login
5000	Firmware upgrade failed
6000	RSTP root bridge node
6001	VRRP master - VRID

Screen Objective	This screen shows the supported alarms.
Navigation	System > System Alarms > System Alarms Supported
Fields	ID—displays the ID of the alarm Description—displays the description of the alarm.

2.3. System Resources

The System Resources related parameters are configured through the screens described in this section.

To access **System Resources** screen, go to **System > System Resources**.

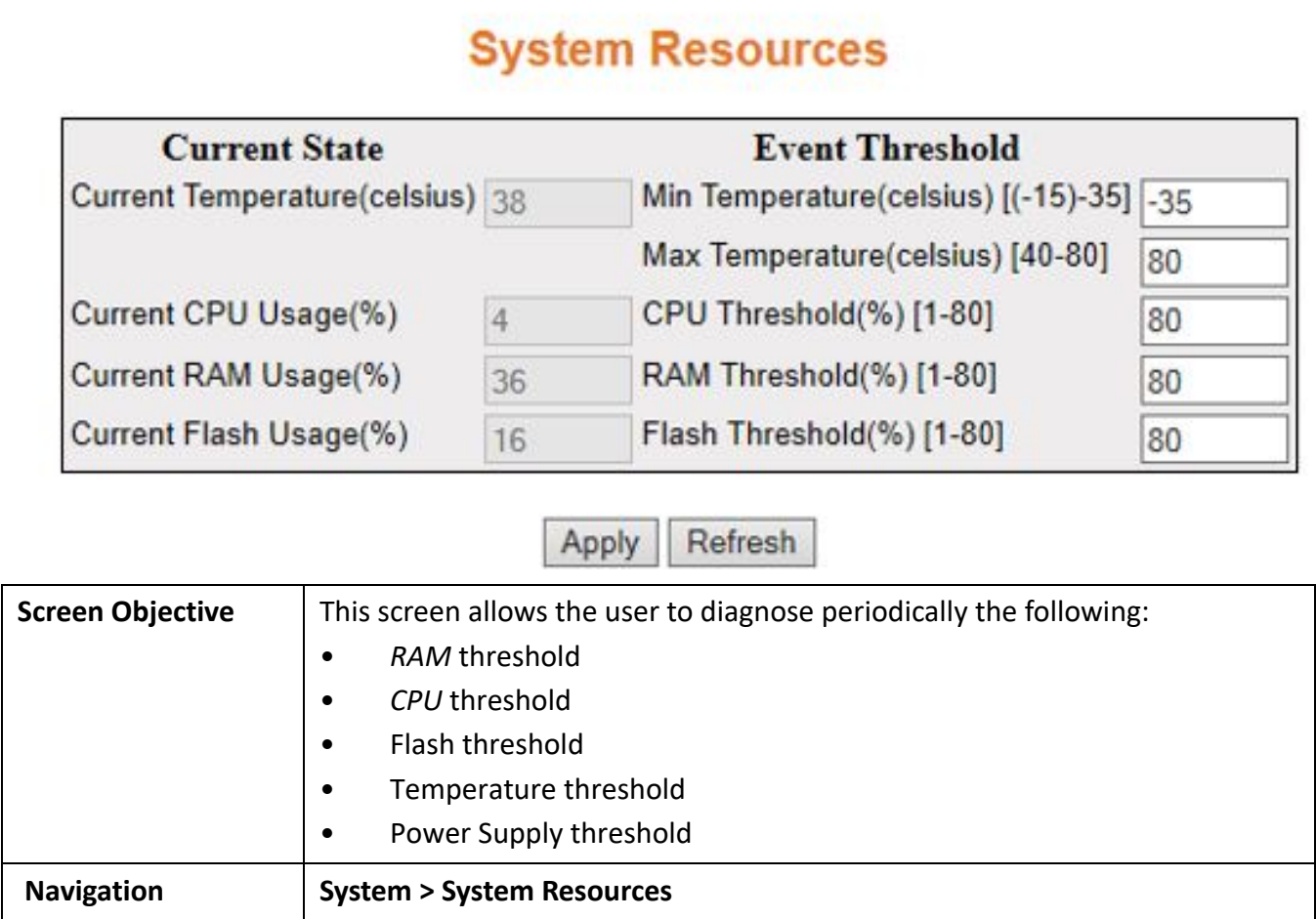
The System Resources related parameters are configured through the screens displayed in the following tabs:

- [System Resources](#)

By default, the tab **System Resources** displays the **System Resources** screen.

System Resources

Figure 10: System Resources



Fields	• Current Temperature (Celsius)—displays the current temperature of the switch in Celsius. NOTE: An <i>SNMP</i> trap with maximum severity is sent to the <i>SNMP</i> Manager if there is any rise or drop in the temperature of the switch. • Current CPU Usage (%)—displays the percentage of current <i>CPU</i> usage of the switch. The default value is 0 percent. • Current RAM Usage (%)—displays the percentage of the current <i>RAM</i> usage of the switch. • Current Flash Usage (%)—displays the percentage of current Flash usage of the switch. • Min Temperature (Celsius)—enter the minimum threshold temperature of the switch in Celsius. The configurable minimum range of threshold temperature is from -15 to -35° Celsius. When the current temperature drops below the threshold, an <i>SNMP</i> trap with maximum severity is sent to the <i>SNMP</i> Manager. • Max Temperature (Celsius)—enter the maximum threshold temperature of the switch in Celsius. This value ranges from 35 to 80° Celsius. The default value is 40. NOTE: When the current temperature rises above the threshold, an <i>SNMP</i> trap with maximum severity is sent to the <i>SNMP</i> Manager. • CPU Threshold (%)—enter the percentage of maximum <i>CPU</i> usage of the switch. This value ranges from 1 to 80 percent. The default value is 80 percent. NOTE: When the <i>CPU</i> load exceeds the threshold value, an <i>SNMP</i> trap with maximum severity is sent to the <i>SNMP</i> Manager. • RAM Threshold (%)—enter the percentage of maximum <i>RAM</i> usage of the switch. This value ranges from 1 to 80 percent. The default value is 80 percent. NOTE: When the <i>RAM</i> usage crosses the threshold percentage, an <i>SNMP</i> trap with maximum severity is sent to the <i>SNMP</i> Manager. • Flash Threshold (%)—enter the percentage of maximum Flash usage of the switch. This value ranges from 1 to 80 percent. The default value is 95 percent. NOTE: When the Flash usage crosses the threshold percentage, an <i>SNMP</i> trap with maximum severity is sent to the <i>SNMP</i> Manager.
Buttons	• Apply—modifies attributes and saves the changes. • Refresh—resets to default value for respective fields and discards all user inputs.

2.4. NVRAM Settings

The *NVRAM* Settings tab allows the user to configure the initialization parameters stored in the *NVRAM* (Non-Volatile Random Access Memory) of the switch.

Whenever the switch is started or rebooted, these initialization parameters are read before task initialization and updated in the local data structure. These parameters are applied to *SNMP*, when the task is created for that component.

NVRAM Settings

Figure 11: NVRAM Settings

NVRAM Settings

IP Address Mode	Manual ▼
IP Address Allocation Protocol	DHCP ▼
Default IP Address	192.168.10.1 *
Subnet Mask	255.255.255.0
Switch Base MAC Address	e8:e8:75:90:5f:c1
Switch Secondary MAC Address	e8:e8:75:90:5f:c0
Default Interface Name	Gi0/1
SNMP Engine ID	80.00.08.1c.04.46.53
PIM Mode	Sparse ▼
Snoop Forward Mode	MAC Based ▼
CLI Serial Console	Yes ▼
MGMT Port Access	Yes ▼
External Storage Access	Yes ▼
Default VLAN Identifier	1
Dynamic Port Count	28
Reset Dynamic Port Count	☐
Incremental Save	Disable ▼
Auto-Save Trigger	Disable ▼
Rollback	Enable ▼
Apply	

Note: Restart of switch required, if any value is changed.

Screen Objective	This screen allows the user to configure the initialization parameters that are stored in the <i>NVRAM</i> of the switch. The screen lists only some of the initialization parameters and not all parameters such as <i>MSR</i> (MIB Save and Restore) feature related parameters of the <i>iS5Comnvram.txt</i> .
Navigation	System > NVRAM Settings

Fields	• IP Address Mode—select the mode by which the default interface in the device gets the IP address. The default option is Manual. The list contains: – Manual—assigns the Static IP address to the default interface. The IP address defined in the field Default IP Address and the IP mask defined in the field Subnet Mask are assigned to the interface. NOTE: If the network in which the switch is implemented contains a server such as DHCP server, allocating IP address, the manually assigned 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. – Dynamic—assigns IP address dynamically; that is, IP address provided by the server in the network is assigned to the default interface on switch reboot. The IP address is fetched through the dynamic IP address configuration protocols such as <i>DHCP</i> client, <i>RARP</i> client, <i>BOOTP</i> client, etc. NOTE: The static IP address is assigned to the default interface even if the mode is selected as Dynamic if the switch fails to fetch the IP address dynamically. • IP Address Alloc Protocol—select the dynamic IP address configuration protocol to be used for fetching the IP address dynamically, if the field IP Address Mode is selected as Dynamic. Allows the user to only view the selected dynamic IP address configuration protocol, if the field IP Address Mode is selected as Manual. The default option is <i>DHCP</i>. The list contains: – RARP—Reverse Address Resolution Protocol (<i>RARP</i>) that allows a client device to dynamically find its IP address, when it has only its hardware address such as <i>MAC</i> address. NOTE: Currently, the <i>RARP</i> option is not supported. – DHCP—Dynamic Host Configuration Protocol (<i>DHCP</i>) that allows a client device to obtain configuration parameters, such as network address, from the server. – BOOTP—Bootstrap Protocol (<i>BOOTP</i>) that allows a client device to obtain its own IP address, address of a server host and name of a boot file to be executed. NOTE: This parameter can be set only when IP Address Mode is dynamic. When set as manual IP Address Alloc Protocol is greyed out. • Default IP Address—enter the default IP address to change the IP address, if the field IP Address Mode is selected as Manual. The default value is 192.168.10.1. NOTE: Default IP address can be configured only when IP address mode is set as Manual. Default IP address is greyed out when IP address mode is set as dynamic. NOTE: If the network in which the switch is implemented contains a server such as <i>DHCP</i> server, 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. NOTE: The configured IP address should be in the same IP range of the network in which the switch is placed.

- **Subnet Mask**—enter the subnet mask for the configured IP address, if the field IP Address Mode is selected as Manual. Allows the user to only view the configured subnet mask, if the field IP Address Mode is selected as Dynamic. The default value is **255.0.0.0**.

NOTE: Subnet Mask can be configured only when IP address mode is set as Manual. Subnet Mask is greyed out when IP address mode is set as dynamic.
NOTE: The configured subnet mask should be in the same subnet of the network in which the switch is placed
- **Switch Base MAC Address**—enter the base *MAC* address of the switch. This *MAC* address is assigned to the default interface of the switch. The switch uses this address as its hardware address. Layer 3 modules use the switch *MAC* address as the source *MAC* address in the transmitted packets. The default value should be from iS5 range e.g. e8:e8:75.
- **Default Interface Name**—enter the interface to be set as the default interface. This is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number. The format is <interface type><slot number/port number>. There is no space between these two entries. All ports available in the switch at that time are populated in the list. Example: Gi0/1 (Here Gi is interface type Gigabit Ethernet interface 0 is slot number and 1 is port number). The default value is Gi 0/1.
- **SNMP EngineID**—Enter 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. The default value is 80.00.08.1c.04.46.53.
- **PIM Mode**—select the operation mode of the *PIM*. The default option is Sparse. The list contains:
 - Dense—sets operation mode of *PIM* as Dense Mode. *PIM* implements a flood and prune mechanism. *PIM* floods multicast traffic periodically and prunes branches of shortest-path tree where no interested receivers are present. This mode is best suited for networks where few or no prunes occur.
 - Sparse—sets operation mode of *PIM* as Sparse Mode. *PIM* forwards multi-cast traffic to the device only if an explicit request is received from that device for this traffic. This mode is best suited for Internet.
- **Snoop Forward Mode**—select the mode to be used for building the forwarding table that is used during *IGS / MLDS*. The default option is *MAC-Based*. The list contains:
 - IP Based—uses table containing IP multicast forwarding information based on both outer and inner *VLAN*, during snooping.
 - MAC Based—uses table containing *MAC*-based multicast forwarding information, during snooping.

- **CLI Serial Console**—select whether the *CLI* console prompt is required for the session through serial console. The default option is Yes. The list contains:
 - Yes—specifies that *CLI* prompt is made available in the serial console session.
 - No—specifies that *CLI* prompt is not made available in the serial console session

NOTE: This value does not affect the availability i55Com *CLI* prompt in the sessions established through Telnet. That is, i55Com *CLI* prompt is always available in the Telnet session.
- **MGMT Port Access** -- Select whether the MGMT Port will be active. This port is typically used for factory use and advanced debugging with factory support. Selecting No will disable the MGMT Port.
- **External Storage Access**-- Selecting No will disable the SD Card and USB peripherals.
- **Default VLAN Identifier**—enter the default *VLAN* identifier to be used at system startup. This *VLAN* is set as default *VLAN* during reboot of the switch. The format of this field is integer. This value ranges from 1 to 4094. The default value is 1 which means that *VLAN* 1 is set as the default *VLAN*.

NOTE: Once the Default *VLAN* ID is configured, the switch has to be restarted before saving any configuration.

NOTE: It is not advisable to change the default *VLAN* ID when some configurations are already saved.
- **Dynamic Port Count**—enter the number of ports required for the i55com. The maximum count equal to the system defined maximum physical interfaces. The default value is the system defined maximum physical interfaces.
- **Reset Dynamic Port Count**—click to enable the Reset Dynamic Port Count. If this check box is enabled, the system takes the default value on restarting the system again.
- **Incremental Save**—select one of the options to indicate whether *SNMP* Update Trigger for Incremental Save is to be generated or not. The default option is Disable. The list contains:
 - Enable—enables the incremental save which generates the update trigger for each time an nmhSet operation is successful.
 - Disable—disables the Incremental Save option which will not generate the update trigger at all.

NOTE: To disable Incremental Save, Auto-save Trigger should be disabled.
- **Auto-save Trigger**—the auto-save trigger option is for saving the completed configuration automatically or manually. The default option is Disable. The list contains:
 - Enable—Specifies that every configuration is saved automatically.
 - Disable—Specifies that completed configuration will not be saved automatically.

NOTE: To enable Auto-Save Trigger, Incremental Save option should be enabled

	• Rollback—select the <i>SNMP</i> rollback feature. The default option is Enable. The list contains: – Enable—enables the <i>SNMP</i> rollback feature. The enabled value specifies that it allows the failure in set operation for any varbind (variable binding), which results in rollback of all <i>Varbinds</i> whose values has been set in this SET PDU. A <i>Varbind</i> (Variable Binding) represents a set of Oid/Value pairs. – Disable—disables the <i>SNMP</i> rollback feature. The disabled value specifies that it allows the failure in set operation to simply return error. • Factory Reset—select to perform factory reset.
Buttons	• Apply—modifies attributes and saves the changes

2.5. Peripheral Settings

The Peripheral Settings tab allows the user to configure the peripheral parameters stored in the *NVRAM* (Non-Volatile Random Access Memory) of the switch. Users may enable/disable peripherals.

Whenever the switch is started or rebooted, these initialization parameters are read before task initialization and updated in the local data structure. These peripheral settings are applied to the switch.

Peripheral Settings

Figure 12: Peripheral Settings

Peripherals Settings

The screenshot shows a configuration window titled "Peripherals Settings". It contains three rows of settings, each with a label and a dropdown menu:

- CLI Serial Console: Yes ▼
- MGMT Port Access: Yes ▼
- External Storage Access: Yes ▼

Below these settings is an "Apply" button.

Screen Objective	This screen allows the user to configure the peripheral setting parameters that are stored in the <i>NVRAM</i> of the switch.
Navigation	System > Peripheral Settings
Fields	• CLI Serial Console — the user may enable or disable the CLI Serial console port. • MGMT Port Access —the user may enable or disable the MGMT Port Access port. • External Storage Access — the user may enable or disable the USB and SD card slots.
Buttons	• Apply—modifies attributes and saves the changes NOTE: Changes to these settings are applied only after the switch restarts.

2.6. System Users

The administrator may add, delete and modify system users through this interface.

Figure 13: User Manager

User Manager

Username *

Password *

Password Verification *

Access Level *

	Username	Password	Access Level
☐	admin	•••••	Admin ▾
☒	guest	•••••	Guest ▾
Delete			

Screen Objective	This screen displays the User Manager options.
Navigation	System > Users
Fields	• Username—enter the Username. • Password—enter the assigned password. • Password Verification —enter password verification. • Access Level—select Access Level. – Admin – Technician – Guest
Buttons	• Apply—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs.

2.7. CPU Settings

CPU Settings allows the administrator to control *MAC* learning rates and intervals. It also permits the administrator to force certain types of traffic through the *CPU*.

The **CPU Settings** link allows the user to access the **Protection Against CPU Overloading Settings** screen. This screen allows the user to configure *MAC* learn rate limit and traffic separation control settings for protecting the *CPU* from overloading.

Protecting Against CPU Overloading Settings

Figure 14: Protection Against CPU Overloading Settings

Screen Objective	This screen provides control to administrator to have system default or user defined <i>ACL/QoS</i> rules to carry control traffic to <i>CPU</i> .
Navigation	System > CPU Settings
Fields	MAC Learn Rate Limit—enter the maximum number of unicast dynamic <i>MAC</i> (L2) entries that a hardware can learn in the system, in a configured time interval. This limit is used to control the number of <i>MAC</i> entries to control plane from the hardware, when hardware <i>MAC</i> learning is enabled. This value ranges from 0 to 2147483647. The default value is 1000. A value 0 disables this feature in the system. This configuration does not impose any restrictions on multicast / broadcast and dynamic / static / protocol <i>MAC</i> learning capability limits. NOTE: The hardware can learn the total sum of the previously learnt <i>MAC</i> entries and present <i>MAC</i> entries until <i>MAC</i> learning reaches the maximum number of L2 unicast dynamic entries learning capacity of the system. If rate limit is changed while <i>MAC</i> Learn Rate Limit Interval timer is running, the modified new rate limit value takes effect during next timer restart.

Fields (cont)	• MAC Learn Rate Limit Interval—enter the time interval within which the maximum number of <i>MAC</i> entries is learned in the system. Any changed timer interval takes effect only in next timer restart. This value ranges from 1 to 100000 milli-seconds. The default value is 1000 milli-seconds. • Traffic Separation Control—select the type of configuration to be implemented for carrying control traffic to <i>CPU</i>. The default option is None. All below three options can be configured during system runtime. The list contains: – systemdefault—specifies that the software automatically installs <i>ACL/QoS</i> rules for all control packets during system init time. Either a switch-and-copy-to-cpu filter or drop-and-copy-to-cpu filter is installed for getting the control packets to <i>CPU</i> for processing. Each <i>ACL</i> rule is associated with class-map, meter and policy map with protocol ID, and <i>CPU</i> queue number. NOTE: If the configuration is changed from 'systemdefault' to 'userconfig' option, all default <i>ACL/QoS</i> rules for carrying protocol control packets to <i>CPU</i> are removed. Then to carry the intended control packets to <i>CPU</i> for processing, the user has to install the specific <i>ACL/QoS</i> rules. – userconfig—specifies that an administrator installs required rules for the control packets as <i>ACL/QoS</i> rules will be not installed automatically. NOTE: If the configuration is changed from 'userconfig' to 'systemdefault', all default <i>ACL/QoS</i> rules are installed. Already existing (if any) user configured <i>ACL</i> rules in the system are not removed during such change. NOTE: If the configuration is changed from 'userconfig' to 'none', all default <i>ACL</i> filters are installed. Already existing (if any) user configured <i>ACL</i> rules in the system are not removed during such change. – None—specifies that the software automatically installs <i>ACL/QoS</i> rules for all control packets during system init time. Either a switch-and-copy-to-cpu filter or drop-and-copy-to-cpu filter is installed for getting the control packets to <i>CPU</i> for processing. Each <i>ACL</i> rule is associated with class-map, meter and policy map with protocol ID, and <i>CPU</i> queue number. NOTE: If the configuration is changed from 'none' to 'systemdefault' option, then all default <i>ACL</i> filters for carrying protocol control packets to <i>CPU</i> are removed and a new set of filters is installed. Each filter is associated with <i>QoS</i> rules. NOTE: If the configuration is changed from 'none' to 'userconfig' option, then all default <i>ACL</i> filters for carrying protocol control packets to <i>CPU</i> are removed. To carry the intended control packets to <i>CPU</i> for processing, the user has to install the specific <i>ACL/QoS</i> rules.
Buttons	• Apply—modifies attributes and saves the changes

2.8. Audit Log

This section describes how to configure the Audit Log.

The **Audit Log** link allows the user to access the **System Logging Information** screen which is used to configure the logging information.

Figure 15: System Logging Information

System Logging Information

Audit-Logging	Disable ▾
Audit-Logging File-Name	/mnt/config/config.t
Audit-Logging File-Size	4194304
Audit-Logging File-Size-Threshold	80
Audit-Logging Reset	FALSE ▾
Apply	

Screen Objective	This screen allows the user to configure the logging information. The Audit logs are used for creation and update of confidential information.
Navigation	System > Audit Log
Fields	• Audit-Logging—select the Audit logging feature status in the system. The default option is disable. The list contains: – Enable—enables the Audit logging and email alert features in the system – Disable—disables the Audit logging feature. • Audit-Logging File-Name—enter the name of the file that captures the log information. Default file name is config.txt. • Audit-Logging File-Size—enter the size of the log file that captures the information. The value ranges from 1024 to 1048576. The default file size is 1024 bytes. • Audit-Logging File-Size-Threshold—enter the threshold value which indicates the maximum log storage size value. The unit in use is percent. The value ranges from 1 to 99 percent. The default value is 70 percent. • Audit-Logging Reset—select the reset option in the module. The default option is False. The Syslog server IP Address and log level information are captured during configuration and stored in log file. The list contains. – True –The syslog server IP address and log level information are flushed. – False—Disables the Audit logging reset.
Fields (cont)	NOTE: The logging reset automatically reverts to False, once the configuration is applied to the switch NOTE: Setting the audit logging reset field to true, erases the contents in audit logging file name and starts logging.

Buttons	Apply—modifies attributes and saves the changes.

2.9. System Upgrade

System Upgrade describes the fields and file sources used to upgrade firmware on the switch.

The **System Upgrade** link allows the user to access the **System Upgrade** screen which is used to perform an image download operation on a switch stack or on a standalone switch.

Figure 16: System Upgrade

System Upgrade

Upgrade From	TFTP ▾
Address Type	IPv4 ▾
Server IP Address	
SFTP User Name	
SFTP Password	
File Name	firmware_upgrade.tgz
Apply	

Image download not started

Screen Objective	This screen allows the user to perform an image download operation on a switch stack or on a standalone switch to download a new image from a <i>TFTP</i> or <i>SFTP</i> from a remote location, to the switch and to overwrite or keep the existing image.
Navigation	System > System Upgrade
Fields	Upgrade From—select the type of server from which the image is to be downloaded. The default option is <i>TFTP</i>. The list contains: <i>TFTP</i>—sets the server type as <i>TFTP</i> (Trivial File Transfer Protocol) mode. <i>SFTP</i>—sets the server type as <i>SFTP</i> (SSH File Transfer Protocol) mode. <i>USB</i>—sets the server type to USB. Address Type—select the IP Address type of the machine from which the image is to be downloaded. The default option is <i>IPv4</i>. Server IP Address—enter the IP address of the machine from which the image is to be downloaded.

Fields (cont)	• SFTP User Name—enter the user name required for downloading the image from <i>SFTP</i> server. This field is a string with the maximum size 20. NOTE: This field is disabled if the Upgrade Form is set as <i>TFTP</i> server. • SFTP Password—enter the password required for downloading the image from <i>SFTP</i> server. This field is a string with the maximum size 20. NOTE: This field is disabled if the Upgrade Form is set as <i>TFTP</i> server. • File Name—enter the name of the image to be downloaded from the remote system.
Buttons	• Apply—modifies attributes and saves the changes.

2.10. Save and Restore

Used to save and restore configuration files to and from the switch.

The **Save and Restore** link allows the user to configure the current configuration **Save and Restore** options for the switch.

To access **Save and Restore** screens, go to **System > Save and Restore**.

The **Save and Restore** link parameters are configured through the screens displayed by the following tabs:

[Save Configuration](#)

[Restore Configuration](#)

[Factory Reset](#)

By default, the tab **Save** displays the **Save Configuration** screen.

Save Configuration

Figure 17: Save Configuration

Save configuration

Save option

☒ Flash Save
☐ USB Save
☐ Remote Save

Save Format

MiB OID ▾

Transfer Mode

TFTP ▾

Address Type

IPv4 ▾

IP Address

0.0.0.0

SFTP User Name

SFTP Password

File Name

iss.conf

Apply

Reset

Saving configuration not started

Screen Objective	This screen allows the user to save the current configuration of the switch in a file. When save operation is initiated, all configurations made through <i>CLI</i>, <i>SNMP</i> or Web interfaces are saved in a configuration file – iss.conf. There are three options to save the configuration data: Flash Save, USB Save, and Remote Save. A Flash Save Configures that the configurations need to be saved in Flash, USB Save to a USB, whereas a Remote Save specifies that the configurations need to be saved to a remote system.
Navigation	System > Save and Restore > Save

Fields	• Save option—click one of the option buttons to specify the save option to be used. The options are: – Flash Save—saves the configurations in the specified file name of Flash. – USB Save—saves on a USB. – Remote Save—saves the configurations in the remote system which is specified by Address Type and IP address. • Save Format—select from the 2 available options (<i>MIB OID</i> is the current option): – Script – <i>MIB OID</i> • Transfer Mode—select the transfer mechanism to save the Switch configurations in the remote system. The remote host machine should have a <i>TFTP / SFTP</i> capable Server running for this operation to be successful. The default option is <i>TFTP</i>. The list contains: – TFTP—saves the switch configuration to the remote system through <i>TFTP</i> (Trivial File Transfer Protocol) mode. – SFTP—saves the switch configuration to the remote system through <i>SFTP</i> (SSH File Transfer Protocol) mode. • Address Type—select the IP Address type of the remote system in which the Switch configurations are to be saved. The default option is <i>IPv4</i>. <i>IPv4</i>—Sets the Address type as <i>IPv4</i>. NOTE: This field is configurable only if the Save Option is set as Remote Save. • IP Address—enter the IP Address of the remote system in which the Switch configurations are to be saved. NOTE: This field is configurable only if the Save Option is set as Remote Save. • SFTP User Name—enter the user name required for saving the configurations to the remote system in <i>SFTP</i> mode. This field is a string of maximum size 20. NOTE: This field is configurable only if the Save Option is set as Remote Save and the Transfer Mode is set as <i>SFTP</i>.
Fields (cont)	• SFTP Password—enter the password required for saving the switch configurations on to the remote system in <i>SFTP</i> mode. This field is a string of maximum size 20. The specified <i>SFTP</i> username / password should have been configured in the <i>SFTP</i> server running the remote station, for the remote save operation through <i>SFTP</i> to be successful. NOTE: This field is configurable only if the Save Option is set as Remote Save and the Transfer Mode is set as <i>SFTP</i>. • File Name—Enter the name of the file in which the switch configurations are to be saved. The default file name where the switch configurations are saved is <i>iss.conf</i>. All configurations are saved in a single configuration file only. NOTE: This file name is used for saving the switch configuration, irrespective of the configuration Save Option which can be Flash or Remote Save.

Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs.

Restore Configuration

Figure 18: Restore Configuration

Startup Configuration Restore Source

Restore Option

☐ No Restore
☒ Flash Restore
☐ USB Restore

Restore Format

MiB OID ▾

File Name

iss.conf

Apply

Reset

Notes :

To skip loading existing saved config on startup use "No Restore" option
To enable loading existing locally saved config on startup use "Flash Restore" option
To transfer config file from USB to Raptor device and enable loading newly saved config on startup use "USB Restore" option. (The USB storage may be removed after changes are applied.)

Restoring configuration was successful. Please reboot.

Screen Objective	This screen allows the user to restore the previously saved configurations of the Switch from the Startup Configuration File.
Navigation	System > Save and Restore > Restore

Fields	• Restore option—click one of the option buttons to specify whether the Switch configurations have to be restored. The options are. – No Restore—Specifies that the switch configurations need not be restored when the system is restarted – Flash Restore—Restores the configurations from the Startup Configuration File in the Flash, when the system is restarted. – USB Restore—Restores the configurations on a USB drive, when the system is restarted • Restore Format—select from the 2 available options (<i>MIB OID</i> is the current option): – Script – <i>MIB OID</i> • File Name—enter the configuration file name available in the remote system. The default file name is <i>iss.conf</i>.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs.

Factory Reset

Figure 19: Factory Reset



Screen Objective	This screen allows the user to perform factory reset. The following configuration can be erased: 1) Startup-config 2) <i>NVRAM</i> Settings 3) Flash Files – Users – Privil – Groups – Logs – SSL Certificate
NOTE: Reload device after this command to apply factory default settings.	
Navigation	System > Save and Restore > Reset
Buttons	• Apply—saves the configuration.

2.11. Reboot

This page shows the WebUI to reboot the system.

Figure 20: Rebooting the System

Rebooting the System

Reboot

Screen Objective	This screen allows the user to restart the switch. NOTE: The user should wait for 5 minutes before logging in after reboot. NOTE: All updates to nvram.file using the screen System > NVRAM Settings > Factory Default Settings are effective only after reboot.
Navigation	System > Reboot
Buttons	• Reboot—restarts the switch.

2.12. Syslog Transfer

This screen allows the user configure syslog transfer parameters.

Figure 21: Syslog Transfer

Syslog Transfer

Backup To TFTP ▾

Address Type IPv4 ▾

Server IP Address

SFTP User Name

SFTP Password

Source File Name

Destination File Name

Log transfer not started

Screen Objective	This screen allows the user configure syslog transfer parameters.
Navigation	System > Syslog Transfer
Fields	Backup To—select the transfer mode for uploading log file to the remote system. The default option is <i>TFTP</i>. The list contains: <i>TFTP</i>—uploads the syslog file in <i>TFTP</i> (Trivial File Transfer Protocol) mode. It is used to transfer small amounts of data between hosts on a network. Any transfer begins with a request to read or write a file, which also serves to request a connection. <i>SFTP</i>—uploads the syslog file in <i>SFTP</i> (SSH File Transfer Protocol) mode. It is a network protocol designed to provide secure file transfer and manipulation facilities over <i>SSH</i>. <i>USB</i>—uploads the syslog file in a USB drive. <i>SD card</i>—uploads the syslog file in a SD card. Address Type—select the IP address type. The default option is <i>IPv4</i>. Server IP Address—enter the IP address of the machine to which the syslog file is to be uploaded. SFTP User Name—enter the user name required for uploading syslog file in <i>SFTP</i> mode. This field is a string with size varying from 1 to 20. NOTE: This field is enabled when Transfer Mode is set as <i>SFTP</i>.

Fields (cont)	• SFTP Password—enter the password required for downloading the image from SFTP server. This field is a string with the maximum size 20. NOTE: This field is disabled when Transfer Mode is set as <i>SFTP</i> server. • Source File Name—enter the file name in which the syslogs are saved in the remote system. The default file name is <i>is5</i>. This field is a string of size varying from 1 to 128. • Destination File Name—enter the file name in which the syslogs are saved in the remote system. The default file name is <i>is5</i>. This field is a string of size varying from 1 to 128.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs.

2.13. File Transfer

File Transfer allows the user to upload or download files to or from remote servers.

To access File Transfer screens, go to **System > File Transfer**.

The **File Transfer** link parameters are configured through the screens displayed by the following tabs:

[File Upload](#)

[File Download](#)

[Diagnostic File Transfer](#)

File Upload

By default, the tab **File Upload** displays the **File Upload** screen.

Figure 22: File Upload

File Upload

Transfer Protocol	TFTP ▾
Address Type	IPv4 ▾
Server IP Address	
SFTP User Name	
SFTP Password	
Remote File Name	iss.log
Source File Name	iss.log
	Startup-Config ☐
Apply Reset	

File transfer not started

Screen Objective	This screen allows the user to upload a file from remote server.

Navigation	System > File Transfer > File Upload
Fields	• Transfer Protocol—select the transfer mode for uploading file to the remote system. The default option is <i>TFTP</i>. The list contains: – <i>TFTP</i>—Uploads the file in <i>TFTP</i> (Trivial File Transfer Protocol) mode. – <i>SFTP</i>—Uploads the file in <i>SFTP</i> (SSH File Transfer Protocol) mode. • Address Type—select the IP Address type of the machine from which the file is to be downloaded. The default option is <i>IPv4</i>. • Server IP Address—enter the IP address of the machine from which the file is to be downloaded.
Fields (cont)	• SFTP User Name—enter the user name required for uploading file in <i>SFTP</i> mode. This field is a string with size varying from 1 to 20. NOTE: This field is enabled when Transfer Protocol is set as <i>SFTP</i>. • SFTP Password—enter the password required for uploading file in <i>SFTP</i> mode. This field is a string with the maximum size 20. NOTE: This field is enabled when Transfer Protocol is set as <i>SFTP</i>. • Remote File Name—enter the file name in which the syslogs are saved in the remote system. The default file name is <i>is5com.log</i>. This field is a string of size varying from 1 to 128. • Source File Name—enter the filename or filename with path to which the local file need to be copied in the remote system. • Startup config—select the function Startup configuration. A startup configuration contains configuration information that the iS5com uses at reboot. This command takes a backup of the initial configuration in flash or at a remote location.
Buttons	• Apply—modifies attributes and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs.

File Download

Figure 23: File Download

File Download

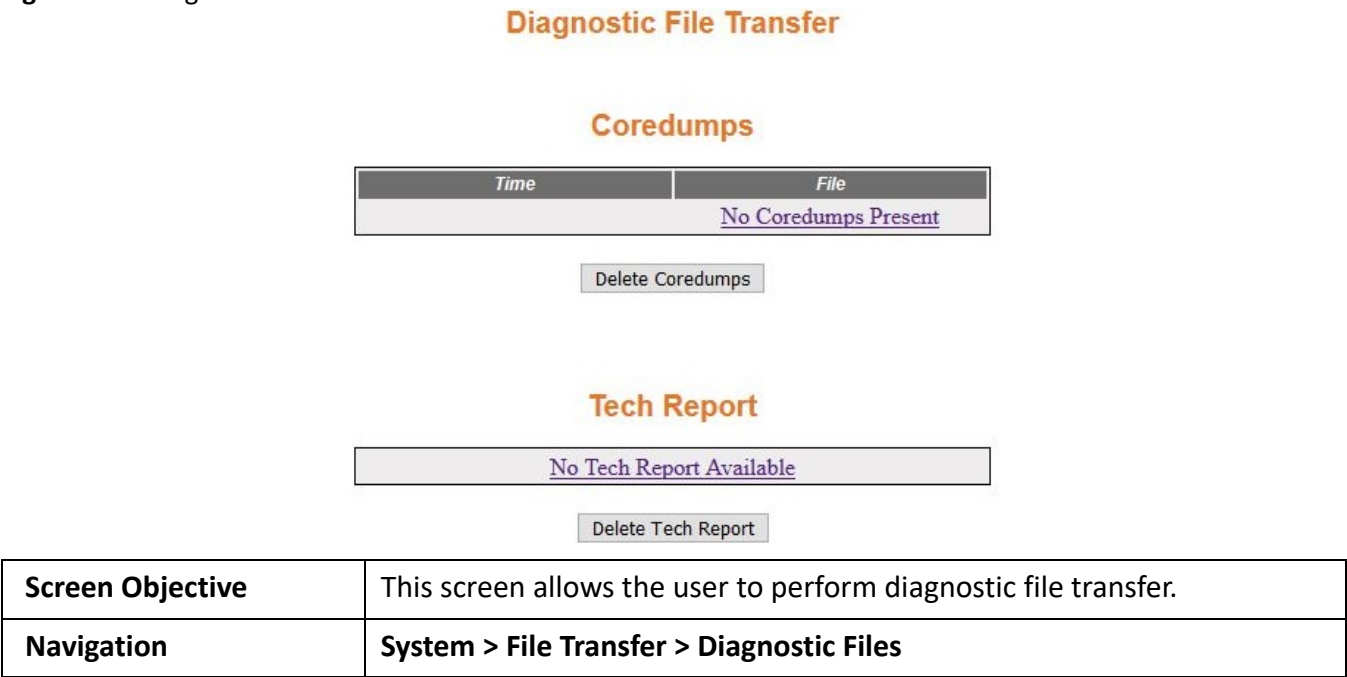
Transfer Protocol	TFTP ▾
Address Type	IPv4 ▾
Server IP Address	
SFTP User Name	
SFTP Password	
File Name	firmware_upgrade.tgz
	Startup-Config ☐
Apply Reset	

File transfer not started

Screen Objective	This screen allows the user to configure the file download details.
Navigation	System > File Transfer > File Download
Fields	• Transfer Protocol—select the transfer mode for downloading file to the remote system. The default option is <i>TFTP</i>. The list contains: – TFTP—Downloads the file in <i>TFTP</i> (Trivial File Transfer Protocol) mode. – SFTP—Downloads the file in <i>SFTP</i> (SSH File Transfer Protocol) mode. • Address Type—select the IP Address type of the machine from which the file is to be downloaded. The default option is <i>IPv4</i>. • Server IP Address—enter the IP address of the machine of the file. • SFTP User Name—enter the user name required for downloading file in <i>SFTP</i> mode. This field is a string with size varying from 1 to 20. NOTE: This field is enabled when Transfer Protocol is set as <i>SFTP</i>. • SFTP Password—enter the password required for downloading file in <i>SFTP</i> mode. This field is a string with the maximum size 20. NOTE: This field is enabled when Transfer Protocol is set as <i>SFTP</i>. • Remote File Name—enter the file name of the file from the remote system. • Startup config—select the function Startup configuration. A startup configuration contains configuration information that the iS5com uses at reboot. This command backs up the initial configuration in a flash or at a remote location.
Buttons	• Apply—modifies attributes and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs.

Diagnostic File Transfer

Figure 24: Diagnostic File Transfer



2.14. Audit Log

This screen allows the user configure audit log parameters.

Figure 25: Audit Log

System Logging Information

Local Logging File-Name

audit.txt

Apply

Local Logging Status

Disable ▾

Apply

Server IP Address

0.0.0.0

Server TCP/UDP port

514

Server TLS port

6514

Protocol

udp ▾

Apply

Remote Logging Status

Disable ▾

Apply

Screen Objective	This screen allows the user configure audit log parameters.
Navigation	System > File Transfer > Audit Log

Fields	- Local Logging Status—enable or disable local logging of audit messages, which can be saved under a default or user defined filename. - Local Logging File-Name—the default filename for the audit log is “audit.txt”. The user can change the name of the audit log file by first disabling the audit logging, changing the name, applying the changes and then enabling the audit log feature. Remote Logging Status—the user may enable remote audit-logging. Please note that remote logging status must be disabled in order to change parameters. Re-enable the logging once the server parameters have been changed and applied. Server IP Address—enter the IP address of the machine to which the syslog file is to be uploaded. Server TCP/ UDP port—the port the remote audit-logging feature will use to transmit logs Server TLS port—the port number for the <i>TLS</i> protocol. Protocol—this is the protocol used for remote logging. <i>UDP/ TCP</i> or <i>TLS</i>.
Buttons	Apply —adds and saves new configuration.

2.15. ACL

Used to control the traffic allowed to pass through ports on the switch.

ACL (Access Control List) specifies rules that allow or block specific traffic through the switch. These rules place certain restrictions on the request types sent from computers to the Internet and vice versa. iS5Com provides support for *ACLs* based on chipsets capability and provides separate configuration parameters for the same.

To access **ACL** screen, go to **System > ACL**.

The *ACL* link allows the user to configure the *ACL* for the switch through the following links:

- [MAC ACL Configuration](#)
- [IP Standard ACL Configuration](#)
- [IP Extended ACL Configuration](#)

MAC ACL Configuration

By default, the tab **ACL** displays the **MAC ACL Configuration** screen.

Figure 26: MAC ACL Configuration—Part A

MAC ACL Configuration

ACL Number(1-65535)

*

Source MAC

Destination MAC

Action

Permit

▼

Priority

*

VLAN ID

-

▼

Port List (Incoming)

Port List (Outgoing)

Encapsulation

Protocol

-

▼

0

Sub-Action

None

▼

Sub-Action-Id

OuterEtherType

SVLAN-ID

SVlan Priority

CVlan Priority

Packet Tag Type

Single-Tag

▼

CFI/DEI

Drop Precedence

Green

▼

Add

Reset

Figure 27: MAC ACL Configuration—Part B

Select	Number	Source MAC	Destination MAC	Action	Priority	VLAN-ID	Port List (Incoming)	Port List (Outgoing)	Encapsulation	Protocol
Protocol Number	SubAction	SubAction-Id(VLAN-ID)	OuterEtherType	SVLAN-ID	SVLAN Priority	CVLAN Priority	Packet Tag Type	CFI-DEI	Drop Precedence	
Apply		Delete								

Screen Objective	This screen allows the user to create a <i>MAC</i> (Media Access Control) <i>ACL</i> and configure its parameters.
Navigation	System > ACL > MAC ACL

Fields	• ACL Number—enter the <i>ACL</i> number which is the unique identifier for the access list. This value ranges from 1 to 65535. • Source MAC—enter the source unicast <i>MAC</i> address for which the access control must be applied. The default value is 0 which implies that any source <i>MAC</i> address can be filtered • Destination MAC—enter the destination unicast <i>MAC</i> address for which the access control must be applied. The default value is 0, which implies that any destination <i>MAC</i> address can be filtered. NOTE: The status of the access list can be Active only if both the source and destination <i>MAC</i> addresses are configured. • Action—select the action to be taken on the packet if the filter rule matches. The default option is Permit. The list contains: – Permit—forwards the packet according to the forwarding rules. – Deny—discards the packet. – Redirect—switches the packet according to the redirect rules. NOTE: If the selected Action is Redirect, the Redirect Interface Group screen needs to be configured. • Priority—enter priority of the L3 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. This value ranges from 1 to 255. The default value is 1. • VLAN ID—select the <i>VLAN</i> ID (Identifier) for which the access control has to be applied. This value ranges from 0 to 4094. The default value is 0, which implies that this object is not used. NOTE: For provider bridge, the <i>VLAN</i> ID is treated as customer <i>VLAN</i> ID. • Port List (Incoming)—enter the incoming port list which is the set of ports for which the ingress filtering is applied. • Port List (Outgoing)—enter the outgoing port list which is the set of ports for which the egress filtering is applied.

Fields (cont).	• Encapsulation—enter the encapsulation type of the packet for which the access control has to be applied. This value ranges from 1 to 65535. • Protocol—select the non-IP Protocol type of the packet for which the access control has to be applied. The default value is 0, which means that the filter is applicable for all protocols. The list contains: – aarp—specifies EtherType AppleTalk Address Resolution Protocol (AARP) that maps a data-link address to a network address. – amber—specifies EtherType DEC-Amberdec-spanning—specifies EtherType Digital Equipment Corporation (DEC) spanning tree – decnet_iv—specifies EtherType DECnet Phase IV protocol – diagnostic—specifies EtherType DEC-Diagnostic – dsm—specifies EtherType DEC-DSM/DDP – etype-6000—specifies EtherType 0x6000 – etype-8042—specifies EtherType 0x8042 – at—specifies EtherType DEC-LAT – lavc-sca—specifies EtherType DEC-LAVC-SCA – mop-consol—specifies EtherType DEC-MOP Remote Console – mop_dump—specifies EtherType DEC-MOP Dump – msdos—specifies EtherType DEC-MSDOS – mumps—specifies EtherType DEC-MUMPS – netbios—specifies EtherType DEC—NETwork Basic Input / Output System (NETBIOS) – vines-echo—specifies EtherType Virtual Integrated NETwork Service (VINES) – vines-ip—specifies EtherType VINES IP – xns-id—specifies EtherType Xerox Network Systems (XNS) protocol suite – other—specifies other protocols. NOTE: The protocol number corresponding to the selected protocol is displayed in the text box next to the protocol. NOTE: The protocol number can be configured only if the Protocol is selected as other. This value ranges from 1 to 65535. • Sub-Action—Id (VLAN-ID)—enter the unique identifier for the VLAN specific sub action to be performed on the packet. This value ranges from 0 to 4094. The default value is 0. NOTE: If the Sub Action is selected as Modify CFIDEI, the Sub Action Id is either 0 or 1. NOTE: If the Sub Action is selected as Modify DP, the Sub Action Id ranges from 0 to 3. NOTE: If the Sub Action is selected as Modify DP, the Sub Action Id ranges from 1 to 7. NOTE: This field cannot be configured if the Action is selected as DenY. NOTE: This field cannot be configured if the Sub Action is selected as None or Strip-Outer Header.

Fields	• OuterEtherType—enter the EtherType value of the outer <i>VLAN</i> tag of a packet. This value ranges from 1 to 65535. The default value is 0, which implies the don't care condition—packet with any EtherType value is considered. • SVLAN-ID—enter the <i>SVLAN-ID</i> present in the outer tag to be filtered. This value ranges from 1 to 4094. The default value is 0. • SVLAN Priority—enter the service <i>VLAN</i> priority present in the outer tag to be filtered. This value ranges from 0 to 7. The default value is 1. • CVlan Priority—enter the customer <i>VLAN</i> priority value present in the outer tag to be filtered. This value ranges from 0 to 7. The default value is 1. • Packet Tag Type—elect the packet tag type for which the access control has to be applied. The list contains Single-Tag and Double-Tag. The default value is Single-Tag. – Single-Tag—applies the configured filter parameters on single <i>VLAN</i> tagged packets – Double-Tag—applies the configured filter parameters on double <i>VLAN</i> tagged packets. • CFI/DEI—enter the <i>CFI/DEI</i> bit value in the c-vlan tag or s-vlan tag of the packet for which the access control has to be applied. This value ranges from 0 to 1. • Drop Precedence/DEI—select the drop precedence level for which the access control has to be applied. The default option is Green. The list contains: – None—sets the drop precedence level as None. – Green—sets the drop precedence level as Green. – Yellow—sets the drop precedence level as Yellow. – Red—sets the drop precedence level as Red.
Buttons	• Apply—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes. • Delete—deletes the selected entry.

IP Standard ACL Configuration

Figure 28: IP Standard ACL Configuration

IP Standard ACL Configuration

ACL Number(1-1000) *

Action Permit ▼

Source IP Address

Subnet Mask

Destination IP Address

Subnet Mask

Port List (Incoming)

Port List (Outgoing)

Priority

Note : If Action selected is Redirect , then navigate to Redirect Interface Group Tab.

ACL Number	Action	Source IP	Subnet Mask	Destination IP	Subnet Mask	Port List (Incoming)	Port List (Outgoing)	Priority

Screen Objective	This screen allows the user to set the IP Standard ACL Configuration. Standard ACLs create filters based on IP address and network mask only (L3 filters only).
Navigation	System > ACL > IP Standard ACL
Fields	ACL Number—enter the standard ACL Number which is the unique identifier for the standard ACL. This value ranges from 1 to 1000. Action—select the action to be taken for the access list. The default option is Permit. The list contains: - Permit—allows the packets when a match has been found - Deny—drops the packets when a match has been found - Redirect—switches the packet according to the redirect rules. NOTE: If Action selected is Deny, SubAction, and SubAction-Id(VLAN-ID) fields cannot be configured. NOTE: If Action selected is Redirect, the Redirect Interface Group screen needs to be configured

Field (cont).	• Source IP Address—enter the IP Address matching the packet's source IP address. • Destination IP Address—enter the destination IP Address to match against the packet's destination IP address. NOTE: The status of the access list can be Active only if both the source and destination MAC addresses are configured. • Subnet Mask—enter the address mask corresponding to the IP Address. • Ports List (Incoming)—enter the incoming port list which is the set of ports over which the filter is to be applied for packets ingress at ports in this list. • Ports List (Outgoing)—enter the out port list which is the set of ports over which the filter is to be applied for packets egress at ports in this list. • Priority—enter priority of the L3 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. This value ranges from 1 to 255. The default value is 1.
Buttons	• Apply—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes. • Delete—deletes the selected entry.

IP Extended ACL Configuration

Figure 29: IP Extended ACL Configuration—Part A

IP Extended ACL Configuration

ACL Number(1001-65535)		*
Action	Permit	▼
Address Type	IPv4	▼ *
Source IP Address		
Subnet Mask		
Destination IP Address		
Subnet Mask		
Port List (Incoming)		
Port List (Outgoing)		
Protocol	ICMP	▼
		1
Message Code	255	
Message Type	255	
Priority		
Dscp		
TOS	None	
Source Port (Min)	0	Source Port (Max) 65535
Destination Port (Min)	0	Destination Port (Max) 65535
Destination Prefix Length		Source Prefix Length
Add Reset		

Note : If Action selected is Redirect , then navigate to Redirect Interface Group Tab.

Note : Range for Both Source and Destination Ports cannot be given.

Figure 30: IP Extended ACL Configuration—Part B

Select	Filter No	Action	Address Type	Source IP	Subnet Mask	Destination IP	Subnet Mask

Figure 31: IP Extended ACL Configuration—Part C

Port List (Incoming)	Port List (Outgoing)	Protocol	Other	Code	Type	Priority	Dscp	TOS	Source Port (Min)	Source Port (Max)	Destination Port (Min)	Destination Port (Max)	Destination Prefix Length	Source Prefix Length

Screen Objective	The screen allows the user to set the IP Extended ACL Configuration. Extended access lists enable specification of filters based on the type of protocol, range of <i>TCP /UDP</i> ports as well as the IP address and network mask (Layer 4 filters).
Navigation	System > ACL > IP Extended ACL
Fields	• ACL Number—enter the <i>ACL</i> Number which is the unique identifier for the Extended access list. This value ranges from 1001 to 65535. • Action—select the action to be taken for the access list. The default option is Permit. The list contains: – Permit—allows the packets when a match has been found – Deny—drops the packets when a match has been found – Redirect—switches the packet according to the redirect rules. NOTE: If Action selected is Redirect, the Redirect Interface Group screen needs to be configured • Address Type Number—select the type of IP address used by the entry. The list contains: – IPV4—sets the IP address type for the <i>ACL</i> as IPv4. • Source IP Address—enter the IP Address matching the packet's source IP address. • Subnet Mask—enter the address mask corresponding to the IP Address. • Destination IP Address—enter the destination IP Address to match against the packet's destination IP address. NOTE: The status of the access list can be Active only if both the source and destination MAC addresses are configured. • Ports List (Incoming)—enter the incoming port list which is the set of ports over which the filter is to be applied for packets ingress at ports in this list. • Ports List (Outgoing)—enter the out port list which is the set of ports over which the filter is to be applied for packets egress at ports in this list.

Field (cont)	Protocol—select the Protocol type to be checked against the packet. The default option is <i>ICMP</i>. The list contains: - ICMP—specifies that the filter is to be applied for Internet Control Message Protocol packets (<i>ICMP</i>). - IP—specifies that the filter is to be applied for Internet Protocol packet. - TCP—specifies that the filter is to be applied for Transmission Control Protocol (<i>TCP</i>) packets. - UDP—specifies that the filter is to be applied for User Datagram Protocol (<i>UDP</i>) packets. - OSPF—specifies that the filter is to be applied for Open Shortest Path First (<i>OSPF</i>) packets - PIM—specifies that the filter is to be applied for Protocol Independent Multicasting (<i>PIM</i>) packets - OTHER—specifies that the filter is to be applied for any other protocol packets <i>The protocol number for the respective protocol can be entered in the text box next to this field. This value ranges from 1 to 255. The default value is 255, which implies that any protocol packet can be filtered</i> NOTE: The protocol value can be configured only if the protocol is selected as other. Message Code—enter the message code to be checked for <i>ICMP</i> Packets. This value ranges from 0 to 255. The default value is 255, which implies that the message code is not checked against the packet. Some of the <i>ICMP</i> message Codes are: - Value ———ICMP code 0 ———Network Unreachable 1 ———Host Unreachable 2 ———Protocol Unreachable 3 ———Port Unreachable 4 ———Fragment Need 5 ———Source Route Fail 6 ———Destination Network Unknown 7 ———Destination Host Unknown 8 ———Source Host Isolated 9 ———Destination Network Administratively Prohibited 10 ———Destination Host Administratively Prohibited 11 ———Network Unreachable <i>TOS</i> 12 ———Host Unreachable <i>TOS</i> 255 ———No ICMP Code NOTE: This field can be configured only if the protocol is selected as <i>ICMP</i>.

Field(cont).	• Priority—enter priority of the L3 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. This value ranges from 1 to 255 (default of 1). • DSCP—enter the <i>DSCP</i> (Differentiated Services Code Point) value to be checked against the packet. This value ranges from 0 to 63. The default value is 1. NOTE: This field cannot be configured if the protocol is selected as <i>ICMP</i> or <i>OTHER</i>. • TOS—select the type of service. The default is None. The list contains: – None—the <i>ACL</i> does not match the <i>TOS</i> field in the packets. – High Reliability—the <i>ACL</i> matches the packets with <i>TOS</i> field as high reliability. – High Throughput—the <i>ACL</i> matches the packets with <i>TOS</i> field as high throughput. – High Reliability and High Throughput—the <i>ACL</i> matches the packets with <i>TOS</i> field as high reliability and High throughput. – Low Delay—the <i>ACL</i> matches the packets with <i>TOS</i> field as Low delay. – Low Delay and High Reliability—the <i>ACL</i> matches the packets with <i>TOS</i> field as Low Delay and High Reliability – Low Delay and High Throughput—the <i>ACL</i> matches the packets with <i>TOS</i> field as Low Delay and High Throughput. – Low Delay, High Throughput and High Reliability—the <i>ACL</i> matches the packets with <i>TOS</i> field as Low Delay, High Throughput, and High Reliability. NOTE: This field cannot be configured if the protocol other than <i>ICMP</i> is selected. • Source Port (Min)—enter the <i>TCP /UDP</i> (User Datagram Protocol) source port from which the access list has to be applied. This value ranges from 0 to 65535. The default value is 0. NOTE: This field can be configured only if the protocol is configured as <i>TCP</i> or <i>UDP</i>. • Source Port (Max)—enter the <i>TCP /UDP</i> source ports to which the access list has to be applied. This value ranges from 0 to 65535. The default value is 65535. NOTE: This field can be configured only if the protocol is configured as <i>TCP</i> or <i>UDP</i>. • Destination Port (Min)—enter the <i>TCP /UDP</i> destination port from which the access list has to be applied. This value ranges from 0 to 65535. The default value is 0. NOTE: This field cannot be configured if the protocol is selected as <i>ICMP</i> or <i>OTHER</i>. • Destination Port (Max)—enter the <i>TCP /UDP</i> destination port from which the access list has to be applied. This value ranges from 0 to 65535. The default value is 0. NOTE: This field cannot be configured if the protocol is selected as <i>ICMP</i> or <i>OTHER</i>. • Destination Prefix Length—enter the length of the <i>CIDR</i> (Classless Inter Domain Routing) prefix carried in the destination IP address. This value ranges from 0 to 32 for <i>IPv4</i> addresses and from 0 to 128 for <i>IPv6</i> addresses. The default value is 0.

Field(cont).	• Source Prefix Length—enter the length of the <i>CIDR</i> prefix carried in the source IP address. This value ranges from 0 to 32 for <i>IPv4</i> addresses and from 0 to 128 for <i>IPv6</i> addresses. The default value is 0.
Buttons	• Apply—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes. • Delete—deletes the selected entry.

2.16. IP Authorized Manager

This screen allows the user to configure the IP Authorized Manager.

Figure 32: IP Authorized Manager

IP Authorized Manager

IP Address *

Subnet Mask *

Port List (Incoming)

VLANs Allowed

Services Allowed ☐ ALL ☐ SNMP ☐ TELNET ☐ HTTP ☐ HTTPS ☐ SSH

IP Address	Subnet Mask	Port List (Incoming)	VLANs Allowed	Services Allowed
Apply Delete				

Figure 14-1: IP Authorized Manager

Screen Objective	This screen allows the user to configure the IP Authorized Manager.
Navigation	System > IP Authorized Manager

Fields	• IP Address—enter the Network or Host address from which the switch can be managed. The maximum length of address is 15. An address 0.0.0.0 indicates Any Manager. • Subnet Mask—enter the subnet mask for the configured IP address. The maximum length of subnet mask is 15. Value 0.0.0.0 indicates mask for Any Manager. NOTE: By default, the authorized manager is allowed to access the switch through all ports. If a set of ports are configured in the Port List, the manager can access the switch only through the configured ports • Port List (Incoming)—enter the subnet mask for the configured IP address. The maximum length of subnet mask is 15. Value 0.0.0.0 indicates mask for Any Manager. NOTE: The configured subnet mask should be in the same subnet of the network in which the switch is placed. • VLANs Allowed—enter the <i>VLANs</i> in which the IP authorized manager can reside NOTE: By default, the manager is allowed to reside in any <i>VLAN</i>. If a set of <i>VLANs</i> are configured in the <i>VLANs Allowed</i> list, the manager can reside only in the configured <i>VLAN</i> set. Access to the switch will be denied from any other <i>VLAN</i>.

Fields (cont)	• Services Allowed—click the allowed services through which the manager can access the switch. The default option is ALL. Options are: – ALL—Supports all services – SNMP— <i>SNMP</i> (Simple Network Management Protocol) is a set of protocols for managing complex networks. <i>SNMP</i> works by sending messages, called protocol data units (<i>PDU</i>)s, to different parts of a network. <i>SNMP</i>-compliant devices or so called agents store data about themselves in Management Information Bases (<i>MIB</i>)s and return this data to the <i>SNMP</i> requesters. – TELNET—Telnet is a user command and an underlying <i>TCP/IP</i> protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. On the Web, <i>HTTP</i> and <i>FTP</i> protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer. With Telnet, the user can log on as a regular user with whatever privileges you may have been granted to the specific application and data on that computer. – HTTP— <i>HTTP</i> (Hyper Text Transfer Protocol) is an underlying protocol used by the World Wide Web. <i>HTTP</i> 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 <i>HTTP</i> command to the Web server directing it to fetch and transmit the requested Web screen. – HTTPS—Another protocol for transmitting data securely over the World Wide Web is Secure <i>HTTP</i> (<i>S-HTTP</i>). <i>S-HTTP</i> is designed to transmit individual messages in a secured manner. – SSH—Secure Shell (<i>SSH</i>) is a program to log 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 <i>rlogin</i>, <i>rsh</i>, <i>rcp</i>, and <i>rdist</i>. <i>SSH</i> protects a network from attacks such as IP spoofing, IP source routing, and <i>DNS</i> spoofing. An attacker who has managed to take over a network can only force <i>ssh</i> to disconnect. He or she cannot play back the traffic or hijack the connection when encryption is enabled.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. The attributes of the default Queue Template cannot be modified. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

2.17. Port Isolation

This screen allows the user to configure the list of allowed forwarding / egress ports, where the ingress packets for particular *VLAN* can be forwarded. This rule is applied for all packets that ingress the given port if the *VLAN* is not configured.

Figure 33: Port Isolation Configuration

Screen Objective	This screen allows the user to configure the list of allowed forwarding / egress ports, where the ingress packets for particular <i>VLAN</i> can be forwarded. This rule is applied for all packets that ingress the given port if the <i>VLAN</i> is not configured.
NOTE: The configuration can be done only for physical and link aggregated ports.	
Navigation	System > Port Isolation
Fields	Ingress Port—select the ingress port that should be mapped with the egress port. This is a combination of interface type and interface ID. The interface ID represents the port channel ID or is a combination of slot number and the port number (slot number/port number). NOTE: This list contains only available physical and link aggregated ports. VLAN ID—enter the <i>VLAN</i> ID that uniquely identifies a specific <i>VLAN</i>. The port isolation rule is applied only for the specified <i>VLAN</i> packets received on the configured ingress ports. This value ranges from 1 to 4094. Egress Ports—enter the egress port or set of egress ports that should be mapped with the ingress port. Use comma as a separator between the ports when configuring a list of ports. The format of this entry is <interface type><slot number/port number>. There is no space needed between these two entries. Example: Gi0/1, Gi0/2. Here, Gi is interface type Gigabit Ethernet Interface, 0 is slot number, and 1 is port number.

Fields (cont)	• Storage—select the storage type for the conceptual row. The default option is Non-Volatile. Options are: – Volatile—reflects the configurations for an interface whose interface index has been assigned, and for which the supporting implementation is currently present. – Non-Volatile—reflects the configuration for an interface whose interface index has been assigned, but for which the supporting implementation is currently not present.
Buttons	• Add—adds and saves new configuration. • Delete—resets to default value for respective fields and discards all user inputs. The attributes of the default Queue Template cannot be modified. • DELETE—deletes the selected entry.

QoS Map

3. QoS

QoS Introduction

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.

3.1. QoS Ingress

Describes the *QoS* Ingress settings.

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.

The *QoS* module provides a complete IP *QoS* 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.

QoS Ingress refers to the quality of service offered to the incoming packets.

To access **QoS Ingress** screens, go to **System > QoS Ingress**.

The *ACL* link allows the user to configure the *ACL* for the switch through the following tabs:

- Basic Settings
- Data Path
- Classifier
- Classifier Element
- Meter
- Token Bucket Meter
- Action
- Priority Map Settings
- Class Map Settings
- Class to Priority Settings
- Policy Map Settings

- Def UserPri Settings

Basic Settings

By default, the tab **Basic Settings** displays the **Basic Settings** screen.

Figure 1: QoS Basic Settings



Screen Objective	This screen allows the user to configure the basic settings of QoS.
Navigation	System > QoS Ingress > Basic Settings

Fields	• System Control—select the control type of the QoS module in the system. The default option is start. The list contains: – start—starts QoS in the system. Resources required by QoS module are allocated and the QoS module starts running. – shutdown—shuts down QoS in the system. All pools used by QoS module are released to the system. • DS Status—select the status of the QoS module in the system. The default option is Enabled. The list contains. – Enabled—enables QoS Module. The QoS module programs the hardware and starts protocol operation. – Disabled—disables QoS Module. This stops protocol operation by deleting the hardware configuration NOTE: DS Status can be enabled only if QoS is started in the system. • DS Rate Unit—displays the unit for the information rate values based on target platform. The default value is Kbps. The rate unit can be any one of the following: – bps—bits per second. – Kbps—Kilobits per second – mbps—megabits per second – gbps—gigabits per second • DS Rate Granularity—displays the acceptable granularity level for configuring the information rate (CIR, EIR, PIR, PTR, and CTR) values for a target platform. The default value is 64.
Buttons	• Apply—modifies attributes and saves the changes.

Data Path

Figure 2: Data Path

Data Path

Interface *
IfDirection *

*
*

Data Path Start *

Index *

Storage

*
*
*
*

☐	Gi0/22	Egress	None	0	Non-Volatile
☐	Gi0/23	Ingress	None	0	Non-Volatile
☐	Gi0/23	Egress	None	0	Non-Volatile
☐	Gi0/24	Ingress	None	0	Non-Volatile
☐	Gi0/24	Egress	None	0	Non-Volatile
☐	Ex0/1	Ingress	None	0	Non-Volatile
☐	Ex0/1	Egress	None	0	Non-Volatile
☐	Ex0/2	Ingress	None	0	Non-Volatile
☐	Ex0/2	Egress	None	0	Non-Volatile
☐	Ex0/3	Ingress	None	0	Non-Volatile
☐	Ex0/3	Egress	None	0	Non-Volatile
☐	Ex0/4	Ingress	None	0	Non-Volatile
☒	Ex0/4	Egress	None	0	Non-Volatile

Screen Objective	This screen allows the user to configure the data path settings. The Data Path table enumerates the differentiated services functional data paths within the device.
NOTE: - This screen can be configured only if QoS is started in the system using the Basic Settings screen. - The entries in the bottom form are displayed only if QoS is started in the system.	
Navigation	System > QoS Ingress > Data Path

Fields	• Interface—select the interface index from the list of interface created in the system. The default option is None. • IfDirection—select the option to specify whether the reception or transmission path for this interface is in view. The default option is Ingress. Options are: – Ingress—sets the interface direction as Ingress. Reception path for this interface is in view. – Egress—sets the interface direction as Egress. Transmission path for this interface is in view. • Data Path Start—select the first differentiated services functional data path element to handle traffic for this data path. The default option is None. Options are: – None—disables the first differentiated services functional data path element to handle traffic. – Classifier—enables the first differentiated services functional data path element to handle traffic. • Index—select the Classifier Index from the list of classifiers configured in the system: NOTE: This field lists the Classifier Index created using the Classifier screen. NOTE: This field can be configured only if Data Path Start is set as Classifier. • Storage—Select the storage type for this conceptual row. The default option is Non-Volatile. Options are: – Volatile—reflects the configurations for an interface whose interface index has been assigned, and for which the supporting implementation is currently present. – Non-Volatile—reflects the configuration for an interface whose interface index has been assigned but for which the supporting implementation is currently not present.
Buttons	• Add—adds and saves new configuration. • Modify—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs. • Delete—deletes the selected entry.

Classifier

Figure 3: Classifier

Screen Objective	This screen allows the user to configure the classifier settings. Packet classifiers select packets in a traffic stream based on the content of some portion of the packet header. Classifiers are used to steer packets matching some specified rule to an element of a traffic conditioner for further processing.
NOTE: This screen can be configured only if QoS is started in the system using the Basic Settings screen.	
Navigation	System > QoS Ingress > Classifier
Fields	Classifier Id—enter the index that enumerates the classifier entries. This value ranges from 1 to 65535. Next Free Index—displays an integer which may be used as a new index in the table. The value of zero indicates that no more new entries can be created in the relevant table. This is a read only field. Storage—select the storage type for the conceptual row. The default option is Volatile. Options are: - Volatile—reflects the configurations for an interface whose interface index has been assigned, and for which the supporting implementation is currently present. - Non-Volatile—reflects the configuration for an interface whose interface index has been assigned but for which the supporting implementation is currently not present
Buttons	Add—adds and saves new configuration Modify—modifies attributes and saves the changes Reset—resets to default value for respective fields and discards all user inputs Delete—deletes the selected entry.

Classifier Element

Figure 4: Classifier Element

Classifier Element

Classifier Id: * Next Free Id:

Classifier Element Id: *

Classifier Element Next: * Index:

Classifier Element Specific: * Index: *

Storage:

Select	Classifier Id	Classifier Element Id	Classifier Element Next	Index	Classifier Element Specific	Index	Storage
☒	0	1	Meter	1		0	
☐	0	2	Meter	1		0	
☐	0	3	Meter	1		0	
☐	0	4	Meter	1		0	
☐	0	5	Meter	1		0	
☐	0	6	Meter	1		0	
☐	0	7	Meter	1		0	
☐	0	8	Meter	1		0	

Screen Objective	This screen allows the user to configure the Classifier Element settings. All traffic presented to a classifier must match at least one classifier element within the classifier, with the classifier element parameters specified by a filter. The classifier element table enumerates the relationship between classification patterns and subsequent downstream Differentiated Services Functional Data Path elements.
NOTE:	This screen can be configured only if QoS is started in the system using the Basic Settings screen.
Navigation	System > QoS Ingress > Classifier Element
Fields	Classifier Id—select the index that enumerates the classifier entries. NOTE: This field lists the Classifier Index created using the Classifier screen. Next Free Id—displays an integer which may be used as a new index in the table. The value of zero indicates that no more new entries can be created in the relevant table. This is a read only field. Classifier Element Id—enter the index that enumerates the classifier element entries. This value ranges from 1 to 65535. NOTE: By default, the classifier elements with the IDs 1 to 8 are already created in the system and cannot be deleted.

Fields (cont)	• Classifier Element Next—select the next differentiated services functional data path element to handle traffic for this data path. Options are: – None—disables next differentiated services functional data path element to handle traffic for this data path. – Meter—enables meter settings for the next differentiated services functional data path element to handle traffic for this data path. – Queue—enables queue settings for the next differentiated services functional data path element to handle traffic for this data path. • Index—select the available entries of corresponding functional blocks displayed by Classifier Element Next. NOTE: This field can be configured only if the Classifier Element Next is selected as Meter or Queue. • Classifier Element Specific—select a pointer to a valid entry in another table, filter table, which describes the applicable classification parameters. Options are: – None—disables mapping of an access control list (ACL) entry or a priority-map to a CLASS of Service. – Multi-Field Classifier—enables mapping of an access control list (ACL) entry or a priority-map to a CLASS of Service. • Index—select the available entries of corresponding functional blocks displayed by Multi-Field Classifier. NOTE: This field can be configured only if the Classifier Element Specific is selected as Multi-Field Classifier. • Storage—select the storage type for the conceptual row. The default option is Volatile. Options are: – Volatile—reflects the configurations for an interface whose interface index has been assigned, and for which the supporting implementation is currently present. – Non-Volatile—reflects the configuration for an interface whose interface index has been assigned but for which the supporting implementation is currently not present.
Buttons	• Add—adds and saves new configuration. • Modify—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs. • Delete—deletes the selected entry.

Meter

Figure 5: Meter

Meter

Meter Id * Next Free Id

Meter Succeed Next * Index

Meter Fail Next * Index

Meter Specific * Index

Storage

Select	Meter Id	Meter Succeed Next	Index	Meter Fail Next	Index	Meter Specific	Index	Storage
☒	1	None	0	None	0	None	0	Volatile

Screen Objective	This screen allows the user to configure the meter settings. Meters are used to police a stream of traffic. The traffic stream to be metered is determined by the Differentiated Services Functional Data Path Element(s) upstream of the meter.

NOTE:

- This screen can be configured only if QoS is started in the system using the **Basic Settings** screen.

Navigation	System > QoS Ingress > Meter

Fields	Meter Id—select the index that enumerates the meter entries. This value ranges from 1 to 65535. NOTE: The default meter with the Id of 1 is already created in the system and cannot be deleted. Next Free Id—displays an integer which may be used as a new index in the table. The value of zero indicates that no more new entries can be created in the relevant table. This is a read only field. Meter Succeed Next—select the Meter Id to be used for applying the second / next level of conformance on the incoming packet. The default option is None. Options are: - None—disables the next differentiated services functional data path element to handle traffic for this data path if the traffic conforms. - Action—enables the next differentiated services functional data path element to handle traffic for this data path if the traffic conforms.

Fields (cont)	• Index—displays the available entries of corresponding functional blocks displayed by Meter Succeed Next. NOTE: This field can be configured only if the selected option of Meter Succeed Next is Action. • Meter Fail Next—select a pointer to a valid entry in another table, filter table, which describes the applicable classification parameters. Options are: – None—disables the next differentiated services functional data path element to handle traffic for this data path if the traffic conforms. – Action—enables the next differentiated services functional data path element to handle traffic for this data path if the traffic conforms. • Index—displays the available entries of corresponding functional blocks displayed by Meter Fail Next. NOTE: This field can be configured only if the Meter Fail Next is selected as Action. • Meter Specific—Select the behavior of the meter pointing to an entry containing detailed parameters. The default option is None. Options are: – None—does not indicate the behavior of the meter by pointing to an entry containing detailed parameters. – TB Param—indicates the behavior of the meter by pointing to an entry containing Token Bucket parameter (<i>TB Param</i>). • Index—displays the available entries of corresponding functional blocks displayed by Meter Specific. NOTE: This field can be configured only if the Meter Specific is selected as <i>TB Param</i>. • Storage—select the storage type for the conceptual row. The default option is Volatile. Options are: – Volatile—reflects the configurations for an interface whose interface index has been assigned, and for which the supporting implementation is currently present. – Non-Volatile—reflects the configuration for an interface whose interface index has been assigned but for which the supporting implementation is currently not present.
Buttons	• Add—adds and saves new configuration • Modify—modifies attributes and saves the changes • Reset—resets to default value for respective fields and discards all user inputs • Delete—deletes the selected entry.

Token Bucket Meter

Figure 6: Token Bucket Meter

Token Bucket Meter

Meter Id		*	Next Free Id	1
MeterType	None	*		
MeterInterval(in Microseconds)				
Color Mode	ColorBlind			
CIR		*		
CBS				
EIR				
EBS				
NextMeterId	0			
Storage	Volatile			

Select	MeterId	MeterType	MeterInterval	ColorMode	CIR	CBS	EIR	EBS	NextMeterId	Storage Type

Screen Objective	This screen allows the user to configure the token bucket parameters. Each entry in the Token Bucket (<i>TB</i>) Parameter Table is used to configure a single token bucket. Multiple token buckets can be used together to parameterize multiple levels of conformance.
NOTE: This screen can be configured only if <i>QoS</i> is started in the system using the Basic Settings screen.	
Navigation	System > QoS Ingress > TB Meter
Fields	Meter Id—select the index that enumerates the <i>TB</i> meter entries. This value ranges from 1 to 65535. Next Free Id—displays an integer which may be used as a new index in the table. The value of zero indicates that no more new entries can be created in the relevant table. This is a read only field.

Fields (cont)	Meter Type—select the metering algorithm associated with the token bucket parameters. Options are: - None—does not sets any metering algorithm associated with the token bucket parameters. - simpleTokenBucket—sets the meter type as Two Parameter Token Bucket Meter. NOTE: When this option is selected, MeterInterval, <i>EIR</i>, and <i>EBS</i> are greyed out. - avgRate—sets the meter type as Average Rate Meter. It supports interval and committed information rate (<i>CIR</i>) parameters. NOTE: When this option is selected, <i>CBS</i>, <i>EIR</i>, and <i>EBS</i> are greyed out. - srTCM—sets the meter type as Single Rate Three Color Marker Metering as defined by RFC 2697. It supports <i>CIR</i>, committed burst size (<i>CBS</i>) and excess burst size (<i>EBS</i>) parameters. NOTE: When this option is selected, MeterInterval and <i>EIR</i> are greyed out. - trTCM—sets the meter type as Two Rate Three Color Marker Metering as defined by RFC 2698. It supports <i>CIR</i>, <i>CBS</i>, excess information rate (<i>EIR</i>), and excess burst size (<i>EBS</i>) parameters. NOTE: When this option is selected, MeterInterval is greyed out. - tswTCM—sets the meter type as Time Sliding Window Three Color Marker Metering as defined by RFC 2859. NOTE: When this option is selected, <i>CBS</i> and <i>EBS</i> are greyed out. - mefDecoupleMeter—sets the meter type as Dual bucket meter as defined by RFC 4115. NOTE: When this option is selected, MeterInterval is greyed out. - mefCoupledMeter—sets the meter type as Dual bucket meter as defined by RFC 2697 and MEF coupling Flag. NOTE: When this option is selected, MeterInterval and <i>EIR</i> are greyed out. MeterInterval(in Microseconds)—enter the time interval used with the token bucket. This value ranges from 1 to 10000 microseconds. NOTE: Meter Interval is mandatory if the Meter Type is set as avgRate and tswTCM. This field is greyed out for all other meter types. Color Mode—select the color mode of the meter. The default option is ColorBlind. Options are: - ColorBlind—sets the meter to ignore the pre-color of the packet. - ColorAware—sets the meter to consider the pre-color of the packet.

- **CIR**—enter the Committed Information Rate (*CIR*). It defines the average rate in bits/s of Service Frames up to which the network delivers Service Frames and is committed to meeting the performance objectives defined by the CoS Service Attribute. This value ranges from 0 to 65535. The default value is 0.
NOTE: CIR must be less than or equal to EIR if EIR is greater than 0.
NOTE: This configuration is applicable for all meter type.
- **CBS**—enter the committed burst size (*CBS*). This value ranges from 0 to 65535. The default value is 0.
NOTE: CBS must be greater than 0 if *CIR* is greater than 0.
NOTE: This configuration is not applicable if meter type is avgRate and tswTCM.
- **EIR**—enter the excess information rate (*EIR*). This value ranges from 0 to 65535. The default value is 0.
NOTE: EIR must be greater than or equal to CIR if EIR is greater than 0.
NOTE: This configuration is not applicable if meter type is simpleTokenBucket, avgRate, srTCM, and mefCoupledMeter.
- **EBS**—enter the excess burst size (*EBS*). This value ranges from 0 to 65535. The default value is 0.
NOTE: EBS must be greater than 0 if EIR is greater than 0.
NOTE: This configuration is not applicable if meter type is simpleTokenBucket, avgRate, and tswTCM.
- **NextMeterId**—select the meter entry ID to be used for applying the second/next level of conformance on the incoming packet. The default value is 0.
- **Storage**—select the storage type for the conceptual row. The default option is Volatile. Options are:
 - Volatile—reflects the configurations for an interface whose interface index has been assigned, and for which the supporting implementation is currently present.
 - Non-Volatile—reflects the configuration for an interface whose interface index has been assigned but for which the supporting implementation is currently not present.

Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. NOTE: The attributes cannot be modified for the meter id which is set as a Next Meter ID by another entry. • Delete—deletes the selected entry. NOTE: The meter Id which is set as the Next Meter Id by another entry cannot be deleted. To delete this Meter ID, the Meter ID which uses this ID as its Next Meter ID should be deleted first. NOTE: For example, if the Meter ID 2 is set as the Next Meter ID for the Meter ID 6, the Meter ID 6 should be deleted first, and then only Meter ID 2 can be deleted.

Action

Figure 7: Action

Screen Objective	This screen allows the user to configure the action settings. The Action table allows enumeration of the different types of actions to be applied to a traffic flow.
NOTE: • This screen can be configured only if QoS is started in the system using the Basic Settings screen.	
Navigation	System > QoS Ingress > Action
Fields	• Action Id—enter the index that enumerates the action entries. This value ranges from 1 to 65535. • Next Free Id—displays an integer which may be used as a new index in the table. The value of zero indicates that no more new entries can be created in the relevant table. This is a read only field.

Fields (cont)	• Interface—specifies the interface index where action occurs. • Action Next—select the next differentiated services functional data path element to handle traffic for this data path. Options are: – None—disables the action to be performed. – AlgoDrop—enables the algorithm drop action. – Queue—enables queue setting action. • Index—specifies the available entries of corresponding functional blocks displayed by Action Next. • Action Specific—select the pointer to an object instance providing additional information for the type of action indicated by this action table entry. Options are: – None—disables the pointer to an object instance providing additional information. – Dscp Mark Act Entry—enables the pointer to an object instance providing description for action table entry. – Count Act Entry—enables the pointer to an object instance providing count for action table entry. – AlgoDrop—enables Drop Algorithm for Congestion Management. • Index—specifies the available entries of corresponding functional blocks displayed by Action Specific. • Storage—select the storage type for the conceptual row. The default option is Volatile. Options are: – Volatile—reflects the configurations for an interface whose interface index has been assigned, and for which the supporting implementation is currently present. – Non-Volatile—reflects the configuration for an interface whose interface index has been assigned but for which the supporting implementation is currently not present.
Buttons	• Add—adds and saves new configuration. • Modify—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs. • Delete—deletes the selected entry.

Priority Map Settings

Figure 8: Priority Map Settings

Prioritymap Settings

PriorityMap Id

Ingress Interface none ▾

VLAN Id

In Priority

PriType VlanPri ▾

Regen Priority

Regen Inner Priority

Select	PriorityMap Id	Ingress Interface	Vlan Id	In priority	Pri Type	Regen Priority	RegenInner
☐	1	none ▾	0	0	VlanPri ▾	0	None
☐	2	none ▾	0	1	VlanPri ▾	1	None
☐	3	none ▾	0	2	VlanPri ▾	2	None
☐	4	none ▾	0	3	VlanPri ▾	3	None
☐	5	none ▾	0	4	VlanPri ▾	4	None
☐	6	none ▾	0	5	VlanPri ▾	5	None
☐	7	none ▾	0	6	VlanPri ▾	6	None
☒	8	none ▾	0	7	VlanPri ▾	7	None

Screen Objective	This screen allows the user to configure the Priority Map settings. The Priority Map table is used to map incoming priority to a regenerated priority. This table is used to regenerate port / VLAN priorities for an incoming packet. It can be used to directly program priority tables in the hardware.
NOTE: This screen can be configured only if QoS is started in the system using the Basic Settings screen.	
Navigation	System > QoS Ingress > Priority Map
Fields	PriorityMap Id—enter a unique ID for priority map. This represents the output priority map index for the incoming packet received over ingress PORT/ VLAN with specified incoming priority. This value ranges from 1 to 65535. NOTE: The default priority maps with the IDs 1 to 8 are already created in the system and cannot be deleted.

Fields (cont)	• Ingress Interface—select the incoming port number from the list of interfaces created in the system. • VLAN ID—enter the <i>VLAN</i> identifier for priority regeneration. The default value is 0. This value ranges from 1 to 4094. • In Priority—enter the incoming priority value determined for the received frame. This value is equivalent to the priority (<i>VLAN</i> (4 bit)/<i>DSCP</i> (6 bit) priority bits) indicated in the received frame or one of the evaluated priorities. This value ranges from 0 to 63. The default value is 0. • PriType—select the incoming priority type used to identify the incoming priority. The default option is <i>VlanPri</i>. Options are: – <i>VlanPri</i>—sets the incoming priority type as <i>VLAN</i>. – <i>IpTos</i>—sets the incoming priority type as IP Type of Service. – <i>IpDscp</i>—sets the incoming priority type as IP Differentiated Services Code Point. – <i>MplsExp</i>—sets the incoming priority type as <i>MPLS</i> Experimental. • Regen Priority—enter the regenerated priority value determined for the received frame. This value ranges from 0 to 63. The default value is 0. • Regen Inner Priority—enter the regenerated inner-vlan (<i>CVLAN</i>) priority value determined for the received frame. This value ranges from 0 to 8.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. NOTE: The attributes of auto generated default Priority Maps (1–8) cannot be modified. • Delete—deletes the selected entry. NOTE: Auto generated default Class Maps (1–8) cannot be deleted

Class Map Settings

Figure 9: ClassMap Settings

ClassMap Settings

Class Map ID

FilterType

MacFilter Id

IpFilter Id

Priority Id

Traffic Class

PreColor

Select	Classmap ID	Filter type	MacFilter Id	IpFilter Id	PriorityMap Id	Traffic Class	PreColour
☐	1	Priority Type	0	0	1	1	None
☐	2	Priority Type	0	0	2	1	None
☐	3	Priority Type	0	0	3	1	None
☐	4	Priority Type	0	0	4	1	None
☐	5	Priority Type	0	0	5	1	None
☐	6	Priority Type	0	0	6	1	None
☐	7	Priority Type	0	0	7	1	None
☒	8	Priority Type	0	0	8	1	None

Screen Objective	This screen allows the user to classify the stream of traffic. The class map table takes input from the <i>ACL</i> or priority-map table and outputs a Class for the traffic-class pattern/match.
NOTE: This screen can be configured only if QoS is started in the system using the Basic Settings screen.	
Navigation	System > QoS Ingress > Class Map
Fields	Class Map Id—enter a unique ID for every classmap. This value ranges from 1 to 65535. NOTE: The auto generated default class with the IDs 1 to 8 are already created in the system and cannot be deleted. FilterType—select the filter type associated with every classmap. The default option is Priority Type. Options are: - Priority Type—set the filter type associated with the Classmap as priority type. - MAC or IP type—set the filter type associated with the Classmap as MAC or IP type.

Fields (cont)	• MacFilter Id—enter the <i>MAC</i> filter ID (L2 Filter Id) associated with this classmap. This value ranges from 0 to 65535. The default value is 0. NOTE: This field can be configured only if Filter Type is set as <i>MAC</i> or <i>IP</i> Type. • IpFilter Id—enter the <i>IP</i> filter ID (L3 Filter Id) associated with this classmap. This value ranges from 0 to 65535. The default value is 0. NOTE: This field can be configured only if Filter Type is set as <i>MAC</i> or <i>IP</i> Type. • Priority Id—select the Priority Map ID for mapping incoming priority against the received packets. The default value is 0. NOTE: This field lists the priority map ids created using the Priority Map Settings screen. NOTE: Priority ID can be associated with the classmap only if Filter Type is set as <i>Priority</i> Type. • Traffic Class—enter the traffic class associated with the classmap. This value ranges from 0 to 65535. The default value is 0. • PreColor—select the color of the packet prior to metering. The default Drop-precedence for the packet can be evaluated using the color assigned to the packet. The default option is <i>None</i>. Options are: – <i>None</i>—sets the color of the packets to <i>None</i>. This implies that traffic is not pre-colored. – <i>Green</i>—sets the color of the packets to <i>None</i>. This implies that traffic conforms to service-level agreements (<i>SLA</i>)s. – <i>Yellow</i>—sets the color of the packets to <i>None</i>. This implies that traffic exceeds the <i>SLAs</i>. – <i>Red</i>—sets the color of the packets to <i>None</i>. This implies that traffic violates the <i>SLAs</i>.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry. NOTE: Auto generated default Class Maps (1–8) cannot be deleted.

Class to Priority Settings

Figure 10: ClasstoPri Settings

ClasstoPri Settings

Class: 1 ▼

RegenPri:

GroupName:

Add Reset

Select	PriorityClass	RegenPri	GroupName

Apply Delete

Screen Objective	This screen allows the user to configure the class to priority settings. The ClassToPriority table assigns local priority values for an input Class. This table provides easy mapping of Class to priority values.
NOTE: This screen can be configured only if QoS is started in the system using the Basic Settings screen.	
Navigation	System > QoS Ingress > Class to Priority Map
Fields	Class—select the traffic class to which an incoming frame pattern is classified. This value ranges from 1 to 2147483647. NOTE: This field lists the traffic class IDs created using the ClassMap Settings screen. RegenPri—enter the regenerated priority value determined for the input class. This value ranges from 0 to 7. GroupName—enter the unique identification of the group to which an input class belongs. This value is a string of size from 1 to 31.
Buttons	Add—adds and saves new configuration. Reset—resets to default value for respective fields and discards all user inputs. Apply—modifies attributes and saves the changes. Delete—deletes the selected entry.

Policy Map Settings

Figure 11: PolicyMap Settings

PolicyMap Settings

Policy Map ID

Ingress Interface

Traffic Class

PHB Type

DefaultPHB Value

Meter Id

Conform Act

ConAct Value1

ConAct Value2

ConAct NEWCLASS

Exceed Action

ExcAct Value 1

ExcAct Value 2

ExcAct NEWCLASS

Violate Act

VioAct Value1

VioAct Value2

VioAct NEWCLASS

Select	PolicyMap Id	Ingress Interface	Traffic class Id	PHB Type	DefaultPHBValue	MeterId	ConAct	ConActVal1	ConActVal2
☒	1	None	1	None	0		None	0	0

ConNewClass	ExcAct	ExcActVal1	ExcActVal2	ExcNewClass	VioAct	VioActVal1	VioActVal2	VioNewClass
0	None	0	0	0	None	0	0	0

Screen Objective	This screen allows the user to configure action for a specified Class Map. This allows the user to map a policy for a classmap.
NOTE: This screen can be configured only if QoS is started in the system using the Basic Settings screen.	
Navigation	System > QoS Ingress > Policy Map
Fields	Policy Map ID—enter the unique ID for policy map. This value ranges from 1 to 65535. NOTE: The auto generated default policy map with the Id of 1 cannot be deleted.

Fields (cont)	• Ingress Interface—select the incoming port number from the list of ports available in the system. • Traffic Class—Select the traffic class for which the policy map needs to be applied. NOTE: This field lists the Traffic class IDs created using the Class Map Settings screen. • PHB Type—select the <i>PHB</i> (Per Hop Behavior) type to be used for filling the default PHB for the policy map entry. Options are: – None—disables the <i>PHB</i> type for the policy map entry. – VlanPri—enables <i>VLAN</i> priority type for the policy map entry. – ipTos—enables IP Type of Service type for the policy map entry. – ipDscp—enables as IP <i>DSCP</i> for the policy map entry. – mplsExp—enables <i>MPLS</i> Experimental for the policy map entry. • DefaultPHB Value—enter the default outgoing <i>PHB</i> values for the policy map. This value ranges from 0 to 63. • Meter Id—select a meter table ID which is the index for the meter table from the list of meters configured in the system. The default value is 0: • Conform Act—enter the default outgoing <i>PHB</i> values for the policy map. This value ranges from 0 to 63. – None—disables action to be performed on the packet – ActionIPsetPort—sets the new port value. – ConformActionIPTos—sets the new IP <i>TOS</i> value. – ConformActionDSCP—sets the new <i>DSCP</i> value. – ConformActionVlanPriandDE—sets the <i>VLAN</i> priority and <i>VLAN</i> Drop Eligible indicator of the outgoing packet. – ConformActionInnerVlanPri—sets the Inner <i>VLAN</i> priority of the outgoing packet. – ConformActionMplsEXP—sets the <i>MPLS</i> Experimental bits of the outgoing packet. • ConAct Value 1—enter the conform action value for either VlanPri or VlanDe. The value ranges from 0 to 7. The default value is 0. NOTE: This field is greyed out and cannot be configured if the Conform Act is set as None. • ConAct Value 2—enter the conform action value for either VlanPri or VlanDe. The value ranges from 0 to 7. The default value is 0. NOTE: This field is greyed out and cannot be configured if the Conform Act is set as None, ActionIPsetPort, ConformActionIPTos and ConformActionClanPriandDE.

Fields (cont)	• ConAct NEWCLASS1—enter the traffic class to which an incoming frame pattern is classified after metering. The priority of the New CLASS should be lower as compared to the CLASS assigned prior to metering. The value ranges from 0 to 65535. The default value is 0. NOTE: This field is greyed out and cannot be configured if the Conform Act is set as None. • Exceed Action—select the action to be performed on the packet, when the packets are found to be in profile. The default option is None. Options are: – None— disables actions to be performed on the packet – Drop—drops the packet. – ExceedActionIPTos—sets the new IP <i>TOS</i> value. – ExceedActionDSCP—sets the new <i>DSCP</i> value. – ExceedActionVlanPriandDE—sets the <i>VLAN</i> priority and <i>VLAN</i> Drop Eligible indicator of the outgoing packet. – ExceedActionInnerVlanPri—sets the Inner <i>VLAN</i> priority of the outgoing packet. – ExceedActionMplsEXP—sets the <i>MPLS</i> Experimental bits of the outgoing packet. • ExcAct Value 1—specifies the exceed action value for either VlanPri or VlanDe. This value ranges from 0 to 7. The default value is 0. NOTE: This field is greyed out and cannot be configured if the Exceed Action is set as None or Drop. • ExcAct Value 2—specifies the exceed action value for either VlanPri or VlanDe. This value ranges from 0 to 7. The default value is 0. NOTE: This field is greyed out and cannot be configured if the Exceed Action is set as None, Drop, ExceedActionIpTos, or ExceedActionDSCP. • ConAct NEWCLASS1—enter the traffic class to which an incoming frame pattern is classified after metering. The priority of the New CLASS should be lower as compared to the CLASS assigned prior to metering. The value ranges from 0 to 65535. The default value is 0. NOTE: This field is greyed out and cannot be configured if the Exceed Action is set as None or Drop.

Fields (cont)	Violate Act—specifies the exceed action value for either VlanPri or VlanDe. This value ranges from 0 to 7. The default value is 0. - None—disables action to be performed on the packet - Drop—drops the packet. - ViolateActionIPTos—sets the new IP <i>TOS</i> value. - ViolateActionDSCP—sets the new <i>DSCP</i> value. - ViolateActionVlanPriandDE—Sets the <i>VLAN</i> priority and <i>VLAN</i> Drop Eligible indicator of the outgoing packet. - ViolateActionInnerVlanPri—sets the Inner <i>VLAN</i> priority of the outgoing packet. - ViolateActionMplsEXP—sets the <i>MPLS</i> Experimental bits of the outgoing packet Violate Value1—specifies the violate action value for either VlanPri or VlanDe. The value ranges from 0 to 7. The default value is 0. The default value is 0. NOTE: This field is greyed out and cannot be configured if the Violate Act is set as None or Drop. Violate Value2—specifies the violate action value for either VlanPri or VlanDe. The value ranges from 0 to 7. The default value is 0. The default value is 0. NOTE: This field is greyed out and cannot be configured if the Exceed Action is set as None, Drop, ExceedActionIpTos, or ExceedActionDSCP. VioActNEWCLASS —represents the traffic class to which an incoming frame pattern is classified after metering. The priority of the New CLASS should be lower as compared to the CLASS assigned prior to metering. The value ranges from 0 to 65535. The default value is 0. NOTE: This field is greyed out and cannot be configured if the Violate Act is set as None or Drop.
Buttons	Add—adds and saves new configuration. Reset—resets to default value for respective fields and discards all user inputs. Apply—modifies attributes and saves the changes. Delete—deletes the selected entry. NOTE: This field is greyed out and cannot be configured if the Violate Act is set as None or Drop.

Def UserPri Settings

Figure 12: Def UserPri Settings

Def UserPri Settings

Select	Port	Def UserPri
☐	Gi0/1	0
☐	Gi0/2	0
☐	Gi0/3	0
☐	Gi0/4	0
☐	Gi0/5	0
☐	Gi0/6	0
☐	Gi0/7	0
☐	Gi0/8	0
☐	Gi0/9	0
☐	Gi0/10	0
☐	Gi0/11	0
☐	Gi0/12	0
☐	Gi0/13	0
☐	Gi0/14	0
☐	Gi0/15	0
☐	Gi0/16	0
☐	Gi0/17	0
☐	Gi0/18	0
☐	Gi0/19	0
☐	Gi0/20	0
☐	Gi0/21	0
☐	Gi0/22	0
☐	Gi0/23	0
☐	Gi0/24	0
☐	Ex0/1	0
☐	Ex0/2	0
☐	Ex0/3	0
☒	Ex0/4	0

Apply

Screen Objective	This screen allows the user to configure the default user priority settings. The default user priority is used to assign ports to the untagged packets and to specify preference for p-bit over <i>DSCP</i> in tagged packets.
NOTE: - This screen can be configured only if <i>QoS</i> is started in the system using the Basic Settings screen. - The entries are displayed only if <i>QoS</i> is started in the system.	
Navigation	System > QoS Ingress > Def UserPri
Fields	Port—specifies the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number) Def UserPri—enter the default ingress user priority for the specified port. The default value is 0. This value ranges from 0 to 7.
Buttons	Apply—modifies attributes and saves the changes.

3.2. QoS Egress

Describes the *QoS* Egress settings.

QoS Egress refers to the quality of service offered to the outgoing packets.

To access **QoS Egress** screens, go to **System > QoS Egress**.

The **QoS Egress** link, allows the user to configure the *QoS* (Quality of Service) offered to outgoing packets through the screens displayed by the following tabs:

[Queue Template Settings](#)

[Red Conf Settings](#)

[Scheduler Table Settings](#)

[Queue Table Settings](#)

[Min Rate](#)

[Max Rate](#)

[Queue Map Settings](#)

[Scheduler](#)

[Queue](#)

Queue Template Settings

By default, the tab **QoS Egress** displays the **Queue Template Settings** screen.

Figure 13: Queue Template Settings

Queue Template Settings

QueueTemplateId: Next Free Id:

Drop Type:

Drop Algo Enable Flag:

Queue Template Size:

Drop Next: Index:

QMeasure: Index:

Drop Specific: Index:

Storage:

Select	QueueTemplateId	DropType	DropFlag	QueueSize	Drop Next	Index	QMeasure	Index	Drop Specific	Index	Storage
☒	1	TailDrop	Disable	10000		0		0		0	Non-Volatile

Screen Objective

This screen allows the user to configure the queue template settings. The QueueTemplate table is a template for specifying the queue parameters and the policing algorithm parameters applied on the queue. The template is re-used for configuring multiple queues.

NOTE:

- This screen can be configured only if QoS is started in the system using the **Basic Settings** screen.

Navigation

System > QoS Egress > QueueTemplate

Fields	• QueueTemplate Id—enter the index that enumerates the queue entries. This value ranges from 1 to 65535. NOTE: The default Queue Template with an Id of 1 is already created in the system and cannot be deleted. • Next Free Id—specifies an integer which may be used as a new index in the table. The value of zero indicates that no more new entries can be created in the relevant table. This is a read only field. • Drop Type—select the type of drop algorithm used by this queue template. The default option is TailDrop. Options are: – Other—sets the drop algorithm type as other. – TailDrop—sets the drop type as Tail Drop. In this algorithm the Queue Template size represents the maximum depth of the queue, beyond which all newly arriving packets are dropped. – HeadDrop—sets the drop type as Head Drop. This algorithm drops the packets currently at the head of the queue to make room for the new packet to be enqueued at the tail of the queue if a packet arrives, when the current depth of the queue is at queue template size. – RED—sets the drop type as RED. This executes an active queue management algorithm which may randomly drop a packet on packet arrival. This algorithm may be proprietary, and it may drop either the arriving packet or another packet in the queue. – AlwaysDrop—sets the drop type as AlwaysDrop. This algorithm implies that the packets are always dropped. – WRED—sets the drop type as WRED (Weighted Random Early Detection). WRED is an enhanced RED mechanism for congestion avoidance with support for six drop profiles maintained separately for each color (green, yellow, and red) TCP or NON-TCP traffic. On packet arrival, an Active Queue Management algorithm is executed which may randomly drop a packet.

Fields	• Drop Algo Enable Flag—select the option for enabling /disabling drop algorithm for congestion management. The default option is Enable. Options are: – Enable—enables drop algorithm for congestion management. – Disable—disables drop algorithm for congestion management. • Queue template size—enter the queue size. This is depth in bytes of the queue being measured, at which a trigger is generated to the dropping algorithm. This value ranges from 0 to 65535. The default value is 10000. NOTE: The value of this field must be greater than or equal to the Random Detect Min Average Threshold and less-than/equal to Random Detect Max Average Threshold if Random Detection is enabled. The threshold value can be configured using the RedConf Settings screen. NOTE: For the tailDrop or headDrop algorithms, this field represents the depth of the queue at which the drop action will take place • Drop Next—selects the next differentiated services functional data path element to handle traffic for this data path. The default option is None. Options are: – None—disables the drop next option. – Classifier—sets classifier as the next differentiated services functional data path element to handle traffic for this data path. – Meter—sets meter as the next differentiated services functional data path element to handle traffic for this data path. – Action—sets Action as the next differentiated services functional data path element to handle traffic for this data path. – Queue—sets Queue as the next differentiated services functional data path element to handle traffic for this data path • Index—select the available entries of corresponding functional blocks displayed by Drop Next. • QMeasure—select the Qmeasure to indicate the queue that a drop algorithm is to monitor when deciding whether to drop a packet. If the row pointed to does not exist, the algorithmic dropper element is considered inactive • Index—select the available entries of corresponding functional blocks displayed by QMeasure. • Drop Specific—select the drop specific entry that provides further detail regarding a drop algorithm. Options are: – Random Drop—enables random points to a table entry that provides further detail regarding a drop algorithm. • Index—select the available entries of corresponding functional blocks displayed by Drop Specific.

Fields (cont)	• Storage—select the storage type for the conceptual row. The default option is Non-Volatile. Options are: – Volatile—reflects the configurations for an interface whose interface index has been assigned, and for which the supporting implementation is currently present. – Non-Volatile—reflects the configuration for an interface whose interface index has been assigned, but for which the supporting implementation is currently not present.
Buttons	• Add—adds and saves new configuration. • Modify—modifies attributes and saves the changes. NOTE: The attributes of the default Queue Template cannot be modified • Reset—resets to default value for respective fields and discards all user inputs. The attributes of the default Queue Template cannot be modified. • Delete—deletes the selected entry. NOTE: The default Queue Template Id 1 cannot be deleted.

Red Conf Settings

Figure 14: Red Conf Settings—Part A

The screenshot displays the 'RedConf Settings' window. At the top, a navigation bar includes tabs for Queue Template, RedConf, Shape Template, Scheduler Table, Queue Table, Min Rate, Max Rate, Hierarchy, Queue Map, Scheduler, and Queue. The 'RedConf' tab is active.

The main configuration area is titled 'RedConf Settings' and contains the following fields:

- QTempld: [Text input field]
- Next Free Id: 2
- Drop Precedence: 0 (dropdown)
- Min Avg Thres: [Text input field]
- Max Avg Thres: [Text input field]
- Max PktSize: [Text input field]
- Max Probability: [Text input field]
- Exponential Weight: [Text input field]
- Gain: [Text input field]
- Dropthreshold Type: DISCARD PACKETS (dropdown)
- ECN Threshold: [Text input field]
- Additional WRED Flags: None (dropdown)
- Min Thresh Packets: [Text input field]
- Max Thresh Packets: [Text input field]
- Sampling Rate: [Text input field]
- Storage: Volatile (dropdown)

At the bottom of the configuration area are 'Add' and 'Reset' buttons.

Below the configuration area is a table showing existing configurations:

Select	Dp	QTempld	MinAvgThres	MaxAvgThres	MaxPktSize	MaxProb	ExpWeight	Gain	DropThreshType
☒	0	1	10000	50000	1000	1	0	0	DISCARD PACKETS

Figure 15: RedConf Settings—Part B

RedConf Settings

QTempId Next Free Id

Drop Precedence

Min Avg Thres

Max Avg Thres

Max PktSize

Max Probability

Exponential Weight

Gain

Dropthreshold Type

ECN Threshold

Additional WRED Flags

Min Thresh Packets

Max Thresh Packets

Sampling Rate

Storage

Select	Dp	QTempId	MinAvgThres	MaxAvgThres	MaxPktSize	MaxProb	ExpWeight	Gain	DropThreshType
☐	0	1	10000	50000	1000	1	0	0	DISCARD PACKETS
☒	0	2	10000	50000	1000	1	0	0	DISCARD BYTES

Figure 16: RedConf Settings—Part A

RedConf Settings

QTempId Next Free Id

Drop Precedence

Min Avg Thres

Max Avg Thres

Max PktSize

Max Probability

Exponential Weight

Gain

Dropthreshold Type

ECN Threshold

Additional WRED Flags

Min Thresh Packets

Max Thresh Packets

Sampling Rate

Storage

MaxProb	ExpWeight	Gain	DropThreshType	ECN Threshold	WRED Flags	Min Thresh Packets	Max Thresh Packets	Sampling Rate	Storage
0	0	0	DISCARD PACKETS	0	None	0	0	0	Volatile
0	0	0	DISCARD BYTES	0	None	0	0	0	Volatile

Screen Objective	This screen allows the user to configure parameters for Random Detect Algorithm.
NOTE: This screen can be configured only if QoS is started in the system using the Basic Settings screen.	
Navigation	System > QoS Egress > Red Conf

Fields	• QTempId—enter the index that enumerates the queue entries. This value ranges from 0 to 65535. • Next Free Id—specifies an integer which may be used as a new index in the table. The value of zero indicates that no more new entries can be created in the relevant table. This is a read-only field. • Drop Precedence—select the drop precedence. The default option is 0. The list contains: – 0—sets low drop precedence—discards <i>TCP</i> Green. – 1—sets medium drop precedence—discards <i>TCP</i> Yellow. – 2—sets high drop precedence—discards <i>TCP</i> Red. – 3—discards <i>NON-TCP</i> Green – 4—discards <i>NON-TCP</i> Yellow – 5—Discards <i>NON-TCP</i> Red • Max Avg Thres—enter the maximum average threshold for the random detect algorithm. Below this threshold, packets are admitted into the queue. This value ranges from 0 to 65535. The default value is 50000. NOTE: The value of this field should be greater than or equal to the Min Avg Threshold and less than or equal to the Queue Size. The Queue Size can be configured using the Queue Template Settings screen. NOTE: The units for this is based on the Drop Threshold Type configured. • Min Avg Thres—enter the minimum average threshold for the random detect algorithm. Below this threshold, packets are admitted into the queue. This value ranges from 0 to 65535. The default value is 10000. NOTE: The value of this field should be less than or equal to the Max Avg Threshold and the Queue Size. The Queue size can be configured using the Queue Template Settings screen. NOTE: The units for this is based on the Drop Threshold Type configured. • Max PktSize—enter the maximum allowed packet size. This value ranges from 0 to 65535 bytes. The default value is 1000. • Max Probability—enter the percentage of maximum probability of discarding a packet. This value ranges from 1 to 100. The default value is 100. • Exponential Weight—enter the exponential weight for determining the average queue size. This value ranges from 0 to 31. The default value is 0. • Gain—enter the gain value which defines an increase in drop-probability on each granular increase of buffer-occupancy due to received traffic. This determines the smoothing that should be applied. The value ranges from 0 to 100. The default value is 0.

Fields (cont).	• Droptreshold Type—select the drop threshold type to set the <i>WRED</i> drop type. The default option is DISCARD PACKETS. The list contains: – DISCARD PACKETS—sets the <i>WRED</i> drop type to Discard packets. – DISCARD BYTES—sets the <i>WRED</i> drop type to Discard in terms of bytes. NOTE: Value configured for Min Avg Thresh and Max Avg Thresh is interpreted as Packets/Bytes based on the selected option • ECN Threshold—enter the Explicit Congestion Notification (<i>ECN</i>) threshold to define the Queue depth in bytes to stop marking and start dropping <i>ECN</i> eligible packets. The value ranges from 0 to 65535. The default value is 0. • Additional WRED Flags—select the option to define the additional flags type for the <i>WRED</i> profiles. The default option is None. The list contains: – None—disables the additional <i>WRED</i> flags option. – CapAverage—sets the average queue size as always less than the actual queue size. – MarkCongestion—marks <i>ECN</i> instead of dropping the <i>WRED</i> profiles. – Both—selects both CapAverage and MarkCongestion options to define the additional flags type for the <i>WRED</i> profiles. • Min Thresh Packets—specifies the average queue depth in packets, beyond which traffic has a non-zero probability of being dropped. This value ranges from 1 to 4294967295. This is read only field. • Max Thresh Packets—specifies the average queue depth beyond which traffic has a probability indicated by Max Probability of being dropped or marked. This value ranges from 1 to 4294967295. This is read only field. • Sampling Rate—enter the number of times per second the queue is sampled for queue average calculation. A value of zero is used to mean that the queue is sampled approximately each time a packet is enqueued (or dequeued). This value ranges from 1 to 1000000. Default value is 0. • Storage—select the storage type for the conceptual row. The default option is Non-Volatile. Options are: – Volatile—reflects the configurations for an interface whose interface index has been assigned, and for which the supporting implementation is currently present. – Non-Volatile—reflects the configuration for an interface whose interface index has been assigned, but for which the supporting implementation is currently not present.

Buttons	• Add—adds and saves new configuration. • Modify—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs. The attributes of the default Queue Template cannot be modified. • Delete—deletes the selected entry. NOTE: The entries can be deleted only if the Drop Algorithm Flag for the queue template is disabled using the Queue Template Settings screen.

Scheduler Table Settings

Figure 17: Scheduler Table Settings

SchedulerTable Settings

Scheduler Id *

Egress Interface ▼

Q Algo ▼

Shape Id ▼

Hierarchy Level

Select	EgressPort	Scheduler Id	Q Algo	shape Id	Hierarchy Level	Global Id
☐	Gi0/1 ▼	1	strictPriority ▼	▼	0	1
☐	Gi0/2 ▼	1	strictPriority ▼	▼	0	2

Screen Objective	This screen allows the user to choose the Scheduler settings.
NOTE: • This screen can be configured only if QoS is started in the system using the Basic Settings screen. • The entries in the bottom form are displayed only if QoS is started in the system.	
Navigation	System > QoS Egress > Scheduler Table

Fields	• Scheduler Id—enter the scheduler identifier that uniquely identifies the scheduler in the system/egress interface. This value ranges from 0 to 65535. • Egress Interface—select the outgoing port number which is already specified in the system. • Q Algo—select the option to set the packet scheduling algorithm for the port. The default option is strictPriority. Options are: – strictPriority—enables the strict priority algorithm for the port. – roundRobin—enables round robin algorithm for the port. – weightedRoundRobin—enables weighted round robin algorithm for the port. • Shape Id—select the shaper identifier that specifies the bandwidth requirements for the scheduler. This value ranges from 0 to 65535. NOTE: This field list the shape IDs configured using the Shape Template Settings scree. • Hierarchy Level—enter the depth of the queue/scheduler hierarchy. This value ranges from 0 to 10. A value of 0 indicates that there is no hierarchy and that all queues/schedulers are port-bound. The default value is 0. • Global Id—specifies the scheduler identifier that uniquely identifies the scheduler in the system / egress interface. This value ranges from 0 to 65535.
Buttons	• Add—adds and saves new configuration. • Modify—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs. The attributes of the default Queue Template cannot be modified. • Delete—deletes the selected entry. NOTE: The default entries cannot be deleted.

Queue Table Settings

Figure 18: Queue Table Settings

QueueTable Settings

Egress Interface Gi0/1 ▼
 Q Id *
 Q Template Id 1 ▼
 Q Scheduler Id
 Q weight
 Q Priority
 Q Shape Id ▼

Add
Reset

Select	Egress Port	Q Id	Q TemplateId	Q SchedulerId	Q Weight	Q Priority	Q shapeId	Global Id
☐	Gi0/1 ▼	1	1 ▼	1	1	0	None ▼	1
☐	Gi0/1 ▼	2	1 ▼	1	1	1	None ▼	2
☐	Gi0/1 ▼	3	1 ▼	1	1	2	None ▼	3
☐	Gi0/1 ▼	4	1 ▼	1	1	3	None ▼	4

Screen Objective	This screen allows the user to choose the queue table settings.
NOTE: - This screen can be configured only if QoS is started in the system using the Basic Settings screen. - The entries in the bottom form are displayed only if QoS is started in the system.	
Navigation	System > QoS Egress > Queue Table
Fields	Egress Interface—select the outgoing port number from the list of interfaces created in the system. Q Id—enter the queue identifier that uniquely identifies the queue in the system/port. This value ranges from 1 to 65535. Q Template Id—select the queue template ID applied for configuring queue attributes. This value ranges from 1 to 65535. NOTE: This field lists the queue template id created using the Queue Template Settings screen. Q Scheduler Id—enter the scheduler identifier that manages the specified queue. This identifier is unique relative to an egress interface. This value ranges from 1 to 65535. Q weight—enter the user assigned weight to the CoS queue. The assigned weights are used only when the scheduling algorithm is a weighted scheduling algorithm. This value ranges from 1 to 1000. The default value is 0.

Fields (cont)	• Q Priority—enter the user assigned priority for the CoS queue. The assigned priority is used only when the scheduler uses a priority based scheduling algorithm. This value ranges from 0 to 15. The default value is 0. • Q Shape Id—select the shaper identifier that specifies the bandwidth requirements for the queue. The default value is None.
Buttons	• Add—adds and saves new configuration. • Modify—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs. The attributes of the default Queue Template cannot be modified. • Delete—deletes the selected entry.

Min Rate

Figure 19: Min Rate

Min Rate

Min Rate Id *
Next Free Id

Priority

Absolute

Relative

Storage Volatile ▼

Add Modify Reset

Select	Min Rate Id	Priority	Absolute	Relative	Storage
☒	1	0	10000	0	▼

Delete

Screen Objective	This screen allows the user to configure the minimum rate settings.
NOTE: • This screen can be configured only if QoS is started in the system using the Basic Settings screen. • The entries in the bottom form are displayed only if QoS is started in the system.	
Navigation	System > QoS Egress > Min Rate
Fields	• Min Rate Id—enter the index that enumerates the minimum rate parameter entries. This value ranges from 1 to 65535. • Next Free Id—specifies an integer which may be used as a new index in the table. The value of zero indicates that no more new entries can be created in the relevant table. This is a read-only field. • Priority—this field is greyed out.

Fields (cont)	• Absolute—enter the minimum absolute rate, in kilobits/sec, that a downstream scheduler element should allocate to this queue. If the value is zero, then there is effectively no minimum rate guarantee. If the value is non-zero, the scheduler will assure the servicing of this queue to at least this rate. This value ranges from 1 to 4294967295. The default value is 10000. • Relative—enter the minimum rate that a downstream scheduler element should allocate to this queue, relative to the maximum rate of the interface as reported by ifSpeed or ifHighSpeed, in units of 1/1000 of 1. If the value is zero, then there is effectively no minimum rate guarantee. If the value is non-zero, the scheduler will assure the servicing of this queue to at least this rate. This value ranges from 1 to 4294967295. • Storage—select the storage type for the conceptual row. The default option is Non-Volatile. Options are: – Volatile—reflects the configurations for an interface whose interface index has been assigned, and for which the supporting implementation is currently present. – Non-Volatile—reflects the configuration for an interface whose interface index has been assigned, but for which the supporting implementation is currently not present.
Buttons	• Add—adds and saves new configuration. • Modify—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs. The attributes of the default Queue Template cannot be modified. • Delete—deletes the selected entry. NOTE: The default entries cannot be deleted.

Max Rate

Figure 20: Max Rate

Max Rate

Max Rate Id * Next Free Id
 Absolute
 Relative
 Threshold
 Storage ▼

Select	Max Rate Id	Level	Absolute	Relative	Threshold	Storage
☒	1	2	10000	0	10000	▼

Screen Objective	This screen allows the user to configure the minimum rate settings.
NOTE: - This screen can be configured only if QoS is started in the system using the Basic Settings screen. - The entries in the bottom form are displayed only if QoS is started in the system.	
Navigation	System > QoS Egress > Max Rate
Fields	Max Rate Id—enter the index that enumerates the minimum rate parameter entries. This value ranges from 1 to 65535. NOTE: The Max rate entries with IDs 1 and 2 are already created in the system and cannot be deleted. Next Free Id—specifies an integer which may be used as a new index in the table. The value of zero indicates that no more new entries can be created in the relevant table. This is a read-only field. Absolute—enter the maximum absolute rate, in kilobits/sec, that a downstream scheduler element should allocate to this queue. If the value is zero, then there is effectively no maximum rate limit, and the scheduler should attempt to work conserving for this queue. If the value is non-zero, the scheduler will limit the servicing of this queue to, at most, this rate in a non-work-conserving manner. This value ranges from 1 to 4294967295.

Fields (cont)	• Relative—enter the maximum rate that a downstream scheduler element should allocate to this queue, relative to the maximum rate of the interface as reported by ifSpeed or ifHighSpeed, in units of 1/1000 of 1. If the value is zero, then there is effectively no maximum rate limit and the scheduler should attempt to work conserving for this queue. If the value is non-zero, the scheduler will limit the servicing of this queue to, at most, this rate in a non-work-conserving manner. This value ranges from 1 to 4294967295. • Threshold—specifies the number of bytes of queue depth at which the rate of a multi-rate scheduler will increase to the next output rate. In the last conceptual row for such a shaper, this threshold is ignored and by convention is zero. This value ranges from 1 to 4294967295. • Storage—select the storage type for the conceptual row. The default option is Non-Volatile. Options are: – Volatile—reflects the configurations for an interface whose interface index has been assigned, and for which the supporting implementation is currently present. – Non-Volatile—reflects the configuration for an interface whose interface index has been assigned, but for which the supporting implementation is currently not present.
Buttons	• Add—adds and saves new configuration. • Modify—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs. The attributes of the default Queue Template cannot be modified. • Delete—deletes the selected entry. NOTE: The default entries cannot be deleted.

Queue Map Settings

Figure 21: QueueMap Settings

QueueMap Settings

Egress Interface None ▾
 Traffic Class
 Priority Type none ▾
 Regen Priority
 Queue Id

Add Reset

Select	Egress Interface	Traffic Class	Pri Type	Regen Pri	Queue Id
☐	None ▾	0	vlanPri ▾	0	1
☐	None ▾	0	vlanPri ▾	1	2
☐	None ▾	0	vlanPri ▾	2	3
☐	None ▾	0	vlanPri ▾	3	4
☐	None ▾	0	vlanPri ▾	4	5
☐	None ▾	0	vlanPri ▾	5	6
☐	None ▾	0	vlanPri ▾	6	7
☒	None ▾	0	vlanPri ▾	7	8

Apply Delete

Screen Objective	This screen allows the user to map an egress port, CLASS of service to a queue.
NOTE: - This screen can be configured only if QoS is started in the system using the Basic Settings screen. - The entries in the bottom form are displayed only if QoS is started in the system.	
Navigation	System > QoS Egress > Queue Map
Fields	Egress Interface—select the outgoing port number from the list of interfaces created in the system. Traffic Class—enter the input class (associated with an incoming packet) that needs to be mapped to an outbound queue. This value ranges from 1 to 65535.

Fields (cont)	• Priority Type—select the regenerated-priority type to interpret the value of RegenPriority object. Options are – None—disables regenerated-priority type to interpret the value of RegenPriority object. – vlanPri—sets the regenerated-priority type to interpret the value of RegenPriority object as Vlan. – ipTos—sets the regenerated-priority type to interpret the value of RegenPriority object as IP Type of Service type. – ipDscp—sets the regenerated-priority type to interpret the value of RegenPriority object as IP Differentiated Services Code Point. – mplsExp—sets the regenerated-priority type to interpret the value of RegenPriority object as MPLS Experimental. – vlanDEI—sets the regenerated-priority type to interpret the value of RegenPriority object as VLAN Drop Eligibility Indicator. • Regen Priority—enter the regenerated-priority (for an incoming packet) that needs to be mapped to an outbound queue. This is mutually exclusive to the CLASS configuration. This value ranges from 0 to 63. • Queue Id—enter the queue identifier that uniquely identifies a queue relative to an interface. It could be configured with a unique value in the system. This value ranges from 1 to 65535.
Buttons	• Add—adds and saves new configuration. • Modify—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs. The attributes of the default Queue Template cannot be modified. • Delete—deletes the selected entry.

Scheduler

Figure 22: Scheduler

Scheduler

Scheduler Id * Next Free Id
 Scheduler Next Index
 Method
 Scheduler Min Rate Index
 Scheduler Max Rate Index
 Storage

Select	Scheduler Id	Scheduler Next	Index	Method	Min Rate	Min Rate Id	Max Rate	Max Rate Id	Storage
☐	1	None	0	Priority		0		0	
☐	2	None	0	Priority		0		0	
☐	3	None	0	Priority		0		0	
☐	4	None	0	Priority		0		0	

Screen Objective	This screen allows the user to choose the Scheduler settings.
NOTE: - This screen can be configured only if QoS is started in the system using the Basic Settings screen. - The entries in the bottom form are displayed only if QoS is started in the system.	
Navigation	System > QoS Egress > Scheduler
Fields	Scheduler Id—enter the index that enumerates the scheduler entries. This value ranges from 0 to 65535. Next Free Id—specifies an integer which may be used as a new index in the table. The value of 0 indicates that no more new entries can be created in the relevant table. This is a read only field. Scheduler Next—select the next differentiated services functional data path element to handle traffic for this data path. Options are: - None—disables traffic handling. - Classifier—enables classifier setting. - Meter—enables the meter setting. - Action—enables the action setting. - AlgoDrop—enables the algorithm drop setting

Fields (cont)	• Method—select the scheduling algorithm used by this scheduler. Options are: – Priority—enables the priority scheduling algorithm. – WRR—enables the weighted round robin scheduling algorithm. – WFQ—enables the weighted fair queuing scheduling algorithm. • Scheduler Min Rate—select the entry in minimum rate table which indicates the priority or minimum output rate from this scheduler. This attribute is used only when there is more than one level of scheduler. • Index—specifies the available entries of corresponding functional blocks displayed by Scheduler Min Rate. • Scheduler Max Rate—select the entry in maximum rate table which indicates the maximum output rate from this scheduler. When more than one maximum rate applies (for example, when a multi-rate shaper is in view), it points to the first of those rate entries. This attribute is used only when there is more than one level of scheduler. • Index—specifies the available entries of corresponding functional blocks displayed by Scheduler Max Rate. • Storage—select the storage type for the conceptual row. The default option is Non-Volatile. Options are: – Volatile—reflects the configurations for an interface whose interface index has been assigned, and for which the supporting implementation is currently present. – Non-Volatile—reflects the configuration for an interface whose interface index has been assigned, but for which the supporting implementation is currently not present.
Buttons	• Add—adds and saves new configuration. • Modify—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs. The attributes of the default Queue Template cannot be modified. • Delete—deletes the selected entry.

Queue

Figure 23: Queue

Queue

Queue Id *
Queue Next *
Queue Min Rate *
Queue Max Rate *
Storage *

Next Free Id 9
Index 13
Index
Index 2

Select	Queue Id	Queue Next	Index	Queue Min Rate	Index	Queue Max Rate	Index	Storage
☐	1		0	Min Rate	0	Max Rate	0	
☐	2		0	Min Rate	0	Max Rate	0	
☐	3		0	Min Rate	0	Max Rate	0	
☐	4		0	Min Rate	0	Max Rate	0	
☐	5		0	Min Rate	0	Max Rate	0	
☐	6		0	Min Rate	0	Max Rate	0	
☐	7		0	Min Rate	0	Max Rate	0	
☐	217		0	Min Rate	0	Max Rate	0	
☐	218		0	Min Rate	0	Max Rate	0	
☐	219		0	Min Rate	0	Max Rate	0	
☐	220		0	Min Rate	0	Max Rate	0	
☐	221		0	Min Rate	0	Max Rate	0	
☐	222		0	Min Rate	0	Max Rate	0	
☐	223		0	Min Rate	0	Max Rate	0	
☒	224		0	Min Rate	0	Max Rate	0	

Screen Objective	This screen allows the user to choose the queue parameters.
NOTE: This screen can be configured only if QoS is started in the system using the Basic Settings screen.	
Navigation	System > QoS Egress > Queue
Fields	Queue Id—enter the index that enumerates the queue entries. This value ranges from 0 to 65535. Next Free Id—specifies an integer which may be used as a new index in the table. The value of 0 indicates that no more new entries can be created in the relevant table. This is a read only field. Queue Next—select the next differentiated services scheduler. Index—specifies the available entries of corresponding functional blocks displayed by Queue Next.

Fields (cont)	• Queue Min Rate—select the minimum rate entry that the scheduler, pointed to by Queue Next, should use to service this queue. • Index—specifies the available entries of corresponding functional blocks displayed by Queue Min Rate. • Queue Max Rate—select the maximum rate entry that the scheduler, pointed to by Queue Next, should use to service this queue. • Index—specifies the available entries of corresponding functional blocks displayed by Queue Max Rate. • Storage—select the storage type for the conceptual row. The default option is Non-Volatile. Options are: – Volatile—reflects the configurations for an interface whose interface index has been assigned, and for which the supporting implementation is currently present. – Non-Volatile—reflects the configuration for an interface whose interface index has been assigned, but for which the supporting implementation is currently not present.
Buttons	• Add—adds and saves new configuration. • Modify—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs. The attributes of the default Queue Template cannot be modified. • Delete—deletes the selected entry.

Authentication Map

4. Authentication Protocols

This section describes the interfaces for 802.1x and TACACS+.

4.1. 802.1x

Describes 802.1x or PNAC settings.

The **802.1X** or **PNAC** ((the IEEE Standard for port-based Network Access Control (*PNAC*)) provides an authentication mechanism to devices attached to a bridge port. It prevents access to a port when the authentication fails. *802.1X* defines port-based authentication as a client-server based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. An authentication server validates each supplicant (client) connected to an authenticator (network access switch) port before making available any services offered by the switch or the LAN.

Until the authentication is provided, *802.1X* access control allows only *EAPOL* (Extensible Authentication Protocol Over LAN) traffic through the port only when the authentication is provided.

To access **802.1X** screens, go to **Layer 2 Management > 802.1X**.

The **802.1X** link parameters are configured through the screens displayed by the following tabs:

[*802.1X Basic Settings*](#)

[*PNAC Traces*](#)

[*802.1X Port Settings*](#)

[*802.1X Timer Configuration*](#)

[*Local Authentication Server Configuration*](#)

[*RADIUS Global Configuration*](#)

[*RADIUS Traces*](#)

802.1X Basic Settings

By default, the tab **Global Settings** displays the **LLDP Global Configuration** screen.

Figure 1: 802.1X Basic Settings

802.1x Basic Settings

System Control

Start

802.1x Authentication

Enable

Authentication Mode

Local

RemoteAuthenticationServerType

Radius Server

Network Access Server ID

fsNas1

Protocol Version

2

Apply

Configure Trace Options

Screen Objective	This screen allows the user to configure Authentication status, Authentication mode, and Authentication server type.
Navigation	Layer 2 Management > 802.1x > Basic Settings

Fields	• System Control—select the system control status of the <i>PNAC</i> module. The default option is Start. The options are: – Start—starts <i>PNAC</i> Module in the system. • Memory Resources required by <i>PNAC</i> module are allocated and <i>PNAC</i> module starts running. • Creates Memory pool, generates the <i>PNAC</i> interface task; initializes all global data structures. • Creates a hash table for storing the session nodes for MAC based authorization entries. • Creates semaphore for controlling concurrent access to critical data-bases • Initializes the timer submodule and <i>PNAC</i> Local authentication server module. – Shutdown—shuts down <i>PNAC</i> Module. • All resources used by <i>PNAC</i> module are released to the system and the <i>PNAC</i> module is shut down. • Initializes all <i>PNAC</i> state machines. • Deactivates the <i>PNAC</i> Local authentication server module, the timer module. Deletes the memory pool for the <i>PNAC</i> module and free its memory. • Deletes semaphore used for database access-control. • 802.1x Authentication—select the status of 802.1X based port security feature in the switch. The default option is Enable. The options are: – Enable—enables 802.1X based port security feature in the switch. The switch initiates authentication and sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame. – Disable—disables 802.1X based port security feature in the switch. <i>EAPOL</i> frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. • Authentication Mode—modifies attributes and saves the changes. – Remote—<i>RADIUS</i> server based authentication. It calls the AS client functions to communicate with the remote authentication server. – Local—provides the authentication service requirements in the local data-base. It maintains a simple database of users who can be permitted on valid proof to access a set of Authenticator's ports. It calls the service functions of the Local AS.

Fields (cont)	• RemoteAuthenticationServerType—select the Remote Authentication Server Type. The default option is <i>RADIUS</i> Server. The options are: – <i>RADIUS</i> Server—sets the remote authentication server as <i>RADIUS</i> Server. <i>RADIUS</i> server is responsible for authentication, authorization and maintaining its account information with port-based authentication. It is a gateway that controls access to the network. <i>RADIUS</i> uses the User Datagram Protocol (<i>UDP</i>). <i>RADIUS</i> server acts as the centralized authentication server. – Tacacs Server—sets the remote authentication server as <i>TACACS</i> Server. The remote <i>TACACS</i>+ server is responsible for <i>TACACS</i>+ client communication to authenticate the user, get authorization information, and send accounting information to the user. <i>TACACS</i>+ uses the Transmission Control Protocol (<i>TCP</i>). This feature is currently not supported. NOTE: This field can be configured only if the Authentication Mode is set as Local. • Network Access Server ID—enter the Network Access Server ID; it is the server ID for which authentication is provided. The Authenticator ID originates from the Access Request packets. The value is a string type. • Protocol Version—specifies the Version Number of the Protocol. This is a read-only field.
Buttons	• Apply—modifies attributes and saves the changes. • Configure Trace Options—accesses the <i>PNAC</i> Traces screen.

PNAC Traces

Figure 2: PNAC Traces

PNAC Traces

TRACES

☐ Errors

☐ Events

☐ Packets

☐ State-Machine

☐ Redundancy

Screen Objective	This screen allows the user to enable the required debug statements that are useful during debug operation. A four-byte integer is used for enabling the level of tracing. Each BIT in the four-byte integer represents a particular level of Trace. Combination of levels is also allowed. System errors such as memory allocation failures are announced by means of LOG messages and TRACE messages. Interface errors and protocol errors are made known by means of TRACE messages.
Navigation	Layer 2 Management > 802.1x > Basic Settings Click Configure Trace Options
Fields	• Traces—select the traces for which debug statements is to be generated. The default option is critical. The options are: – Errors—generates debug statement for all failure traces of the below mentioned trace. – Events—generates debug statements for event handling traces. This trace is generated in case of event processing. – Packets—generates debug statements for packets handling traces. This trace is generated in case of transmission or reception of packets. – State-Machine—generates debug statements for state machine handling traces. This trace is generated in case of State Machine processing. – Redundancy—generates debug statements for redundancy code flow traces. This trace is generated in case of redundancy processing.
Buttons	• Apply—modifies attributes and saves the changes. • Configure Global Options—accesses the <i>802.1X</i> Basic Settings screen.

802.1X Port Settings

Figure 3: 802.1X Port Settings

802.1x Port Settings

Select	Port	Port Control	Authentication Mode/Host Mode	Auth Port Status	Supp Port Status	Access Control	Configured Control Direction	Operational Control Direction	Auth-PM State	Supp-PM State	Reset Authentication	Authentication Retry Count	Timeout	Authentication Max Ret	Reauthentication
☐	G0/1	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/2	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/3	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/4	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/5	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/6	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/7	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/8	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/9	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/10	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/11	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/12	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/13	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/14	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/15	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/16	ForceAuthorized	Port Based/Multi-Host	Authorized	Authorized	INACTIVE	Both	Both	ForceAuth	ForceAuth	False	2	Disabled	3	False
☐	G0/17	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/18	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/19	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/20	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/21	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/22	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/23	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	G0/24	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	Ex0/1	ForceAuthorized	Port Based/Multi-Host	Authorized	Authorized	INACTIVE	Both	Both	ForceAuth	ForceAuth	False	2	Disabled	3	False
☐	Ex0/2	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☐	Ex0/3	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False
☒	Ex0/4	ForceAuthorized	Port Based/Multi-Host	Authorized	Unauthorized	INACTIVE	Both	Both	Initiate	Disconnected	False	2	Disabled	3	False

Apply

Note: To enable re-authentication, Port control should be Auto, Auth mode should be Port-based and Port status should be Authorized

Screen Objective	This screen allows the user to configure the security information at the individual port levels.
Navigation	Layer 2 Management > 802.1x > Port Settings
Fields	Select—select the port for which the configuration needs to be done. Port—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number). Port Control—select the control values of the Authenticator Port. The default option is ForceAuthorized. The options are: ForceAuthorized—allows all traffic through this port; disables 802.1X authentication and causes the port to transition to authorized state without requiring authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. ForceUnauthorized—blocks 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.

Fields (cont)	• Port Control—the options are (cont): – Auto—imposes <i>802.1X</i> authentication process in this port. Causes the port to begin the unauthorized state, allowing only <i>EAPOL</i> 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 <i>EAPOL</i>-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. • Authentication Mode/Host Mode—select the authentication mode to be imposed on the entry. The default option is Port Based. The list contains: – Port Based/Multi-Host—authenticates and authorizes devices attached to a Bridge port that has point-to-point connection characteristics named as Port based network access control. The following occurs when Port Based authentication is selected: • Receives incoming tagged / untagged data / control frames from the CFA Module (Interface Manager) and checks if the Port is authorized. If authorized, the frame is passed to the higher layer. • Receives outgoing data/control frames from the other modules. If authorized, the frame is passed to the CFA module. • When an <i>EAPOL</i> frame is received from CFA, it sends the EAP packet to the PNAC Interface Task, which then passes it to the Authenticator Module or Supplicant Module. • It forwards all received <i>EAPOL</i>-Start, <i>EAPOL</i>-Logoff and <i>EAP</i>-Responses to the Authenticator Module via the <i>PNAC</i> Interface Task. • It forwards all received <i>EAP</i>-Requests, <i>EAP</i>-Success, and <i>EAP</i>-Failure to the Supplicant Module via the <i>PNAC</i> Interface Task. It forwards all received <i>EAPOL</i>-Key frames to the Key Handler Module via the <i>PNAC</i> Interface Task. • It maintains the physical link status information provided by CFA and informs the Authenticator and Supplicant modules to take the necessary action on physical link UP/DOWN conditions. • It forms an <i>EAPOL</i> frame when requested by the Authenticator Module or Supplicant Module or Key Handler Module and transmits it to CFA – Mac Based / Single-Host—authenticates and authorizes devices attached to a Bridge port in the shared LAN named as <i>MAC</i>-based network access control. The following occurs when <i>MAC</i>-based authentication is selected. • On receiving tagged/untagged data/control frames from the CFA Module, it checks if the source <i>MAC</i> 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 dejected, and the frame is dropped at the CFA Module.

Fields (cont)	• Authentication Mode/Host Mode—the list contains (cont): – Mac Based / Single-Host—(cont). • If neither of the above occurs, the Authenticator will initiate a new authentication session for that source <i>MAC</i> address and return the unauthorized status to the CFA Module, which then drops the frame. NOTE: MAC based authentication can be configured only if the Port control option is Auto. • Auth Port Status—displays the status of the Supplicant PAE state machine. The options are: – Authorized—the module is ready for transmission or reception of data. – Unauthorized—the module is not ready for transmission or reception of data. • Supp Port Status—displays the status of the Authenticator Port. The options are: – Authorized—the module is ready for transmission or reception of data. – Unauthorized—the module is not ready for transmission or reception of data. • Access Control—select the Access Control status for the port. This setting is for the application of the Supplicant authorization state when the port is operating as both Supplicant and Authenticator. The default option is INACTIVE. The list contains: – INACTIVE—indicates that the port uses only the Authenticator authorization state to restrict access to the port and not the Supplicant authorization state. – ACTIVE—indicates that the port applies both the Supplicant authorization state and Authenticator authorization state. • Configured Control Direction—select the value of the administrative controlled directions parameter for the port. The options are: – Both—authentication control is imposed on both incoming and outgoing packets. – In—authentication control is imposed on the incoming packets. • Operational Control Direction—select the value of the operational controlled directions parameter for the port. The options are: – Both—authentication control is imposed on both incoming and outgoing packets. – In—authentication control is imposed on the incoming packets.

Fields (cont)	Auth SM State—select the value of the operational controlled directions parameter for the port. The options are: – Initialize—this state occurs when the module is disabled and port is down. – Disconnected—there will be a transition from Initialize to disconnecting. State Machine (<i>SM</i>) never remains in this state—there will be an immediate transition. – Connecting—this state is the beginning of the <i>PNAC</i> packet exchange. – Authenticating—this state occurs whenever authenticator receives response ID from supplicant. – Authenticated—this state occurs whenever authenticator <i>SM</i> port transitions to authorized through EAP exchange. – Aborting—this state occurs when Authenticator <i>SM</i> receives re-authenticating event or EAP start or supplicant log off. – Held—this state occurs when authentication failure occurs due to wrong user name or password. – ForceAuth—this state occurs when the port control is changed to force authorized. – ForceUnauth—this state occurs when the port control is changed to force unauthorized. • SuppSMState—select the state of the Supplicant State Machine (<i>SM</i>). The options are: – Disconnected—there will be a transition from Initialize to disconnecting. State Machine never remains in this state—there will be an immediate transition. – Logoff—state Machine never remains in this state and there will be an immediate transition to the other state. – Connecting—this state is the beginning of the <i>PNAC</i> packet exchange. – Authenticating—this state occurs whenever authenticator receives response ID from supplicant. – Authenticated—this state occurs whenever authenticator <i>SM</i> port transitions to authorized through EAP exchange. – Aborting—this state occurs when Authenticator <i>SM</i> receives re-authenticating event or EAP start or supplicant log off. – Held—this state occurs when authentication failure occurs due to wrong user name or password. – ForceAuth—this state occurs when the port control is changed to force authorized. – ForceUnauth—this state occurs when the port control is changed to force unauthorized.

Fields (cont)	• Restart Authentication—select the value of the administrative controlled directions parameter for the port. The options are: – True—causes the Port to be initialized. – False—reverts to False once initialization is complete. NOTE: This field cannot be set as True when Authentication Mode/Host Mode is set as Mac Based/Single Host. • Reauth—select the re-authentication mechanism on the port. It re-authenticates the port without waiting for the configured number of seconds between re-authentication attempts and automatic re-authentication. The default option is Disabled. The options are: – Enabled—enables re-authentication on the port. – Disabled—disables re-authentication on the port. • Authentication Max Start—enter the maximum number of successive EAPOL-Start messages that will be sent before the supplicant assumes that there is no authenticator present. This value ranges from 1 to 65535. The default value is 3. • Reauthentication—select the re-authentication mechanism on the port. It re-authenticates the port without waiting for the configured number of seconds between re-authentication attempts and automatic re-authentication. The default value is False. The list contains: – True—enables re-authentication on the port. – False—disables re-authentication on the port. NOTE: To enable re-authentication, Port control should be Auto, Auth mode should be Port-based, and Port status should be Authorized.
Buttons	• Apply—modifies attributes and saves the changes.

802.1X Timer Configuration

Figure 4: 802.1X Timer Configuration

802.1x Timer Configuration									
Select	Port	Quiet Period (secs)	Transmit Period (secs)	Re-authentication Period (secs)	Supplicant Timeout	Server Timeout	Held Period	Auth Period	Start Period
☐	Gi0/1	60	30	3600	30	30	60	30	30
☐	Gi0/2	60	30	3600	30	30	60	30	30
☐	Gi0/3	60	30	3600	30	30	60	30	30
☐	Gi0/4	60	30	3600	30	30	60	30	30
☐	Gi0/5	60	30	3600	30	30	60	30	30
☐	Gi0/6	60	30	3600	30	30	60	30	30
☐	Gi0/7	60	30	3600	30	30	60	30	30
☐	Gi0/8	60	30	3600	30	30	60	30	30
☐	Gi0/9	60	30	3600	30	30	60	30	30
☐	Gi0/10	60	30	3600	30	30	60	30	30
☐	Gi0/11	60	30	3600	30	30	60	30	30
☐	Gi0/12	60	30	3600	30	30	60	30	30
☐	Gi0/13	60	30	3600	30	30	60	30	30
☐	Gi0/14	60	30	3600	30	30	60	30	30
☐	Gi0/15	60	30	3600	30	30	60	30	30
☐	Gi0/16	60	30	3600	30	30	60	30	30
☐	Gi0/17	60	30	3600	30	30	60	30	30
☐	Gi0/18	60	30	3600	30	30	60	30	30
☐	Gi0/19	60	30	3600	30	30	60	30	30
☐	Gi0/20	60	30	3600	30	30	60	30	30
☐	Gi0/21	60	30	3600	30	30	60	30	30
☐	Gi0/22	60	30	3600	30	30	60	30	30
☐	Gi0/23	60	30	3600	30	30	60	30	30
☐	Gi0/24	60	30	3600	30	30	60	30	30
☐	Ex0/1	60	30	3600	30	30	60	30	30
☐	Ex0/2	60	30	3600	30	30	60	30	30
☐	Ex0/3	60	30	3600	30	30	60	30	30
☒	Ex0/4	60	30	3600	30	30	60	30	30

Apply

Screen Objective	This screen allows the user configure the Timer parameters at the individual port level.
Navigation	Layer 2 Management > 802.1x > Timers

Fields	• Port—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number). • Quiet Period (secs)—enter the number of seconds that the switch remains in quiet state following a failed authentication exchange with the client. In this the duration the authenticator remains silent and will not attempt to acquire a supplicant. This value ranges from 0 to 65535 seconds. The default value is 60. • Transmit Period (secs)—enter the Time Period used by the Authenticator State machine to define when the EAP Request ID <i>PDU</i> is to be transmitted. This value ranges from 1 to 65535 seconds. The default value is 30. • Re-authentication Period (secs)—enter the time between periodic re-authentication of the supplicant. Re-authentication period denotes the number of times the switch restarts the authentication process before the port changes to the unauthorized state. This value ranges from 1 to 65535 seconds. The default is 3600. • Supplicant Timeout—enter the amount of time the switch waits for a response before resending the request to the client, when relaying a request from the authentication server to the client. This value ranges from 1 to 65535 seconds. The default value is 30. • Server Timeout—enter the amount of time the switch waits for a reply before resending the response to the server, when relaying a response from the client to the authentication server. This value ranges from 1 to 65535 seconds. The default value is 30. • Held Period—enter the amount of time the client will wait before re-attempting a failed 802.1X authentication. When the supplicant (in the client) receives an authentication failure indication from the switch, it remains idle for a period of time which is determined by the value of held-period. After this time, the supplicant initiates authentication again. Authentication failure might occur if supplicant provides a wrong password. This value ranges from 1 to 65535 seconds. The default value is 60. • Auth Period—enter the time interval for resending 802.1X request messages after not receiving a response. This value ranges from 1 to 65535 seconds. The default value is 30. • Start Period—enter the time interval for resending Start messages. Start period denotes the number of seconds between successive EAPOL-Start messages following no response from the authenticator. This value ranges from 1 to 65535 seconds. The default value is 30.
Buttons	• Apply—modifies attributes and saves the changes.

Local Authentication Server Configuration

Figure 5: Local Authentication Server Configuration

Local Authentication Server Configuration

User Name	admin *
Password	 *
Permission	Allow ▾ *
Auth-TimeOut	
Port List	
Add Reset	

Select	User Name	Permission	Auth-TimeOut (secs)	Port List
Apply Delete				

Screen Objective	This screen allows the user configure the local Authentication Server (AS) information. It contains authentication related user configuration information maintained by <i>PNAC</i> local AS. Every entry contains user name, password, authentication protocol used, authenticated session timeout, and access ports list for an user seeking authentication.
Navigation	Layer 2 Management > 802.1x > Local AS
Fields	• User Name—enter the identity of the user seeking authentication. This field is a string of maximum size 20. • Password—enter the password specific to the user name—a maximum size of 20. • Permission—select the allowance /denial of access for local authentication server. The options are: – Allow—authentication request is allowed for the set of ports in the Port List. – Deny—authentication request is not allowed for the set of ports in the Port List. • Auth-TimeOut (secs)—enter the Authentication Timeout in seconds. The time in seconds after which the Authentication offered to the user ceases. When the object value is 0, the ReAuthPeriod of the authenticator port is used by Authenticator. This value ranges from 1 to 7200 seconds. • Port List—enter the complete set of ports of the authenticator to which the user is allowed or denied access, based on the permission.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

RADIUS Global Configuration

Figure 6: RADIUS Global Configuration

RADIUS Global Configuration

Global Status
Disabled ▼

Apply

Screen Objective	This screen allows the user to enable the <i>RADIUS</i> Server.
Navigation	System > RADIUS > Global Configuration
Fields	Global Status—select enable or disable
Buttons	Apply—modifies attributes and saves the changes.

RADIUS Server Configuration

Figure 7: RADIUS Server Configuration

Radius Server Configuration

Server Address Type
IPv4 ▼

IP Address

Primary Server
No ▼

Shared Secret

Response Time (secs)

Retry Count

Authentication Port

Add
Reset

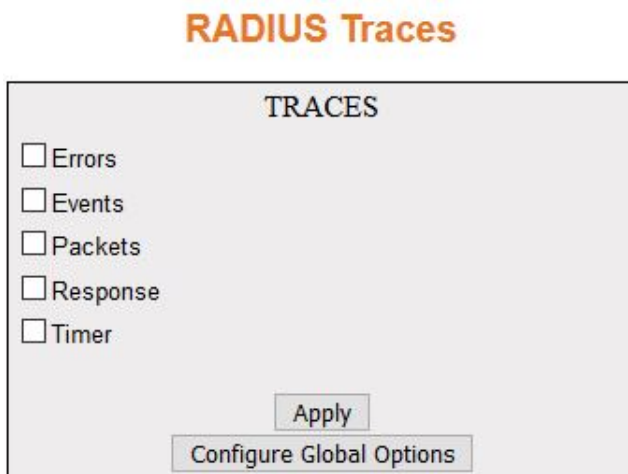
Select	IP Address Type	IP Address	Primary	Shared secret	Response Time (secs)	Retry Count	Authentication Port
Delete Modify							

Configure Trace Options

Screen Objective	This screen allows the user to configure the <i>RADIUS</i> Server settings. <i>RADIUS</i> (Remote Authentication Dial-In User Service) is a portable implementation of the <i>RADIUS</i> client protocol. This protocol carries authentication information between the Network Access Server (NAS) that desires to authenticate its links and the <i>RADIUS</i> server that is responsible for authenticating and maintaining the authentication information.
Navigation	Layer 2 Management > 802.1x > RADIUS Settings
Fields	• Server Address Type—select the <i>RADIUS</i> server address type. The default option is IPv4, <i>RADIUS</i> server address type is set as Internet Protocol Version 4, where a 32-bit address is used • IP Address—enter the IP Address of the <i>RADIUS</i> Server. • Primary Server—select a server type—a primary server or not. Only one server can be configured as the primary server. The default option is No. Options are: – Yes—indicates the server type as a primary server. – No—indicates the server type is not a primary serve • Shared Secret—enter the secret string, which is to be shared between the <i>RADIUS</i> Server and the <i>RADIUS</i> Client. The shared secret is the secret of the server to which the request was sent and from which the response was received. • Response Time (secs)—enter the maximum time within which the <i>RADIUS</i> Server is expected to respond for a request from the <i>RADIUS</i> Client. This value ranges from 1 to 120 seconds. The default value is 10.
Fields (cont)	• Retry Count—enter the maximum number of times a request can be re-transmitted before getting response from the <i>RADIUS</i> Server. If the retransmit count has exceeded the configured maximum retransmissions, the packet and the user entry are deleted from the user request table and the error condition is logged. This value ranges from 1 to 254. The default value is 3. • Authentication Port—enter the port number used for authentication. This value ranges from 1 to 65535.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry. • Configure Trace Options—accesses <i>RADIUS</i> Traces screen.

RADIUS Traces

Figure 8: RADIUS Traces



Screen Objective	This screen allows the user to enable the required debug statements that are useful during debug operation. A four-byte integer is used for enabling the level of tracing. Each BIT in the four-byte integer represents a particular level of Trace. Combination of levels is also allowed. System errors such as memory allocation failures are announced by means of LOG messages and TRACE messages. Interface errors and protocol errors are made known by means of TRACE messages
Navigation	Layer 2 Management > 802.1x > RADIUS Settings > RADIUS Server Configuration Click Configure Trace Options
Fields	• Traces—select the traces for which debug statements is to be generated. The default option is critical. The options are: – Errors—generates debug statement for all failure traces of the below mentioned traces – Events—generates debug statements for event handling traces. This trace is generated in case of event processing. – Packets—generates debug statements for packets handling traces. This trace is generated in case of transmission or reception of packets. – Response—generates debug statements for state machine handling traces. This trace is generated in case of RADIUS processing. – Timer—generates debug statements. This trace is generated for timer functionality.
Buttons	• Apply—modifies attributes and saves the changes. • Configure Global Options—return to the RADIUS Server Configuration screen.

MAC Session Info

Figure 9: Mac Session Info

MAC Session Info							
Select	Supplicant MacAddr	Session Identifier	AuthSM State	Auth-Session Status	Session PortNumber	Session Initialize	Session Reauthenticate
Apply							
Screen Objective	This screen displays the <i>MAC</i> Session information details. It contains authentication session information associated with each Supplicant while the Authenticator operates in <i>MAC</i> -based authentication mode. The <i>MAC</i> session entries are deleted from the port whenever it receives the port operational status down information.						
Navigation	Layer 2 Management > 802.1x > Mac Session Info						
Fields	• Supplicant Mac Addr—displays the Supplicant <i>MAC</i> Address for the session. • Session Identifier—displays the Session Identifier of the supplicant. • Auth SM State—select the state of the Authenticator State Machine (<i>SM</i>) for the entry. The list contains: – Initialize—this state occurs when the module is disabled, and port is down – Disconnected—there will be a transition from Initialize to Disconnected. State Machine never remains in this state and there will be an immediate transition. – Connecting—this state is the beginning of the <i>PNAC</i> packet exchange. – Authenticating—this state occurs whenever authenticator receives response ID from supplicant.						

Fields (cont)	Auth SM State—the list contains (cont): – Authenticated—this state occurs whenever authenticator <i>SM</i> port transitions to authorized through EAP exchange. – Aborting—this state occurs when Authenticator <i>SM</i> receives re-authenticating event or EAP start or supplicant log off. – Held—this state occurs when authentication failure occurs due to wrong user name or password. – ForceAuth—this state occurs when the port control is changed to force authorized. – ForceUnauth—this state occurs when the port control is changed to force unauthorized. • Auth Session Status—displays the Authentication Session Status. – authorized—the module is ready for transmission or reception of data – unauthorized—the module is not ready for transmission or reception of data • Session PortNumber—displays the port number through which a particular Session MAC address is learnt. • Session Initialize—select the Session Initialize status for the Supplicant MAC Address configured. The default value is True. This list contains: – True—indicates Session Initialize is set. – False—indicates Session Initialize is reset. • Session Reauthenticate—select the session reauthentication status for the supplicant mac address configured. The default value is True. This list contains: – True—Indicates session re-authentication is initialized. – False—Indicates session re-authentication is reset.
Buttons	• Apply—modifies attributes and saves the change.

4.2. TACACS

Describes TACACS settings.

The Terminal Access Controller Access-Control System (*TACACS*) is a remote authentication protocol that is used to communicate with an authentication server commonly used in networks. *TACACS* allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network.

TACACS uses a client-server mechanism. The *TACACS* server authenticates the *TACACS* client using information such as user name and password.

To access *TACACS* screens, click **System > TACACS**.

The **TACACS** parameters are configured through the screens displayed by the following tabs:

[TACACS Server Configuration](#)

TACACS Traces
TACACS Active Server Configuration

TACACS Server Configuration

By default, the tab **TACACS Settings** displays the **TACACS Server Configuration** screen.

Figure 10: TACACS Server Configuration

Tacacs Server Configuration

Server Address Type

IPv4

IP Address

Shared Secret

Single Connection

No

Server Port

Server Timeout (secs)

Add

Reset

Configure Trace Options

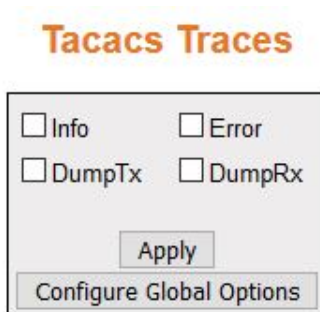
Select	Address Type	IP Address	Shared secret	Single Connection	Server Port	Server Timeout
Apply Delete						

Screen Objective	This screen allows the user to configure the TACACS server configuration.
Navigation	System > TACACS > Server

Fields	• Server—select the Server Address Type to be configured or deleted. • Server Address Type—select the address type of the <i>TACACS+</i> server. The default option is IPv4. • IP Address—enter the IPv4 address of the <i>TACACS+</i> server. The <i>TACACS+</i> client interacts with the server having this IP address. NOTE: IS5Com <i>TACACS</i> allows information for maximum of 5 servers to be configured. • Shared Secret—enter the secret key shared between the client and server (IPv4 or IPv6) for encryption and decryption. The default value is IS5Com. • Single Connection—select whether single connect support is enabled/ disabled for the server. The default option is No. The list contains: – Yes—allows multiple sessions over a single <i>TCP</i> connection. Thus, the authentication, authorization and accounting process are carried out in a single <i>TCP</i> connection. – No—does not allow the multiple sessions to handle over a single <i>TCP</i> connection. Thus, the authentication, authorization and accounting are carried out in separate <i>TCP</i> connection. • Server Port—enter the server port number for <i>TACACS</i> protocol. This value ranges from 0 to 65535. The default value is 49 for IPv4 and 4949 for IPv6. • Server Timeout (secs)—enter the timeout value within which the <i>TACACS</i> client expects a response from server. This value ranges from 1 to 255. The default value is 5 seconds. The <i>TACACS</i> client assumes that the primary server is down and gets connected with secondary server, after the expiry of this time.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. The attributes of the default Queue Template cannot be modified. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry. • Configure Trace Options—click to access the <i>TACACS</i> Traces screen

TACACS Traces

Figure 11: TACACS Traces



Screen Objective	This screen allows the user to enable or to select the required debug statements that will be useful during debug operation.
Navigation	System > TACACS > Server > TACACS Server Configuration screen appears. Click Configure Trace Options .
Fields	• Traces—select the traces for which debug statements is to be generated. The list contains: – Info—generates debug statements for informational messages – Error—generates debug statements for error message – DumpTx—generates debug statements for handling traces. This trace is generated when there is an error condition in transmission of packets. – DumpRx—generates debug statements for handling traces. This trace is generated when there is an error condition in reception of packets
Buttons	• Apply—adds and saves new configuration. • Configure Trace Options—click to access the <i>TACACS</i> Server Configuration screen.

TACACS Active Server Configuration

Figure 12: TACACS Active Server Configuration

Tacacs Active Server Configuration

Active Server Address Type: IPv4

Active Server IP Address:

Retransmit (secs): 2

Apply Reset

Select Active Server Address

Delete

Screen Objective	This screen allows the user to set the <i>TACACS</i> server that should be used as primary server.
Navigation	System > TACACS > Active Server or click TACACS AS tab.
Fields	• Select—select the Active Server IP address to be deleted. • Active Server Address Type—select the address type of the active server. The default option is IPv4. • Active Server IP Address—the IP address of the <i>TACACS</i> server that should be set as primary server. Maximum of 5 server's (IPv4 or IPv6) information can be configured for <i>TACACS</i>. This object indicates the active server among these 5 servers created using <i>TACACS</i> Server Configuration screen. The <i>TACACS+</i> client interacts with the configured server IP address. When set to zero, <i>TACACS</i> disables the active server concept. • Retransmit (secs)—enter the number of times the <i>TACACS</i> client remote server searches the list of maximum number of <i>TACACS</i> servers. This value ranges from 1 to 100 seconds. The default value is 2 seconds. If the <i>TACACS</i> client does not receive any response from the server for the given retransmit time, it searches and gets connected with the next server.
Buttons	• Apply—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs. • Delete—deletes the selected entry.

Timing Map

5. Timing Protocols

This is the introduction page for *PTP* and *SNTP*.

This section will contain descriptions for the *SNTP* and *PTP* interfaces.

5.1. Clock

Used to configure clock features such as *PTP* and Clock *IWF*.

CLOCK link provides the following links to configure the various clock features of the switch:

- **PTP** link allows the user to configure *PTP* IEEE 1588 Precision Time Protocol and some of its optional features—Acceptable Master and Alternate Timescale.
- **Clock IWF** link allows the user to configure various Clock Interworking parameters such as time source, accuracy, variance, etc.

Welcome to the Clock Management Page

The various Clock features of the switch can be configured through the links available in this page.

Through the [PTP](#) link you can configure PTP IEEE 1588 Precision Time Protocol and some of its optional features-Acceptable Master and Alternate Timescale

Through the [Clock IWF](#) link you can configure Various Clock Interworking parameters such as Time Source , Accuracy , Variance etc.,

5.2.

PTP

PTP (Precision Time Protocol) is defined in IEEE 1588 as Precision Clock Synchronization for Networked Measurements and Control Systems and was developed to synchronize the clocks in packet-based networks that include distributed device clocks of varying precision and stability standalone software which implements IEEE 1588. *PTP* is message based protocol which specifies how the real-time clocks in

a distributed system synchronize with each other. *PTP* creates master-slave hierarchy to synchronize the clocks in the system.

To access **PTP** screens, go to **Clock > PTP**.

The **PTP** link on the left pane allows configuring the *PTP* parameters through the following links:

[PTP Global Configurations](#)

[Clock Configuration Page](#)

[PTP Interfaces](#)

PTP Global Configurations

By default, the tab **PTP** displays the **PTP Global Configurations** screen.

Figure 1: PTP Global Configurations

PTP Global Configurations

Global Status	Enabled ▾
Network Protocol	IEEE 802.3

Apply

Screen Objective	This screen allows configuring the basic settings of <i>PTP</i> such as starting the <i>PTP</i> module and creating the primary context.
Navigation	Clock > PTP > Basic Settings
Fields	Global Status—specifies the system control status of the <i>PTP</i> module. The default option is Disabled. The list contains: - Disabled—shuts <i>PTP</i> in a device. This will remove all <i>PTP</i> related configurations from the system. - Enabled—starts <i>PTP</i> in a device. This will allow the user to configure the <i>PTP</i> parameters. NOTE: PTP module should be started for configuring the <i>PTP</i> parameters. Network Protocol—IEEE 802.3.
Buttons	Apply—adds and saves new configuration.

Clock Configuration Page

Figure 2: Clock Configuration Page

Clock Configurations Page

PTP Profile	Power Profile V2 ▾*
Profile ID	1c:12:9d:00:00:00
Clock Mode	Transparent ▾*
Delay Mechanism	P2P ▾*
Domain Number(0-254)	254 ▴ ▾*
Domain VLAN ID(1-4094)	▴ ▾
Domain VLAN Priority(0-7)	▴ ▾
Max Clock Ports(0-24)	24 ▴ ▾
Clock Identity	e8:e8:75:ff:fe:90:5f:82

Apply

Screen Objective	This screen allows the user to configure the clock data set table information. The clock data set table contains information of the clock on a particular domain. The entries in this table are created with the default values.
Navigation	Clock > PTP > Clock Settings

Fields	• PTP Profile—specifies the type of <i>PTP</i> Profile. The default profile is Power Profile V2. The options are: – No Profile – Default <i>E2E</i> – Default <i>P2P</i> – Utility Profile – Power Profile V2 • Profile ID—1c:12:9d:00:00:00 • Clock Mode—specifies the operating mode of the clock in the domain. The default option is Transparent. The list contains: – Transparent – Forward • Delay Mechanism—specifies the delay mechanism of the clock in the domain. The default option is P2P. The list contains: – <i>P2P</i>—the clock is in peer-to-peer (<i>P2P</i>) mode. It measures the time taken for a <i>PTP</i> event message to transit the device. This information will be updated in the correction field of the <i>PTP</i> messages. – <i>E2E</i>— the clock is in end-to-end (<i>E2E</i>) transparent mode. The clock calculates the residence time of <i>PTP</i> messages and measures the link delay of the ingress port of <i>PTP</i>. • Domain Number (0-254)—specifies the unique identifier of the domain. This domain ID defines the scope of the <i>PTP</i> message communication, state, operations, data sets and timescale. this value ranges from 0 to 254. • Domain VLAN ID (1-4094)—Specifies which VLAN that the transparent clock messages will use. • Domain VLAN Priority (0-7)—specifies the priority of the transparent clock messages. • Max Clock Ports (0-24)—specifies the number of the <i>PTP</i> ports. The maximum and default is 24. • Clock Identity—displays the unique ID of the local clock associated with the domain which is e8:e8:75:ff:fe:90:2e:02
Buttons	• Apply—adds and saves new configuration.

PTP Interfaces

Figure 3: PTP Interfaces

PTP Interfaces

Select	Port	Status	Min PDelay Interval (sec)	Propagation Delay (nsec)
☐	gigabitethernet_0/1	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/2	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/3	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/4	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/5	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/6	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/7	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/8	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/9	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/10	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/11	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/12	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/13	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/14	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/15	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/16	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/17	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/18	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/19	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/20	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/21	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/22	Disabled ▾	1 ▾	0
☐	gigabitethernet_0/23	Disabled ▾	1 ▾	0
☒	gigabitethernet_0/24	Disabled ▾	1 ▾	0

Apply

Screen Objective	This screen allows the user to add a <i>PTP</i> interface and configure the port table settings. The port settings table contains <i>PTP</i> configuration information for a particular port. Valid interface number and type have to be provided for configuring the port specific parameters.
Navigation	Clock > PTP > Port Settings
Fields	• Port—the value for the context name is default. It cannot be changed. • Status—select the operational status of the port in <i>PTP</i>. The default option is Disabled. Options are: – Disabled—disables <i>PTP</i> over the interface. – Enabled—enables <i>PTP</i> over the interface. • Min PDelay Interval (sec)—specifies the delay interval. • Propagation Delay (nsec)—an estimate of the current one-way propagation delay in scaled nanoseconds on the link attached to the port, calculated using the peer delay mechanism. If the <i>PTP</i> port delay mechanism is end-to-end, this value will be 0.
Buttons	• Apply—adds and saves new configuration.

Clock IWF

The **Clock IWF** module acts as a layer between the system clock and the protocol which synchronizes the system clock. This module selects the time source to set the system clock and maintains the information about the clock quality such as clock accuracy, class, variance, etc.

Clock Interworking Settings

Figure 4: Clock Interworking Settings

Clock Interworking Settings

Clock Variance	0
Clock Class	248
Clock Accuracy	254
Clock Time Source	PTP ▼
Clock UTC Offset	0
Hold Over Mode	Enabled ▼
Apply	

Note :1. Set Clock Time Source as *PTP/NTP* if *PTP* module/*SNTP* module is used to set the system time respectively.

2. Set Clock UTC Offset as (+HH:MM/-HH:MM) in between (+00:00 to +14:00)/(-00:00 to -12:00).

Screen Objective	This screen allows the user to configure the clock <i>IWF</i> parameters.
Navigation	Clock > Clock IWF
Fields	• Clock Variance—enter the variance of the primary clock. This object reflects the value provisioned by the external source (<i>NTP/SNTP/GPS</i>) that synchronizes the system clock. This value ranges from 0 to 255. The default value is 0 (minimum variance). • Clock Class—enter the class of the primary clock. This object reflects the value provisioned by the external source (<i>NTP/SNTP/GPS</i>) that synchronizes the system clock. This value ranges from 0 to 255. The default value is 248. • Clock Accuracy—enter the accuracy of the primary clock. Clock accuracy is the mean of the time or frequency error between the clock under test and a perfect reference clock, over an ensemble of measurements. This object reflects the value provisioned by the external source (<i>NTP/SNTP/GPS</i>) that synchronizes the system clock. This value ranges from 32 to 254. The default value is 254. • Clock Time Source—select the time source of the primary clock. The system clock is synchronized only through the specified source. The default option is <i>PTP</i>. The options are: – None—does not synchronize the system clock. – Atomic Clock—synchronizes the system clock through atomic clock. – GPS—synchronizes the system clock through Global Positioning System (<i>GPS</i>). – PTP—synchronizes the system clock through Precision Time Protocol (<i>PTP</i>). – NTP—synchronizes the system clock through Network Time Protocol (<i>NTP</i>). – Internal Oscillator—Synchronizes the system clock through Internal Oscillator. • Clock UTC Offset—enter the current <i>UTC</i> (Coordinated Universal Time) offset in scaled nanoseconds with respect to the system time. This value must be in the form of (+HAMM or –HH:MM) and in the range from +00:00 to +14:00 or –00:00 to –12:00. The default value is 0. • Hold Over Mode—select the option to specify whether the system clock is in Hold Over Mode. The default option is Enabled. The options are: – Enabled—enables the clock to be in holdover mode. – Disabled—disables the holdover mode. NOTE: The clock is said to be in Hold Over Mode if it has been previously synchronized or synchronized to another clock but is now free-running based on its own internal oscillator whose frequency is adjusted using data acquired while it had been synchronized or synchronized to the other clock.
Buttons	• Apply—adds and saves new configuration.

5.3. SNTP

This section describes how to configure the *SNTP* features of the switch.

SNTP (Simple Network Time Protocol) is a simplified version of the *NTP* protocol. The *NTP* protocol is meant for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.

To access **SNTP** screens, click **System > SNTP**.

The **SNTP** parameters are configured through the screens displayed by the following tabs:

[SNTP Settings](#)

[SNTP Unicast Table](#)

[SNTP Broadcast Configuration](#)

[SNTP Multicast Configuration](#)

[SNTP Multicast Configuration](#)

SNTP Settings

By default, the tab **SNTP** displays the **SNTP Settings** screen.

Figure 5: SNTP Settings

SNTP Settings

Sntp Admin Status	Disabled ▾
Client Version	Version 4 ▾
Addressing Mode	Unicast ▾
Sntp Client Port	123
Time Display Format	Hours ▾
AuthKey Id	0
Auth Algorithm	None ▾
AuthKey	
TimeZone	+00:00
DST StartTime	
DST EndTime	
Apply Refresh	

Note : To set system time using *SNTP*, set Clock Time Source parameter of **CLKIWF** as *NTP*.

Screen Objective	This screen allows the user to configure the details of <i>SNTP</i> Settings.
NOTE: To set the system time using <i>SNTP</i> , the Clock Time source should be configured as <i>NTP</i> using the CLKIWF screen. <i>CLKIWF</i> is short for Clock InterWorking Function.	

Navigation	System > SNTP > SNTP Settings
Fields	• SNTP Admin Status—select the <i>SNTP</i> client module status. The default option is Disabled. The list contains: – Enabled—enables the <i>SNTP</i> client module. On enabling, the server starts sending the request to the host for synchronization. – Disabled—Disables the <i>SNTP</i> client module. NOTE: All configurations are active only when the <i>SNTP</i> module is enabled. • Client Version—select the <i>SNTP</i> client module version. The default option is Version 4. The list contains: – Version 1—sets the <i>SNTP</i> client version as Version 1. – Version 2—sets the <i>SNTP</i> client version as Version 2. – Version 3—sets the <i>SNTP</i> client version as Version 3. – Version 4—sets the <i>SNTP</i> client version as Version 4. NOTE: All <i>SNTP</i> requests are sent out with the current configured version number. When required, the administrator can change the current version number. • Addressing Mode—select the <i>SNTP</i> client addressing mode. The default option is Unicast. The list contains: – Unicast—<i>SNTP</i> client operates in a point-to-point fashion. A unicast client 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—<i>SNTP</i> client operates in a point-to-multipoint fashion. The <i>SNTP</i> 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—<i>SNTP</i> client operates in point-to-multipoint fashion. The <i>SNTP</i> server uses a multicast group address to send unsolicited <i>SNTP</i> messages to clients. The client listens on this address and sends no requests for updates. – Multicast—<i>SNTP</i> client operates in a multipoint-to-point fashion. The <i>SNTP</i> client sends a request to a designated IPv4 or IPv6 local broadcast address or multicast group address. One or more anycast servers reply with their individual unicast addresses • SNTP Client Port—select the time display format. The default option is Hours. The list contains: • Time Display Format—enter the username. – Hours—Sets the time display as 24 hours format. – Am/Pm—Sets the time display as 12 hours am/pm format.

Fields (cont)	• AuthKey Id—enter the key identifier identifying the cryptographic key used to generate the message-authentication code: NOTE: This field is greyed out when addressing mode is Broadcast, Multicast and Multicast. • AuthKey Algorithm—select the <i>SNTP</i> authentication algorithm. The default authentication algorithm is None. The list contains: – None—the communication will be opened, and no authorization will be provided. – md5—<i>MD5</i> (Message Digest-5) verifies data integrity. <i>MD5</i> is intended for use with digital signature applications, which requires that large files must be compressed by a secure method before being encrypted with a secret key, under a public key cryptosystem. NOTE: This field is greyed out when addressing mode is Broadcast, Multicast and Multicast. • AuthKey—enter the key identifier identifying the cryptographic key used to generate the message-authentication code. NOTE: This field is greyed out when addressing mode is Broadcast, Multicast and Multicast. • TimeZone—enter the system time zone with respect to <i>UTC</i>. The format is (+/-) HH:MM. Where: – +/-—denotes the difference with the Greenwich Mean Time. + indicates forward time zone and— indicates backward time zone. – HH denotes the hours. It is 24-hour format with value ranging from 00 to 23. – mm denotes the minutes. The value ranges from 00 to 59. For example, the valid value is +05:30.

Fields (cont)	• DST Start Time—enter the <i>DST</i> (Daylight Saving Time) start time. The format is weekofmonth-weekofday-month, HH:MM. Where: – weekofmonth denotes the particular week. The valid values are First, Second, Third, Fourth and Last – weekofday denotes the day in the specified week. The valid values are Sun, Mon, Tue, Wed, Thu, Fri and Sat. – month denotes the month for which the specified week and day are applicable. The valid values are Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec – HH denotes the hours. It is 24-hour format with value ranging from 00 to 23. – mm denotes the minutes. The value ranges from 00 to 59. For example, the valid value is First-Sun-Jan, 23:45. NOTE: <i>DST</i> 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 <i>DST</i>, although most have their own rules and regulations for when it begins and ends. The dates of <i>DST</i> may change from year to year.
Buttons	• Apply—adds and saves a new configuration. • Refresh—refreshes the screen.

SNTP Unicast Table

Figure 6: SNTP Unicast Table

SNTP Unicast Table

Forward Address Type IPv4 ▾

Unicast ServerIp Addr *

Server Port

SNTP Version Version 3 ▾

Unicast Server Type Primary ▾

Add Reset

Select	Server Addr Type	Server Address	Server Port	Server Version	Server type	Last Updated	Tx Requests
Apply Delete Refresh							

Screen Objective	This screen allows the user to configure the details of SNTP unicast parameters.
Navigation	System > SNTP > Unicast

Fields	• Select—select the server address for which the configuration need to be modified or deleted. • Forward Address Type—select the address type of the unicast server in the Unicast addressing mode. <i>IPv4</i>—Sets the address type of the unicast server as Internet Protocol Version 4. • unicast serverip addr—enter the unicast ipv4/ipv6 server address in the unicast addressing mode. • server port—enter the <i>sntp</i> port on which the server is up. the value ranges between 123, 1025 to 65535. the default value is 123. • SNTP Version—the <i>SNTP</i> version supported by the server. The list contains: – Version 3—Sets the <i>SNTP</i> version as version 3. – Version 4— Sets the <i>SNTP</i> version as version 4. • Unicast Server Type—select the Unicast server type. This flag is to distinguish between primary and secondary server. <i>SNTP</i> client sends request to different servers until it receives successful response. This flag tells the order in which to query the servers. The list contains: – Primary—sets the unicast server type as primary server – Secondary—sets the unicast server type as secondary server • Last Updated—specifies the local time when the configuration was successful. • Tx Requests—specifies the number of <i>SNTP</i> requests sent in unicast addressing mode.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry. • Refresh—refreshes the screen.

SNTP Broadcast Configuration

Figure 7: SNTP Broadcast Configuration

SNTP Broadcast Configuration

Request InBcast Mode	Disabled ▾
POLL Timeout InBcastMode	5
Delay Time InBcastMode	8000
Primary Addr InBcast Mode	0.0.0.0
Apply	

Screen Objective	This screen allows the user to configure the details of <i>SNTP</i> Broadcast parameters.
Navigation	System > SNTP > Broadcast
Fields	• Request InBcast Mode—select the <i>SNTP</i> send request status in Broadcast mode. The default option is Disabled. The list contains: – Enabled—sends the <i>SNTP</i> request to the broadcast server to calculate the delay time. – Disabled—does not send the <i>SNTP</i> request. • POLL Timeout InBcastMode—enter the number of seconds to wait for a response from a POLL Timeout InBcast <i>SNTP</i> server before considering the attempt to have timed out. This value ranges from 1 to 30 seconds. The default value is 5 seconds. • Delay Time InBcast Mode—enter the delay time when there is no response from the broadcast server. This value ranges from 1000 to 15000 microseconds. The default value is 8000 microseconds. • Primary Addr InBcast Mode—enter the primary server IP address learnt in Broadcast addressing mode. The default address is 0.0.0.0.
Buttons	• Apply—modifies attributes and saves the changes.

SNTP Multicast Configuration

Figure 8: SNTP Multicast Configuration

SNTP Multicast Configuration

Send RequestIn	Disabled ▾
Poll timeout	5
Delay Time	8000
Group Address Type	IPv4 ▾
Group Address	224.0.1.1
Primary Server Addressing Mode	IPv4 ▾
Primary Server Address	0.0.0.0.1
Apply	

Screen Objective	This screen allows the user to configure the details of <i>SNTP</i> Multicast parameters.
Navigation	System > SNTP > Multicast
Fields	• Send Request In—the <i>SNTP</i> send request status in Multicast mode. The default option is Disabled. The list contains: – Enabled—sends the <i>SNTP</i> request to the broadcast server to calculate the delay time. – Disabled—does not send the <i>SNTP</i> request. • Poll timeout—enter the number of seconds to wait for a response from a <i>SNTP</i> server before considering the attempt to have timed out. This value ranges from 1 to 30 seconds. The default value is 5 seconds. • Delay Time—enter the delay time when there is no response from the multicast server. This value ranges from 1000 to 15000 microseconds. The default value is 8000 microseconds. • Group Address Type—select the multicast group address type that can be configured by the administrator. <i>IPv4</i> sets the multicast group address type as Internet Protocol Version 4. • Group Address—enter the multicast group address that can be configured by the administrator. • Primary Server Addressing Mode—select the address type of the primary server learnt in Multicast addressing mode. The list contains. • Primary Server Address—displays the primary server IP address learnt in Multicast addressing mode. This is a read-only field. The default address is 0.0.0.0.
Buttons	• Apply—modifies attributes and saves the changes.

SNTP Multicast Configuration

Figure 9: SNTP Multicast Configuration

SNTP Multicast Configuration

Poll Interval	64
Poll timeout	5
Poll Retry	3
Server Type	BroadCast
Group Address Type	
Group Address	0.0.0.0
Primary Server Address Type	
Primary Server Address	0.0.0.0
Apply	

Screen Objective	This screen allows the user to configure the details of <i>SNTP</i> Multicast parameters.
Navigation	System > SNTP > Multicast
Fields	• Poll Interval—enter the time period in seconds between successive <i>SNTP</i> request transmissions. This value ranges from 16 to 16284. The default value is 64. • Poll timeout—enter the number of seconds to wait for a response from a <i>SNTP</i> server before considering the attempt to have timed out. This value ranges from 1 to 30 seconds. The default value is 5 seconds. • Poll Retry—enter the time period in times to retry a request to a <i>SNTP</i> server that has not successfully responded. This value ranges from 0 to 10 with a default of 3. • Server Type—select the type of servers used in Multicast addressing mode, that is to find a Multicast server the client can send the request to either broadcast or multicast address. The default option is Broadcast. The list contains: – Broadcast—configures <i>SNTP</i> broadcast server address in Multicast mode. – Multicast—configures <i>SNTP</i> multicast server address in Multicast mode. • Group Address Type—select the Multicast group address type to be configured. <i>IPv4</i>—sets the Multicast group address type as Internet Protocol Version 4. • Group Address—enter the Multicast group address to be configured.

Fields	• Primary Server Address Type—select the address type of the primary server learnt in Multicast addressing mode. <i>IPv4</i> sets primary server address type as Internet Protocol Version 4. • Primary Server Address—displays the primary server IP address learnt in Multicast addressing mode. This is a read-only field. The default address is 0.0.0.0.
Buttons	• Apply—modifies attributes and saves the changes.

Interfaces Map

6. Interfaces to the RAPTOR

This section introduces WebUI pages that configure interfaces to the RAPTOR such as SSH, HTTP, SSL, and SNMP.

6.1. SSH

This section describes how to configure the *SSH* protocol.

SSH (secure shell) is a network protocol that allows data to be exchanged using a secure channel between two networked devices. *SSH* uses public-key cryptography to authenticate the remote computer and allows the remote computer to authenticate the user, if necessary. *SSH* is typically used to log into a remote machine and execute commands.

To access *SSH* screens, click **System > SSH**.

SSH Global Settings

Figure 1: SSH Global Settings

SSH Global Settings

SSH Status	Enable ▾
SSH Server Port	22
SSH CipherList	☐ ECDH_RSA_AES256_GCM_SHA256 ☐ ECDH_RSA_AES128_GCM_SHA256 ☐ ECDH_RSA_CHACHA20_POLY1305 ☐ DHE_RSA_AES256_GCM_SHA256 ☐ ECDH_ECDSA_AES128_GCM_SHA256
Trace Level	None ▾
Apply	

Screen Objective	This screen allows the user to configure the <i>SSH</i> initial settings.
Navigation	System > SSH
Fields	• SSH Status—select the status of the <i>SSH</i> module. The default option is Enabled. The list contains: – Enable—enables the <i>SSH</i> feature in the switch. <i>SSH</i> feature enables the user to log into a remote machine and execute commands. – Disable—disables the <i>SSH</i> feature in the switch. This action disconnects the secure channel. • Version compatibility is set at Version 2 and cannot be changed.
Fields	• SSH CipherList—select a Cipher-List. The cipher list takes values as bit mask. Setting a bit indicates that the corresponding cipher-list will be used for encryption. The default option is DES-CBC in NON-FIPS mode and 3DES-CBC in FIPS mode. The options are: – ECDH_RSA_AES256_GCM_SHA256 – ECDH_RSA_AES128_GCM_SHA256 – ECDH_RSA_CHACHA20_POLY1305 – DHE_RSA_AES256_GCM_SHA256 – ECDH_ECDSA_AES128_GCM_SHA256 • Trace Level—this option enables debug logging at specific levels. – None – Warning – Protocol – Packet – Functions
Buttons	• Apply—modifies attributes and saves the changes.

6.2. SSL

Describes how to configure the *SSL* protocol on the switch.

The *SSL* (Secured Socket Layers) is a protocol developed for transmitting private documents through Internet. It works by using a private key to encrypt data that is transferred over the *SSL* connection. Both Netscape Navigator and Internet Explorer support *SSL* and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. 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 is designed to authenticate the server and optionally the client. *SSL* requires a reliable transport protocol (e.g, *TCP*) for data transmission and reception.

The *SSL* Protocol is used by the subscribers of *HTTPS* protocol. *SSL* offers secured data transfer. *SSL* digital certificates are offered to merchants, banks and organizations that collect personal information from their clients. These *SSL* Certificates ensure a safe transportation of data on the inter network in a remote location. *SSL* has encouraged E-commerce, which has grown many folds in the short period of time.

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 ensuring privacy.

To access **SSL** screens, go to **System > SSL**.

The **SSL** parameters are configured through the screens displayed by the following tabs:

[SSL Global Settings](#)

[SSL Digital Certificate](#)

SSL Global Settings

By default, the tab **SSL Global Settings** displays the **SSL Global Settings** screen.

Figure 2: SSL Global Settings

SSL Global Settings

HTTPS Server

Enable

HTTPS Port

443

Minimum SSL Version

TLSv1.2

HTTPS TLSv1.2 Ciphers

☒ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

☒ TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

HTTPS TLSv1.3 Ciphers

☒ TLS_AES_256_GCM_SHA384

☒ TLS_CHACHA20_POLY1305_SHA256

☒ TLS_AES_128_GCM_SHA256

Apply

Note : Please **Refresh** the page after configuration.

Screen Objective	This screen allows the user to configure <i>SSL</i> server on the device and also configures Ciphersuites.
Navigation	System > SSL > SSL Global Settings

Fields	• HTTPS Server—select the status of the <i>HTTP</i> secure server. The default option is Disable. The list contains: – Enable—Enables secure <i>HTTP</i> in the system. When the server status is enabled it establishes the secure layer in the network. – Disable—Disables <i>HTTP</i> secure server on the device and also disables Ciphersuites. • HTTPS Port—Specify the port for the <i>HTTP</i> secure server to listen on. The standard for this is 443, but a different port may be used. • Minimum SSL Version—select the protocols to configure the <i>SSL</i> version. The default minimum option is TLSv1.2. The list contains: – TLSv1.2—Sets the sets the minimum TLS version as 1.2. – TLSv1.3—Sets the sets the minimum TLS version as 1.3.
Fields (cont)	• HTTPS TLSv1.2 Ciphers—select the cipher suite from the list for providing the input. When an <i>SSL</i> connection is established, the client and server exchange information about which cipher suites they have in common. By default all supported ciphers are enabled. The options are: – TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 NOTE: The encryptions use these combinations to send /receive data in a secure manner. • HTTPS TLSv1.3 Ciphers—select the cipher suite from the list for providing the input. When an <i>SSL</i> connection is established, the client and server exchange information about which cipher suites they have in common. By default all supported ciphers are enabled. The options are: – TLS_AES_256_GCM_SHA384 – TLS_CHACHA20_POLY1305_SHA256 – TLS_AES_128_GCM_SHA256 NOTE: The encryptions use these combinations to send /receive data in a secure manner.
Buttons	• Apply—modifies attributes and saves the changes.

SSL Digital Certificate

Figure 3: SSL Digital Certificate - Part A

SSL Digital Certificate

☒ Generate New Key and Self Signed Certificate

RSA Key Size

Country (C)

State/Province (S)

City/Locality (L)

Organization (O)

Organizational Unit (OU)

Common Name (CN)

☐ Generate Certificate Signing Request

☐ Enter Certificate Signed By Certification Authority

Figure 4: SSL Digital Certificate - Part B

☒ Enter Certificate Signed By Certification Authority

-----BEGIN CERTIFICATE REQUEST-----
MIHKMHYCAQAWEETEPMAOGA1UEAxMGc2FtcGx1MFwwDQYJKoZIhvcNAQEBBQADSwAw
wSAJBAMmxOVPXluZhtx8GelrH7o0OuAbnpY01DdxjRVERJ3msZRwOMu4gjGJv8yj
/
fgAKKqmJB7yS+uSFU7BZL2x4JyOCAwEAAaAAMAOGCSqGS Ib3DQEBAUAAOEAW8g
S
1Xd6hX/jtIwtErkDO7wHt/5ynABoTCnhY06jpQOI0y0ZDwppi6uzsf96lpD5sKi
q
R5LGkgO8v1uRUdYipw==

Screen Objective	This screen allows the user to configure the server-certificate input in PEM format. It imports the public certificate of the <i>SSL</i> server. When the <i>SSL</i> server certificate installation is complete, <i>SSL</i> server sends this certificate for authentication of client. <i>SSL</i> digital certificates are offered to merchants, banks and organizations that collect personal information from their clients. These <i>SSL</i> Certificates ensure a safe transportation of data on the inter network in a remote location. <i>SSL</i> has encouraged E-commerce, which has grown many folds in the short period of time. A 4 byte integer is used for enabling the level of tracing. Each bit in the 4 byte integer represents a particular level of trace. System errors such as memory allocation failures are communicated using LOG messages and TRACE messages. Interface errors and protocol errors are communicated using TRACE messages.
Navigation	System > SSL > SSL Digital Certificate
Fields	• Generate Certificate Signing Request—select the traces for which debug statements will be generated. The options are: – RSA Key Size—select the desired key size. The list contains: • 2048—Sets the key size to 2048. – Country—enter the country of the user. – State/Province—enter the state and province of the user. – City/Locality—enter the city of the user. – Organization—enter the organization of the user. – Organizational Unit—enter the organizational unit/department of the user. – Common Name—enter the details of the user requesting for the Digital Certificate. NOTE: The common name is enabled only if the Generate Certificate Signing Request option is selected. Otherwise, it is grayed out and cannot be configured. • Enter Certificate Signed by Certification Authority—select to enter Certificate signed by Certification Authority (CA). The user manually enters the details of the certificate.
Buttons	• Apply—modifies attributes and saves the changes.

Notes on Digital Certificates

In order to have the device participate in a public key infrastructure, a *CSR* (Certificate Signing Request) must be generated. This signing request is in *PEM* format. The *CSR* contains information such as the common name, which is the fully qualified domain name that the certificate will be used for, the public key of the device and key length. When the *CSR* is provided to the Certificate Authority (CA), the CA will respond with a signed certificate. If the response is in *CRT* format, it must be converted back to *PEM* before it can be uploaded to the device.

Once the new certificate has been uploaded to the device, the *HTTPS* service must be disabled and then re-enabled for the new certificate to be used by the web server.

6.3. HTTP

Describes how to enable/disable the *HTTP* server as well as how to configure its authentication schemes.

The *HTTP* (Hyper Text Transfer Protocol) 1.1 Server provides an *HTTP* Authentication framework in addition to the proprietary form-based authentication. The *HTTP* authentication framework provides a simple challenge-response authentication mechanism that is used by a server to challenge a client request and by a client to provide authentication information. It uses an extensible, case-insensitive token to identify the authentication scheme, followed by a comma-separated list of attribute-value pairs which carry the parameters necessary for achieving authentication via that scheme. The *HTTP* Authentication framework supports two authentication schemes namely BASIC and DIGEST (ref. RFC 2617)

The *HTTP* related parameters are configured through the screens displayed by the following tabs:

[HTTP Settings](#)

[Web Session](#)

HTTP Settings

By default, the tab **HTTP Configuration** displays the **HTTP Settings** screen.

Figure 5: HTTP Settings

HTTP Settings

HTTP Status	Enabled ▾
Operational HTTP Authentication Scheme	Default ▾
Configured HTTP Authentication Scheme	Default ▾
Apply	

Note:

*To use the modified value of "Configured HTTP Authentication scheme", save the ISS configuration through **Save and Restore** and restart the ISS.*

Screen Objective	This screen allows the user to configure the <i>HTTP</i> related information.

NOTE: The changes in the screen are effective only after saving the configuration using **System > Save and Restore > Save > Save Configuration** screen.

Navigation	System > HTTP > HTTP Settings
Fields	• HTTP Status—it shows if <i>HTTP</i> is enabled or disabled. • Operational HTTP Authentication Scheme—displays the operational <i>HTTP</i> authentication scheme which is used to authenticate all <i>HTTP</i> sessions. The default option is Default. The options are: – Default—specifies IS5Com proprietary Form-Based authentication mechanism. – Basic—specifies Basic HTTP Authentication scheme of RFC 2617. – Digest—specifies Digest HTTP Authentication scheme of RFC 2617. NOTE: This value is set only once at the start up and cannot be modified at run-time. During the start-up, this field takes the value saved in the Configured <i>HTTP</i> Authentication scheme. • Configured HTTP Authentication Scheme—select the configurable <i>HTTP</i> authentication scheme. The modified value is stored in a configuration file and applied during the next device Startup. The default option is Default. The list contains: – Default—specifies IS5Com proprietary Form-Based authentication mechanism. – Basic—specifies Basic <i>HTTP</i> Authentication scheme of RFC 2617. – Digest—specifies Digest <i>HTTP</i> Authentication scheme of RFC 2617. NOTE: To use the modified value of Configured <i>HTTP</i> authentication scheme, save your configuration through Save and Restore link and restart the device. Also, restart the browser and clear all private data, saved session information, and cache from the browser.
Buttons	• Apply—modifies attributes and saves the changes.

Web Session

Figure 6: Web Session Timeout

Web Session TimeOut

Web Session TimeOut	300
Apply	

Screen Objective	This screen allows the user to configure the web session timeout value.
Navigation	System > HTTP > Web Session TimeOut
Fields	• Web Session Timeout—enter the web session timeout value in seconds. This value ranges from 1 to 300 in seconds. The default value is 300.
Buttons	• Apply—modifies attributes and saves the changes.

6.4. SNMP

Used to configure *SNMP* for network management services.

The *SNMP* (Simple Network Management Protocol) is a widely deployed protocol that is commonly used to monitor and manage network devices. SNMP works by sending messages, called protocol data units (*PDUs*), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (*MIBs*) and return this data to the *SNMP* requesters.

To access **SNMP** screens, go to **System > SNMP**.

The **SNMP** link also allows the user to configure SNMP Agent and AgentX parameters through the following sub-links:

[SNMP Agent Control Settings](#)

[AGENT](#)

SNMP Agent Control Settings

By default, the tab **SNMP** displays the **SNMP Agent Control Settings** screen.

Figure 7: SNMP Agent Control Settings

SNMP Agent Control Settings

☒ Agent
☐ AgentXSubagent
☐ Disable BOTH
 Snmp Agent Port

Note : Either Agent or AgentX_Subagent can be enabled.

Goto AgentXSubagent configuration page on selecting AgentXSubagent.

Screen Objective	This screen allows the <i>SNMP</i> user to configure <i>SNMP</i> Agent Control Settings
Navigation	System > SNMP > SNMP
Fields	Agent—select it to enable <i>SNMP</i> Agent. Enabling this option allows the software to directly interface with the managed modules and configure and monitor them. The default option is Enabled.
Fields	AgentX Subagent— This option is not supported, and will be removed in a future release. Disable BOTH—select Disable BOTH to disable both <i>SNMP</i> Agent and Agent X Subagent. Snmp Agent Port—enter the <i>SNMP</i> Agent Port number on which <i>SNMP</i> agent listens. This value ranges from 1 to 65535. The default value is 161. NOTE: This value can be entered only if Agent is selected. NOTE: This field is grayed for both AgentX Subagent and Disable options.
Buttons	Apply—modifies attributes and saves the changes.

AGENT

The **SNMP Agent** 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.

To access **SNMP Agent** screens, go to **System > SNMP > AGENT**.

The **SNMP AGENT** link also allows the user to configure *SNMP* Agent-related parameters through the following tabs:

[SNMP Community Settings](#)

[SNMP Group Settings](#)

[SNMP Group Access Settings](#)

[SNMP View Tree Settings](#)

[SNMP Target Address Settings](#)

[SNMP Target Parameter Settings](#)

[SNMP Filter Profile Settings](#)

[User SNMP Security Settings](#)

[SNMP Trap Manager](#)

[SNMP Filter Settings](#)

[SNMP Proxy Settings](#)

[SNMP Settings](#)

SNMP Community Settings

By default, the tab **Community** displays the **SNMP Community Settings** screen.

Figure 8: SNMP Community Settings

SNMP Community Settings

Community Index

*

Community Name

*

Security Name

*

Context Name

Transport Tag

Storage Type

Select	Community Index	Community Name	Security Name	Context Name	Transport Tag	Storage Type
☐	NETMAN	NETMAN	none			NonVolatile ▾
☒	PUBLIC	PUBLIC	none			NonVolatile ▾

Screen Objective	This screen allows the user to add a new community configuration to the table and delete existing community configuration from the same.
Navigation	System > SNMP > AGENT > Community

Fields	• Community Index—enter the Index to the community table. The communities NETMAN and PUBLIC are created. • Community Name—enter the community name. The communities NETMAN and PUBLIC are created. • Security Name—enter the security name. The default value is None. • Context Name—enter the context name. The default value is Null. • Transport Tag—enter the transport tag. The default value is Null. • Storage Type—select the required Storage Type for the community. The default option is NonVolatile. The list contains: – Volatile—sets the storage type as temporary and erases the configuration setting during restarting of the system. – NonVolatile—sets the storage type as permanent and saves the configuration to the system. The saved configuration can be viewed when restarting the system.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

SNMP Group Settings

Figure 9: SNMP Group Settings

SNMP GROUP Settings

Security Model

v1 ▾

Security Name

*

Group Name

*

Storage Type

NonVolatile ▾

Add

Reset

Select	Security Model	Security Name	Group Name	Storage Type
☐	v1 ▾	none	iso	NonVolatile ▾
☐	v2c ▾	none	iso	NonVolatile ▾
☐	v3 ▾	noAuthUser	noAuthUser	NonVolatile ▾
☐	v3 ▾	templateMD5	noAuthUser	NonVolatile ▾
☒	v3 ▾	templateSHA	noAuthUser	NonVolatile ▾

Apply

Delete

Screen Objective	This screen allows the user to configure the <i>SNMP</i> Group Settings.
Navigation	System > SNMP > AGENT > Group
Fields	Security Model—select the version of the <i>SNMP</i>. The security model v1, v2c and v3 are created. The list contains: - v1—sets the <i>SNMP</i> version as Version 1. - v2c—sets the <i>SNMP</i> version as Version 2. - v3—sets the <i>SNMP</i> version as Version 3. NOTE: Group Name and Storage Type are created. Group Name and Storage Type can be modified for the default entries. Default entries cannot be deleted.

Fields (cont)	• Security Name—enter the security name of the group. Security names such as none, noAuthUser, templateMD5, and templateSHA are created. This is a read-only field. • Group Name—enter the name of the <i>SNMP</i> group. The <i>SNMP</i> groups iso and initial are created. • Storage Type—select the required storage type for the group entry. The default option is NonVolatile. The list contains: – Volatile—sets the storage type as temporary and erases the configuration setting during restarting of the system. – Non-Volatile—sets the storage type as permanent and saves the configuration to the system. The Saved configuration can be viewed when restarting the system.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

SNMP Group Access Settings

Figure 10: SNMP Group Access Settings

SNMP Group Access Settings

Group Name *

Security Model

Security Level

Read View

Write View

Notify View

Storage Type

Select	Group Name	Context Prefix	Security Model	Security Level	Read View	Write View	Notify View	Storage Type
☐	iso		v1	NoAuthentication	iso	iso	iso	NonVolatile
☐	iso		v2c	NoAuthentication	iso	iso	iso	NonVolatile
☐	noAuthUser		v3	NoAuthentication	restricted	restricted	restricted	NonVolatile
☐	noAuthUser		v3	Authentication	iso	iso	iso	NonVolatile
☒	noAuthUser		v3	Private	iso	iso	iso	NonVolatile

Screen Objective

This screen allows the user to configure the *SNMP* Group Access Settings.

NOTE: A *SNMP* Group has to be created prior to a Group Access configuration. The groups that are created in the *SNMP* Group Access Settings section are displayed in the bottom form of this screen.

Navigation	System > SNMP > AGENT > Group Access
Fields	• Group Name—enter the name of the group. The maximum size is 32. • Security Model—select the version of the <i>SNMP</i>. The versions are: – v1—sets the <i>SNMP</i> version as Version 1. – v2c—sets the <i>SNMP</i> version as Version 2. – v3—sets the <i>SNMP</i> version as Version 3. • Security Level—select the version of the <i>SNMP</i>. The list contains: – NoAuthentication—sets no authentication. – Authentication—enables Message digest (<i>MD5</i>) or Secure Hash Algorithm (<i>SHA</i>) packet authentication. – Private—sets both authentication and privacy. • Read View—enter the Read View identifier from which the user can read the data. The maximum size is 32 characters. • Write View—enter the Write View identifier from which the user has both read and write access. The maximum size is 32 characters. • Notify View—enter the Notify View identifier. From this identifier number, the changes made will be noted and sent to a destination through a tag. The maximum size is 32 characters. • Storage Type—select the required storage type for the group access entry. The list contains: – Volatile—sets the storage type as temporary and erases the configuration setting during restarting of the system. – NonVolatile—sets the storage type as permanent and saves the configuration to the system. The Saved configuration can be viewed when restarting the system.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

SNMP View Tree Settings

Figure 11: SNMP View Tree Settings

SNMP ViewTree Settings

View Name		*
SubTree		*
Mask		
View Type	Excluded	▼
Storage Type		▼
Add Reset		

Select	View Name	SubTree	Mask	View Type	Storage Type
☐	iso	1	1	Included ▼	NonVolatile ▼
☒	restricted	1	1	Included ▼	NonVolatile ▼

Screen Objective	This screen allows the user to configure the <i>SNMP</i> Group Access Settings.
NOTE: SNMP Group has to be created and <i>SNMP</i> Access settings need to be defined prior to the Group View Tree configuration.	
Navigation	System > SNMP > AGENT > View
Fields	• View Name—enter the view name for which the view details are to be configured. The default option is ISO and restricted. The view name iso and restricted are created. • SubTree—enter the sub tree value for the particular view. The default value is 1. • Mask—enter the mask value for the particular view. The default value is 1. • View Type—select the view type. The default option is Included The list contains: – Included—allows access to the subtree. – Excluded—denies access to the subtree.

Fields	• Storage Type—select the required storage type for the view tree entry. The default option is NonVolatile. The list contains: – Volatile—sets the storage type as temporary and erases the configuration setting during restarting of the system. – NonVolatile—sets the storage type as permanent and saves the configuration to the system. The saved configuration can be viewed when restarting the system.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

SNMP Target Address Settings

Figure 12: SNMP Target Address Settings

SNMP Target Address Settings

Target Name *
 Target IP Address *
 Port *
 Transport Tag
 Param *
 Storage Type ▾

Select	Target Name	Target IP Address	Port	Transport Tag	Param	Storage Type
☒	test	172.16.19.50	162		param	NonVolatile ▾

Screen Objective	This screen allows the user to configure the <i>SNMP</i> Target Address Settings.
Navigation	System > SNMP > AGENT > Target Address
Fields	• Target Name—enter a unique identifier of the Target. The maximum size is 32 characters. • Target IP Address—enter a target address to which the generated <i>SNMP</i> notifications are sent.

Fields (cont)	• Port—enter the port number through which the generated <i>SNMP</i> notifications are sent to the target address. • Transport Tag—enter the tag identifier that is used to select the target address for the <i>SNMP</i> notifications. • Param—enter <i>SNMP</i> parameters to be used when generating messages to be sent to transport address. The maximum size is 32 characters. • Storage Type—select the required storage type for target address entry. The list contains: – Volatile—sets the storage type as temporary and erases the configuration setting during restarting of the system. – NonVolatile—sets the storage type as permanent and saves the configuration to the system. The Saved configuration can be viewed when restarting the system.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

SNMP Target Parameter Settings

Figure 13: SNMP Target Parameter Settings

SNMP Target Parameter Settings

Parameter Name *
MP Model
Security Model
Security Name *
Security Level
Storage Type

Add Reset

Configure Filter Profile

Select	Parameter Name	MP Model	Security Model	Security Name	Security Level	Storage Type
☐	internet	v2c	v2c	none	NoAuthentication	NonVolatile
☒	test1	v2c	v1	none	NoAuthentication	NonVolatile

Apply Delete

Note : To delete a Target Parameter Entry, please delete the associated **Filter Profile** Entry first.

Screen Objective	This screen allows the user to configure the <i>SNMP</i> Target Parameter Settings.
Navigation	System > SNMP > AGENT > Target Parameter
Fields	• Parameter Name—enter a unique identifier of the Target. The maximum size is 32. • MP Model—select the MP model of the <i>SNMP</i>. The default option is v2c. The list contains: – v1—sets the MP model as Version 1. – v2c—sets MP model as Version 2. – v3—sets the MP model as Version 3. • Security Model—select the version of the <i>SNMP</i>. The default option is v2c. The list contains: – v1—sets the security model as Version 1. – v2c—sets the security model as Version 2. – v3—sets the security model as Version 3. • Security Name—enter the security name used in the generation of <i>SNMP</i> messages. The default option is None. The maximum size is 32. • Security Level—select the level of security to be used when generating <i>SNMP</i> messages. The default option is NoAuthentication. The list contains: – NoAuthentication—sets no authentication. – Authentication—enables Message digest (<i>MD5</i>) or Secure Hash Algorithm (<i>SHA</i>) packet authentication. – Private—enables both authentication and privacy. • Storage Type—select the required Storage Type for target parameter entry. The list contains: – Volatile—sets the storage type as temporary and erases the configuration setting during restarting of the system. – NonVolatile—sets the storage type as permanent and saves the configuration to the system. The saved configuration can be viewed when restarting the system.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry. • Configure Filter Profile—click to access <i>SNMP</i> Filter Profile Settings screen.

SNMP Filter Profile Settings

Figure 14: SNMP Filter Profile Settings

SNMP Filter Profile Settings

Parameter Name *

Filter Profile Name *

Filter Profile Storage Type

Select	Parameter Name	Filter Profile Name	Filter Profile Storage Type
Apply Delete			

Screen Objective	This screen allows the user to configure the <i>SNMP</i> Filter Profile Settings.
Navigation	System > SNMP > AGENT > Target Parameter > SNMP Target Parameter Settings Click Configure Filter Profile
Fields	• Parameter Name—select the existing parameter name to which the filter profile setting should be assigned. • Filter Profile Name—enter the name for the filter profile. This name is used when generating notifications using the corresponding entry in the target address table. This value is a string with maximum size of 32 characters. • Filter Profile Storage Type—select the required storage type for filter profile entry. The list contains: – Volatile—sets the storage type as temporary and erases the configuration setting during restarting of the system. – NonVolatile—sets the storage type as permanent and saves the configuration to the system. The Saved configuration can be viewed when restarting the system.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry. • Configure Target Parameter—click to access <i>SNMP</i> Target Parameter Settings screen.

User SNMP Security Settings

Figure 15: SNMP Security Settings

SNMP Security Settings

Engine ID *

User Name *

Authentication Protocol ▾

Authentication Key

Privacy Protocol ▾

Privacy Key

Storage Type ▾

Select	Engine Id	User Name	Authentication Protocol	Private Protocol	Storage Type
☐	80:00:08:1c:04:46:53	noAuthUser	No Authentication ▾	No Privacy ▾	NonVolatile ▾
☐	80:00:08:1c:04:46:53	templateMD5	HMAC-MD5 ▾	No Privacy ▾	NonVolatile ▾
☒	80:00:08:1c:04:46:53	templateSHA	HMAC-SHA ▾	AES ▾	NonVolatile ▾

Screen Objective	This screen allows the user to configure the <i>SNMP</i> Security Settings.
Navigation	System > SNMP > AGENT > User
Fields	Engine ID—enter the global SNMP engine id. The value is an octet string with maximum size of 5 to 32 octets, e.g., 80:00:08:1c:04:46:53. NOTE: This value is used only for identification and not for addressing. This value be read from iS5Comnvram.txt file or from System > NVRAM Settings > Factory Default Settings screen during system initialization. User Name—enter the user name which is the User-based Security Model dependent security ID. Authentication Protocol—select the type of authentication protocol used for authentication. The default option is No Authentication. The list contains: - No Authentication—sets the authentication status as no authentication required. - HMAC-MD5—sets the <i>MD5</i> based authentication. - HMAC-SHA—sets the <i>SHA</i> based authentication. Authentication Key—enter the secret authentication key used for messages sent on behalf of this user to/from the <i>SNMP</i>. This value is a string with maximum size of 40.

Fields (cont)	• Privacy Protocol—select the type of protocol to be is used in this case. The default option is No Privacy. The list contains: – No Privacy—sets no privacy. – DES—sets the privacy protocol as Data Encryption Standard (<i>DES</i>). This protocol provides an algorithm to encrypt PPP encapsulated packets. – AES—sets the privacy protocol as Advanced Encryption Standard (<i>AES</i>). • Privacy Key—enter the privacy key. The messages sent on behalf of a user to/from the <i>SNMP</i>, can be protected from disclosure. This value is a string of maximum size of 32 characters. • Storage Type—select the required storage type for target parameter entry. The list contains: – Volatile—sets the storage type as temporary and erases the configuration setting during restarting of the system. – NonVolatile—sets the storage type as permanent and saves the configuration to the system. The Saved configuration can be viewed when restarting the system.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

SNMP Trap Manager

Figure 16: SNMP Trap Settings

SNMP Trap Settings

Notify Name *
 Notify Tag *
 Notify Type Trap ▾
 Storage Type NonVolatile ▾

Select	Notify Name	Notify Tag	Notify Type	Storage Type
☐	iss	iss	Trap ▾	NonVolatile ▾
☒	iss1	iss1	Trap ▾	NonVolatile ▾

Screen Objective	This screen allows the user to configure set of management targets for receiving notifications.
Navigation	System > SNMP > AGENT > Trap Manager
Fields	• Notify Name—enter a unique identifier associated with the entry. The maximum size is 32 characters. • Notify Tag—enter the notification tag used to select entries in the Target Address Table. The maximum size is 32 characters. • Notify Type—select the notification type. The list contains: – Trap—allows routers to send traps to <i>SNMP</i> managers. Trap is a one-way message from a network element such as a router, switch or server to the network management system. – Inform—allows routers / switches to send inform requests to SNMP managers. • Storage Type—select the required storage type for trap settings entry. The list contains: – Volatile—sets the storage type as temporary and erases the configuration setting during restarting of the system. – NonVolatile—sets the storage type as permanent and saves the configuration to the system. The saved configuration can be viewed when restarting the system.

Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

SNMP Filter Settings

Figure 17: SNMP Filter Settings

SNMP Filter Settings

Profile Name

*

SubTree

*

Mask

Filter Type

Excluded

▼

Storage Type

▼

Add

Reset

Select

FilterProfile Name

SubTree

Mask

Filter Type

Storage Type

Apply

Delete

Screen Objective	This screen allows the user to configure the notification filters used to determine whether the management target should receive a particular notification. The generated notification is compared with filters associated with each management target to determine the target to which the notification is to be sent.
Navigation	System > SNMP > AGENT > Filter Conf

Fields	• Profile Name—enter the filter profile name that should be used during generating notifications. This value is a string with maximum size of 32 characters. NOTE: The profile name should have been already created through <i>SNMP</i> Filter Profile Settings screen. • SubTree—enter the MIB subtree that is combined with corresponding instance of mask to define a family of subtrees which are included in or excluded from the filter profile. • Mask—enter the bit mask that is combined with MIB subtree to define a family of subtrees. This is an octet string with a maximum size of 16 characters. • Filter Type—select the type of filter to be applied for the filter entry. The default option is included. The list contains: – Included—indicates that the family of filter subtrees is defined using MIB subtree and a bit mask is included in a filter. – Excluded—indicates that the family of filter subtrees is defined using MIB subtree and a bit mask is excluded from a filter.
Fields (cont)	• Storage Type—select the required Storage Type for trap settings entry. The list contains: – Volatile—sets the storage type as temporary and erases the configuration setting during restarting of the system. – NonVolatile—sets the storage type as permanent and saves the configuration to the system. The Saved configuration can be viewed when restarting the system.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

SNMP Proxy Settings

Figure 18: SNMP Proxy Settings

SNMP PROXY Settings

Proxy Name

*

Proxy Type

Read

▼

Proxy Context Engine ID

*

Proxy Context Name

Proxy TargetParamIn

*

Proxy SingleTargetOut

*

Proxy MultipleTargetOut

*

Proxy Storage Type

▼

Add

Reset

Select	Proxy Name	Proxy Type	Proxy ContextEngineID	Proxy ContextName	Proxy TargetParamIn	Proxy SingleTargetOut	Proxy MultipleTargetOut	Proxy Storage Type
Apply Delete								

Screen Objective

This screen allows the user to configure the configure translation parameters for forwarding SNMP messages.

Navigation

System > SNMP > AGENT > Proxy

Fields

- Proxy Name**—enter the unique proxy name that identifies an entry in the proxy table.This value is a string with maximum size of 32 characters.

Fields (cont)	• Proxy Type—select the type of message to be forwarded using the translation parameters defined by proxy entry. The list contains: – Read—read messages are forwarded to get the request from the manager. – Write—write messages are forwarded to set configurations. – Inform—notification messages are forwarded to the agent. – Trap—SNMP trap messages are forwarded to the agent • Proxy Context Engine ID—enter the context engine ID of the agent with whom the manager communicates through the proxy. • Proxy Context Name—enter a unique context name for an <i>SNMP</i> sub agent. This name is used to identify the corresponding sub agent when more than one sub agent exists. • Proxy TargetParamIn—enter the <i>SNMP</i> version that the manager sends as request to the proxy. • Proxy Single TargetOut—enter the <i>SNMP</i> version that the proxy uses to communicate with the agent. • Proxy Multiple TargetOut—enter the <i>SNMP</i> version that the proxy uses to communicate with multiple agent. • Proxy Storage Type—select the required Storage Type for the proxy. The list contains: – Volatile—the configuration is lost after the switch is rebooted, even if the entry is saved. – Non-Volatile—the configuration is available even after the switch is rebooted if the entry is saved
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

SNMP Settings

Figure 19: SNMP Settings

SNMP Settings

snmpEnableAuthenTraps	Disabled ▾
snmpListenTcpTrapPort	162
snmpTrapOverTcpStatus	Disabled ▾
snmpOverTcpStatus	Disabled ▾
snmpProxyListenTrapPort	162
snmpListenTrapPort	162
snmpListenTcpPort	161
Apply	

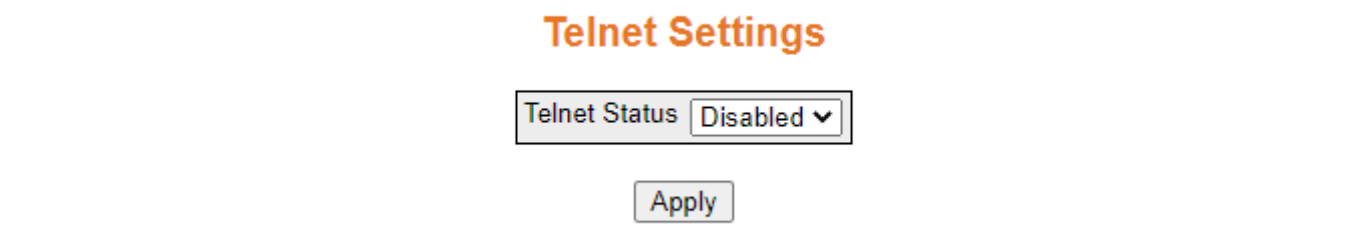
Screen Objective	This screen allows the user to configure <i>SNMP</i> scalar parameters which are independent of each other.
Navigation	System > SNMP > AGENT > Proxy
Fields	• snmpEnableAuthenTrap—select the status of the authentication failure traps. The list contains: – Enabled—enables generation of authentication failure traps. – Disabled—disables generation of authentication failure traps • snmpListenTcpTrapPort—enter the port number on which <i>SNMP</i> trap message are sent to the manager over TCP. The default value is 162. • snmpTrapOverTcpStatus—select the status of sending <i>SNMP</i> trap messages over TCP. The list contains: – Enables—allows sending of <i>SNMP</i> trap messages over TCP. – Disables—blocks sending of <i>SNMP</i> trap messages over TCP • snmpOverTcpStatus—select the status of sending <i>SNMP</i> messages over TCP. The list contains: – Enables—allows sending of <i>SNMP</i> messages over TCP. All <i>SNMP</i> messages are sent over TCP instead of UDP. – Disables—blocks sending of <i>SNMP</i> messages over TCP. • snmpProxyListenTrapPort—enter the port number on which proxy listens for trap and inform messages from the agent. The default value is 162. • snmpListenTrapPort—enter the port number on which <i>SNMP</i> trap messages are sent to the manager. The default value is 162. • snmpListenTcpPort—enter the port number on which <i>SNMP</i> trap messages are sent to the manager over TCP. The default value is 161.
Buttons	• Apply—modifies attributes and saves the changes.

6.5. Telnet

This section describes how to enable *Telnet*.
The *Telnet* networking protocol is used to provide a command line interface to a remote host. For security reasons, *SSH* is the preferred method of gaining command line access and is replacing Telnet.

Telnet Settings

Figure 20: Telnet Settings



Screen Objective	This screen allows the user to enable or disable the <i>Telnet</i> interface.
Navigation	System > Telnet
Fields	Telnet Status drop-down option may be used to enable or disable the <i>Telnet</i> interface.
Buttons	Apply—modifies attributes and saves the changes.

7. Syslog

This section describes how to configure all Syslog-related parameters.

The **Syslog** is a standard for logging program messages. It separates the software that generates and stores messages from the software that reports and analyze them.

Syslog is a protocol used to capture log information from the devices on a network. This protocol provides a transport for allowing a machine to send event notification messages across IP networks to event message collectors, also known as Syslog servers. This protocol is simply designed to transport the event messages.

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.

To access **SYSLOG Settings** screens, go to **System > SYSLOG**.

In the figure below, click the hyperlink **BSD SYSLOG**.

BSD stands for Berkeley Software Distribution (BSD) at University of California where this protocol has been originally developed.

Figure 1: SYSLOG Settings



7.1. BSD Syslog

To access **SYSLOG Settings** screens, go to **System > SYSLOG > BSD SYSLOG**

Syslog-related parameters are configured through the screens displayed by the following tabs:

[BSD Syslog Settings](#)

[BSD Syslog File Table](#)

[BSD Syslog Mail Table](#)

[BSD Syslog Forward Table](#)

By default, the tab **Syslog Settings** displays the **BSD Syslog Settings Configuration** screen.

Figure 2: BSD Syslog Settings

BSD Syslog Settings

Syslog Role	Relay ▾
SyslogFile Status	Enabled ▾
SyslogMail Status	Disabled ▾
SMTP Sender Mail Id	Reset
Syslog Profile	Raw ▾
Syslog FileName One	is5
Syslog FileName Two	
Syslog FileName Three	
Syslog Snmp Trap	Enabled ▾
Syslog Relay Port	514
Syslog Relay Transport Type	UDP ▾
Syslog Authentication Type	No Authentication ▾
Apply	

7.2. BSD Syslog Settings

Screen Objective	This screen allows the user configure the <i>BSD</i> Syslog settings.
Navigation	System > SYSLOG > BSD SYSLOG > Syslog Settings

Fields	• Syslog Role—select Syslog Role. The default option is Device. The list contains: – Device—sets the syslog role as Device. This generates and forwards the syslog messages. – Relay—sets the role as Relay. This receives, generates, and forwards the syslog messages. It checks if the received packet is as per <i>BSD</i> Syslog format, and if it is not, the message is made to <i>BSD</i> Syslog format and then forwarded. • SyslogFile Status—select the status of the syslog storage. When enabled, the syslog messages are stored in a file (as configured by admin). The default option is Disabled. The list contains: – Enabled—enables the syslog local storage option. – Disabled—disables the syslog local storage option. • SyslogMail Status—select the status of syslog mail storage in the system. Syslog supports sending syslog message to any mail-id as configured by the admin. The default option is Disabled. The list contains: – Enabled—enables the syslog mail storage option. When enabling syslog mail storage, the device sends the Syslog messages as mail messages to the mail-server configured in the system. – Disabled—disables the syslog mail storage option.

Fields (cont)	• SMTP Sender Mail Id—enter the sender mail ID to which email alerts should be sent using SMTP. The user can customize to add support for specific event for which email alerts should be sent. This maximum length is 100. The default value is syslog@is5com.com. • Syslog Profile—select the status of the syslog storage. When enabled, the syslog messages are stored in a file (as configured by admin). The default option is Disabled. The list contains – Raw—sets the syslog profile as Raw which is the profile for the transport type beep. – Cooked—sets the syslog profile as Cooked. • Syslog FileName One—enter the first file where the syslog can store the messages locally in three different files. This scalar is to get the file name. This is a string with maximum size of 32. • Syslog FileName Two—enter the first file where the syslog can store the messages locally in three different files. This scalar is to get the file name. This is a string with maximum size of 32. • Syslog FileName Three—enter the first file where the syslog can store the messages locally in three different files. This scalar is to get the file name. This is a string with maximum size of 32. • Syslog Relay Port—enter the syslog port on which the relay listens irrespective of the transport type. The relay opens the socket and listens on the configured port. This value ranges from 0 to 65535. The default value is 514. • Syslog Snmp Trap—select the status for generating Syslog server up/ down traps when connectivity fails. The default option is Enabled. The list contains: – Enabled—enables the Syslog <i>SNMP</i> Traps. This generates trap whenever connectivity to the external server collecting logs is lost. – Disabled—disables the Syslog <i>SNMP</i> Traps. This does not generate Syslog <i>SNMP</i> server up or down traps • Syslog Relay Transport Type—select the transport type to be used to send syslog messages. The default option is <i>UDP</i>. The list contains: – <i>UDP</i>—sets the relay transport type as <i>UDP</i> i.e. receiving syslog messages through <i>UDP</i> socket. <i>TCP</i>—sets the relay transport type as <i>TCP</i> i.e. receiving syslog messages through <i>TCP</i> socket.

Fields (cont)	• Syslog Authentication Type—select the authentication mode to be used for sending email alerts to the mail server configured. The default option is No Authentication. The list contains: – No Authentication—sets the <i>SMTP</i> authentication mode as No Authentication, where email alerts are sent without authentication. – AUTH LOGIN—sets the <i>SMTP</i> authentication mode as AUTH LOGIN in which both the user name and password are BASE64 encoded—email alerts are sent after authenticating the user – AUTH PLAIN—sets the authentication mode as AUTH PLAIN in which the authentication is done by sending the BASE64 encoded username and password in a single statement—email alerts are sent after authenticating the user. – CRAM MD5—sends 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 <i>SMTP</i> server original challenge as the message—E-mail alerts are sent after authenticating the user. – DIGEST MD5—sets the <i>SMTP</i> 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, and where email alerts are sent after authenticating the user.
Buttons	• Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes

7.3. BSD Logging Settings

Figure 3: BSD Logging Settings

BSD Logging Settings

Number of Log Buffers	200
Console Log	Disable ▾
Logging Facility	Local0 ▾
Logging Severity	Critical ▾
Syslog Logging	Enable ▾
Logs	☐ Clear
Apply	

Screen Objective	This screen allows the user configure the BSD Logging. This screen lists several parameters, such as logging severity. All parameters are related to the configuration of logging mechanism of Syslog and email alert messages in the local system.
Navigation	System > SYSLOG > BSD SYSLOG > Logging

Fields	• Number of Log Buffers—enter the number of logs and email alert messages that can be stored in a local buffer for the syslog messages. This value ranges from 1 to 200. The default value is 50. • Console Log—select the option to set the status of console log. This enables or disables the logs and email alert messages to be displayed in the console while being sent to the server. The default option is Enable. The list contains: – Enable—enables the console Log option. This sends the log and email alert messages to the server and it will be displayed in the console as well. – Disable—disables the console log option. This sends the log and email alert messages to the server alone and it will not be displayed in the console. • Logging Facility—select the facility level used for storing the logs and email alert messages. The facility refers to different general classification of the messages. The default option is Local0. The list contains: – Local0—specifies that it is reserved for local use facility – Local1—specifies that it is reserved for local use facility – Local2—specifies that it is reserved for local use facility – Local3—specifies that it is reserved for local use facility – Local4—specifies that it is reserved for local use facility – Local5—specifies that it is reserved for local use facility – Local6—specifies that it is reserved for local use facility – Local7—specifies that it is reserved for local use facility • Logging Severity—select the facility level used for storing the logs and email alert messages. The facility refers to different general classification of the messages. The default option is Local0. The list contains: – Emergency—sets the severity level as emergency where the messages can be logged during panic condition. – Alert—sets the severity level as alert where the messages require immediate attention. – Critical—sets the severity level as critical where the messages represent critical error. – Error—sets the severity level as error where t error messages can be logged. – Warning—sets the severity level as warning i.e. warning messages can be logged. – Notice—sets the severity level as notice or where the log messages represent significant condition but not errors. – Info—sets the severity level as info or where informational messages can be logged. – Debug—sets the severity level as debug or where the debug messages can be logged.

Fields (cont)	• Syslog Logging—select the status of syslog logging. The default option is Enable. The list contains: – Enable—enables the syslog feature in the system. The syslog messages and email alert messages are logged in the system. – Disable—disables the syslog feature in the system. The syslog messages and email alert messages are not logged in the system. • Logs—add a check mark to clear/delete the logs buffered in the system. By default, the check box is not selected. NOTE: Once the buffered logs are cleared, the check box changes to default status (i.e. the check box is not selected).
Buttons	• Apply—modifies attributes and saves the changes

7.4. BSD Syslog File Table

Figure 4: BSD Syslog File Table

BSD Syslog File Table

File Priority *
 File Name *

Select	Priority	FileName
☐	128	is5
☒	129	is5

Screen Objective	This screen allows the user configure the BSD syslog file table settings.
Navigation	System > SYSLOG > BSD SYSLOG > File Table
Fields	• File Priority—enter the priority for which the log messages should be written in file. This value ranges from 0 to 191, where 0 is considered the lowest priority and 191 is the highest priority. • File Name—enter the file name in which the syslog message should be written. NOTE: The file name should be one of the file names configured in BSD Syslog Setting screen.
Buttons	• Add—adds and saves a new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Delete—deletes the selected entry.

7.5. BSD Syslog Mail Table

Figure 5: BSD Syslog Mail Table

Syslog MailTable

Mail Priority		*
Server Address Type	IPv4	▼
Server Address		*
Mail ID		*
User Name	admin	
Password	•••••	
Create Reset		

Note : For Syslog Mail Server, **BSD Syslog Settings** Syslog Mail should be enabled and SMTP Sender Mail ID should be configured.

Select	Mail Priority	Server Address Type	Server Address	Mail Id	UserName	Password
Apply Delete						

Screen Objective	This screen allows the user configure the <i>BSD</i> syslog mail table settings.
Navigation	System > SYSLOG > BSD SYSLOG > Mail Table
Fields	• Mail Priority—enter the priority for the mail-server for mailing the mail. This value ranges from 0 to 191. • Server Address Type—select the mail server address type. <i>IPv4</i> stands for Server Address Type of Internet Protocol Version 4. • Server Address—enter the mail server IP; the IP address can be <i>IPv4</i> or <i>IPv6</i>. • Mail ID—enter the receiver mail ID. This is a string with maximum size of 100. • User Name—enter the distinguished user name of the account in the mail server to which the mails to be sent. The user name is used only if an authentication method is configured for the system. This is a string with maximum size of 64. NOTE: When Syslog Authentication Type is set as No Authentication, the user name is not used while sending mails. • Password—enter 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 is a string with maximum size of 64. NOTE: When Syslog authentication type is set as No Authentication, the password is not used while sending mails.
Buttons	• Create—adds and saves a new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes. • Delete—deletes the selected entry.

7.6. BSD Syslog Forward Table

Figure 6: BSD Syslog Forward Table

Syslog Forward Table

Forward Priority *
 Forward Address Type IPv4 ▾
 Server Ip Address *
 Forward Port
 Forward Transition Type SYSLOG_UDP ▾

Select	Forward Priority	Forward Address Type	Server Ip Address	Forward Port	Forward TransType
Apply Delete					

Screen Objective	This screen allows the user configure the <i>BSD</i> Syslog Forward table settings.
Navigation	System > SYSLOG > BSD SYSLOG > Forward Table
Fields	• Forward Priority—enter the priority at which the syslog messages are to be forwarded to the desired server. This value ranges from 0 to 191.0 is considered as the lowest priority and 191 is the highest priority. • Forward Address Type—select the address type for the server at which the syslog messages need to be forwarded. <i>IPv4</i> stands for Server Address Type of Internet Protocol Version 4. • Server IP Address—enter the server IP to which the syslog messages are to be forwarded. • Forward Port—enter the port through which the syslog message can be forwarded. This value ranges from 0 to 65535. The default value is 514. • Forward Transition Type—select the transport type by which the syslog message can be forwarded. The default option is SYSLOG_UDP. The list contains: – SYSLOG_UDP—sets the forward transition type as SYSLOG_UDP – SYSLOG_TCP—sets the forward transition type as SYSLOG_TCP
Buttons	• Create—adds and saves a new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes. • Delete—deletes the selected entry.

8. Port Manager

The **Port Manager** link helps to configure parameters of the ports such as *MTU*, *IP* specific configuration, and *WAN* interface specific configuration such as maximum burst size.

To access **Port Manager** screens, go to **Layer 2 Management > Port Manager**.

The **Port Manager** link parameters are configured through the screens displayed by the following tabs:

[Port Basic Settings](#)

[VLAN Traffic Class Mapping](#)

[Port Control](#)

[Storm Control](#)

[Port Role](#)

8.1. Welcome to Layer 2 Management Page

By default, the tab **Basic Settings** displays the **Port Basic Settings** screen.

NOTE: **Port Manager** is the first option from the **Layer 2 Management** features. The **Welcome to the Layer 2 Management Page** is as shown below.

Figure 1: Welcome to the Layer 2 Management Page

Welcome to the Layer 2 Management Page

The various Layer 2 features of the iS5com can be configured through the links available in this page.

Through the [Port Manager](#) link you can configure the Port settings related to all the physical ports in a the switch, the mirroring feature, the traffic class associated with each priority class.

Through the [VLAN](#) link you can view the mode in which the VLAN is operating and other basic information. Also you can configure the PVID settings, Static VLANS and the Dynamic Vlan status for the various ports.

Through the [GARP](#) link you can configure garp options

Through the [Dynamic VLAN](#) link you can view and Modify the Dynamic Vlan status in different Contexts and for the various ports.

Through the [MSTP](#) link you can configure the MSTP status and other related information. You can also configure the various port related information through this link.

Through the [RSTP](#) link you can configure the RSTP status and other port related information.

Through the [Link Aggregation](#) link you can configure the Link Aggregation status and the various policies that are associated with the link.

Through the [LLDP](#) link you can configure the Link Layer Discovery Protocol.

Through the [802.1x](#) link you can configure the various security information for Port based Network Access Control and Radius Client.

Through the [Filters](#) link you can configure the L2 Unicast and Multicast Filters.

Through the [Mirroring](#) link you can configure the Mirroring related information.

Through the [PVRST](#) link you can configure the PVRST status and other related information.

Through the [Split-Horizon](#) link you can configure the Uplink Failure Detection(UFD) information.

Through the [UFD](#) link you can configure the Uplink Failure Detection(UFD) information.

8.2. Port Basic Settings

Figure 2: Port Basic Settings

Port Basic Settings

Select	Port	Link Status	Admin State	Bridge Port Type	Default User Priority	SwitchPort Mode	MTU	Link Up/Down Trap	Port Type	Mac Address
☐	Gi0/1		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:82
☐	Gi0/2		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:83
☐	Gi0/3		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:84
☐	Gi0/4		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:85
☐	Gi0/5		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:86
☐	Gi0/6		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:87
☐	Gi0/7		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:88
☐	Gi0/8		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:89
☐	Gi0/9		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:8a
☐	Gi0/10		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:8b
☐	Gi0/11		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:8c
☐	Gi0/12		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:8d
☐	Gi0/13		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:8e
☐	Gi0/14		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:8f
☐	Gi0/15		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:90
☐	Gi0/16		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:91
☐	Gi0/17		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:92
☐	Gi0/18		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:93
☐	Gi0/19		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:94
☐	Gi0/20		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:95
☐	Gi0/21		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:96
☐	Gi0/22		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:97
☐	Gi0/23		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:98
☐	Gi0/24		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:99
☐	Ex0/1		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:9a
☐	Ex0/2		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:9b
☐	Ex0/3		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:9c
☒	Ex0/4		Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	e8:e8:75:90:25:9d

Screen Objective	This screen allows the user to configure general information applicable for all physical ports in a switch on port basis. All physical ports of the switch can be customized at any time.
Navigation	Layer 2 Management > Port Manager > Basic Settings

Fields	• Select—click to select the port for which the configuration needs to be done. • Port—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and port number (slot number/port number). • Link Status—displays the status of the link using graphics. The link represents a physical connection established between the switches or switch and device in a network. The graphical representation is: – Green up arrow—denotes that the link is working; that is, the physical connection established for the port is active and is ready for exchange of traffic. – Red down arrow—denotes that the link is not working; that is, no physical connection is established for the port, or the established physical connection is not active and a faulty one. • Admin State—select the desired state of the port. The default option is Up. The state changes to Up or Down state, as a result of either explicit management action or per configuration information retained by the managed system. The list contains: – Up—allows the port to transmit/receive the traffic. The port cannot transmit / receive the traffic if the Link is not working. – Down—blocks the port from transmitting/receiving the traffic. The port will not transmit / receive the traffic, even if the Link is working. – Down*—blocks the port from transmitting / receiving the traffic with some conditions. – LoopBack—sets the desired admin state as loopback. • Bridge Port Type—displays the bridge port type for the particular port. The configuration associated with the port is flushed, once the bridge port type is changed. The port type can be configured, only if the bridge mode is selected other than Customer Bridge and Provider Bridge in the Bridge Mode selection screen. The default option is CustomerBridgePort for customer bridges and as ProviderNwPort for provider core and edge bridges. The list contains: – ProviderNwPort—denotes that the port is connected to a single provider. – CustomerNwPort—denotes that the port is in the <i>S-VLAN</i> component and can transmit or receive frames for single customer. All packets received on this port are mapped to single service instance identifier by <i>PVID</i> of the port. The Acceptable Frame Type is always set as UnTagged and Priority Tagged. This bridge port type is supported only in provider bridging. – CustomerNwPortStagged—denotes that the port is in <i>S-VLAN</i> component and can transmit or receive frames for a single customer. <i>VLAN</i> classification is based on S-tag received on the interface or <i>PVID</i> of the port. The Ingress Filtering is always set as Enabled on the port.

Fields (cont)	• Bridge Port Type— The list contains (cont): – CustomerEdgePort—denotes that the port is in a <i>PCB</i> (Provider Core Bridge); that is, connected to a single customer. The packets received on this port are initially classified as a <i>CVLAN</i>. <i>CVLAN</i> classification is done based on the VID in the C-tag present in the packet or from the <i>PVID</i> 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). – PropCustomerEdgePort—denotes that the port is connected to a single customer, where multiple services can be provided based on only proprietary <i>S-VLAN</i> classification tables. <i>S-VLAN</i> classification is not done based on C-VID registration table on the port. – PropCustomerNwPort—denotes that the port is connected to a single customer, where multiple services can be provided based on <i>CVLANs</i> by assigning one of the proprietary <i>S-VLAN</i> classification tables to the port. The services can also be assigned using other proprietary <i>S-VLAN</i> classification tables, where <i>CVLAN</i> is not the index of the table. – PropProviderNwPort—denotes that the port is connected to a <i>Q-in-Q</i> bridge located inside the provider network. The port acts as a part of <i>S-VLAN</i> component. The packets to be tagged and sent out of the port contain 0x8100 as its Ethertype. The packets received with standard Q tag are considered as S-Tagged packets. – CustomerBridgePort—denotes the port to be used in customer bridges and in provider (Q-in-Q) bridges. This port type is not valid in <i>PCBs</i> and <i>PEBs</i>. – None—denotes that bridge port type is not set for the port. This is currently not supported. Example: – The following details are flushed, when port types CustomerNwPortStagged and ProviderNwPort are changed to any other type: • Unicast entries learnt on the port • VID translation table entries associated with the port – The following details are flushed, when port type CustomerBridgePort is changed to any other type. • Unicast entries learnt on the port • C-VID registration table entries associated with the port • PEP configuration table entries • Service priority regeneration table entries

Fields (cont)	NOTE: Bridge port type can be set only for switch ports and not for router ports, IVR interfaces, and I-LAN interfaces. The port type can be set only as CustomerBridgePort in customer bridges. The port type can be set only as ProviderNwPort in provider core and edge bridges. The port type can be set only as CustomerNwPort or ProviderNwPort, in provider backbone bridge. The port types CustomerEdgePort and PropCustomerEdgePort, are allowed only in PEBs. 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 a part of a port-channel. • Default User Priority—select the default ingress user priority for the port. The default value is 0. The list contains values from 0 to 7. The value 0 represents the lowest priority and the value 7 represents the highest priority. <i>NOTE: This priority is useful only on media, such as Ethernet, that does not support native user priority. The default user priority is greyed out and cannot be configured if the Port Type is set as Router Port.</i> • Switch Port Mode—select the mode of operation for the switch port. The mode defines the way of handling of traffic for VLANs. The default option is Hybrid. The list contains: – Access—configures the port as access port that accepts and sends only untagged frames, is added as a member to specific VLAN only, and carries traffic only for the VLAN to which the port is assigned. – Trunk—configures the port as trunk port that accepts and sends only tagged frames, 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. – Hybrid—configures the port as a hybrid port that accepts and sends both tagged and untagged frames. – Host—enables Ingress Filtering and configures the port as a host port that operates based on the secondary VLAN to which it is configured as a member port. • If a host port is a member port of an isolated VLAN, traffic from the host port is sent only to the promiscuous port of the private VLAN and the trunk port. • If a host port is a member port of the community VLAN, traffic from the host port can be sent only to other ports of the community VLAN, trunk port and promiscuous port of the private VLAN. – Promiscuous—enables Ingress Filtering and configures the port as promiscuous port that is used to move traffic between ports in community or isolated VLANs. This port communicates with all interfaces, including the isolated and community ports within a PVLAN.

Fields
(cont)

NOTE: The switch port mode can be set to Access for a port, only if the Dynamic *VLAN* status is set as Disabled, and Acceptable Frame Type is set as UnTagged and Priority Tagged for that port.

The switch port mode can be set to Trunk for a port, only if the port is not a member of Untagged Ports for a *VLAN*.

The switch port mode is greyed out and cannot be configured if the Port Type is set as a Router Port.

A host port can be associated only with one secondary *VLAN* and with the associated primary *VLAN*.

Promiscuous ports should be configured as member port of primary *VLAN* and member port of all secondary *VLANs* associated with that primary *VLAN*.

Host and promiscuous ports should be configured as untagged members of primary / secondary *VLANs*.

An access / hybrid port automatically changes as a host port, when configured as a member port of a primary/secondary *VLAN*.

Ingress Filtering cannot be disabled on host and promiscuous ports.

The port is removed from the associated *PVLAN* domain, when the mode is changed from promiscuous / host to access/hybrid.

- **MTU**—enter the maximum transmission unit frame size *MTU* for the interface. 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. This value ranges from 46 to 9216 bytes. The default value is assigned for *MTU* based on the type/protocol of the interface (as tabulated below), if the *MTU* value is not configured during creation of interface.

Protocols	Default MTU in bytes
Ethernet v2, PPP default	1500
Ethernet 802.3	1492
Ethernet Jumbo Frames	1500–9000
PPPoE	1480
L2TP	1460
FDDI	4500

NOTE: The MTU value can be changed for the interface, only if the Admin State of the interface is set as Down. The MTU value should be set as lowest of the MTU values of the member ports, while configuring for logical *VLAN* interfaces.

	• Link Up/Down Trap—select whether the Link Up / linkDown trap should be generated for the interface. The Link Up 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 default option is Enabled for interfaces that do not operate on top of any other interface. Otherwise, the trap is set as Disabled. The list contains: – Enabled—enables the generation of Link Up/linkDown traps for the interface. – Disabled—disables the generation of Link Up/linkDown traps for the interface • Port Type—select the port type as an L2 port or an L3 port. The default option is Switch Port for the newly enabled physical port. The list contains: – Switch Port—sets the port as an L2 port. The port forwards traffic based on the MAC address and operates in Layer 2. – Router Port—sets the port as an L3 port. The port forwards traffic based on the IP address and operates in Layer 3. The port is not associated with a particular <i>VLAN</i>, does not support <i>VLAN</i> sub interfaces, and behaves like a normal L3 interface. NOTE: The port type can be configured, only if the Admin State of the interface is set as Down. • Mac Address—enter the unicast <i>MAC</i> address of the interface. This value is set as an octet string of zero length for interface (e.g., serial line) that does not have address at its protocol sub-layer. By default, the <i>MAC</i> address is obtained from the switch. NOTE: The MAC address can be configured only if the Admin State of the interface is set as Down. This field is valid only if the type/protocol of interface is ethernetCsmacd (Ethernet/802.3) or ieee8023ad (Link Aggregation <i>MIB</i>).
Buttons	• Apply—modifies attributes and saves the changes.

8.3. VLAN Traffic Class Mapping

Figure 3: VLAN Traffic Class Mapping

VLAN Traffic Class Mapping

Select	Port	Priority 0	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Priority 6	Priority 7
Traffic Class									
☐	Gi0/1	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/2	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/3	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/4	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/5	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/6	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/7	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/8	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/9	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/10	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/11	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/12	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/13	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/14	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/15	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/16	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/17	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/18	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/19	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/20	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/21	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/22	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/23	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Gi0/24	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Ex0/1	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Ex0/2	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Ex0/3	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾
☐	Ex0/4	2 ▾	0 ▾	1 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾

Apply

Screen Objective

This screen allows the user to map evaluated user priority onto traffic class for forwarding by the bridge. For handling priority traffic, eight traffic classes are supported. Traffic types are assigned based on the time sensitiveness of the traffic. 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

NOTE: The number of supported traffic classes depends on the hardware used, which may limit the number of traffic classes to a lower number.

Navigation	Layer 2 Management > Port Manager > Traffic Class
Fields	• Select—click to select the port for which the configuration needs to be done. • Port—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and port number (slot number/port number). • Traffic Class—select the traffic class value to which the received frame of specified priority is to be mapped. The priority value ranges from 0 to 7. 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 (configurable only through <i>CLI</i>) value for the ingress port and media-specific user priority if the untagged frames are received from non-Ethernet media. The default value is 0. The list for the traffic class contains: – 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 traffic class but of 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 for ensuring 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.
Buttons	• Apply—modifies attributes and saves the changes.

8.4. Port Control

Figure 4: Port Control

Port Control

Select	Port	Mode	Duplex	Speed	FlowControl Admin Status	FlowControl Oper Status	HOL-Block Prevention	CPU Controlled Learning	Pause High Water Mark (kbps)	Pause Low Water Mark (kbps)	Auto MDI/MDIX Capability
☐	Gi0/1	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/2	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/3	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/4	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/5	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/6	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/7	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/8	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/9	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/10	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/11	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/12	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/13	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/14	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/15	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/16	Auto	Full	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/17	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/18	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/19	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/20	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/21	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/22	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/23	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Gi0/24	Auto	Half	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Ex0/1	NoNegot	Full	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Ex0/2	NoNegot	Full	10GBPS	Disabled	Disabled	Enabled		0	0	Auto
☐	Ex0/3	NoNegot	Full	10GBPS	Disabled	Disabled	Enabled		0	0	Auto
☒	Ex0/4	NoNegot	Full	10GBPS	Disabled	Disabled	Enabled		0	0	Auto

Screen Objective	This screen allows the user to configure port specific parameters, such as negotiation mode of the switch.
Navigation	Layer 2 Management > Port Manager > Port Control
Fields	Select—click to select the port for which the configuration needs to be done. Port—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and port number (slot number/port number).

Fields (cont)	• Mode—select the negotiation mode for the port. The negotiation avoids the risk of network disruption that arises from interference of dissimilar technologies with each other. The default option is Auto. The list contains: – Auto—advertises and negotiates parameters such as speed, duplex mode, and flow control of one port on an end of a link with another port on another end of the link for finding an optimal connectivity between them. When the mode is set as Auto, the hardware senses the speed and negotiates with the port on the other end of the link for data transfer operation as full-duplex or half-duplex and for flow control. – NoNegot—uses the configured values for parameters such as speed, duplex mode, and flow control. This mode is used when the other switch does not have the capability to configure negotiation mode as auto and no-negotiation. When the mode is set as NoNegot, the configured values for interface speed, duplex mode, and flow control become effective. • Duplex—select the duplex mode that represents the flow of data through the port. The list contains: – Full—configures interface data transfer mode as full-duplex. Ports can send and receive data at the same time. – Half—configures interface data transfer mode as half-duplex. Ports can either send or receive data at that specified time. NOTE: The duplex mode can be configured, only if the negotiation Mode is set as NoNegot. The duplex mode is automatically configured based on the hardware after negotiating with the peer if the negotiation Mode is set as Auto. • Speed—select the speed of the interface. The list contains: – 10 MBPS—sets the port speed as 10MBPS. This implies that the port can transfer data at the rate of 10 Megabits per second. – 100 MBPS—sets the port speed as 100MBPS. This implies that the port can transfer data at the rate of 100 Megabits per second. – 1 GBPS—sets the port speed as 1GBPS. This implies that the port can transfer data at the rate of 1 Giga bits per second. – 10 GBPS—sets the port speed as 10GBPS. This implies that the port can transfer data at the rate of 10 Giga bits per second. – 40 GBPS—sets the port speed as 40 GBPS. This implies that the port can transfer data at the rate of 40 Giga bits per second. – 56 GBPS—sets the port speed as 56 GBPS. This implies that the port can transfer data at the rate of 56 Giga bits per second. – 2.5 GBPS—sets the port speed as 2.5 GBPS. This implies that the port can transfer data at the rate of 2.5 Giga bits per second. – Full—configures interface data transfer mode as full-duplex. Ports can send and receive data at the same time. – Half—configures interface data transfer mode as half-duplex. Ports can either send or receive data at that specified time.

Fields (cont)	NOTE: The speed can be configured, only if the negotiation Mode is set as NoNegot. The speed is automatically configured based on the hardware after negotiating with the peer if the negotiation Mode is set as Auto. • FlowControl Admin Status—select the default administrative PAUSE mode for the interface. PAUSE is a flow control mechanism that is implied on full duplex Ethernet link segments. The mechanism uses <i>MAC</i> control frames to carry the PAUSE commands. This command is used to pause the flow of data for a time that is measured in units of quanta, where each unit is equal to 512-bit times. The list contains: – Disabled—disables the flow control mechanism (that is, PAUSE). – Transmit—enables the transmission of <i>MAC</i> control frames used for PAUSE to a remote device. – Receive—enables the reception of <i>MAC</i> control frames used for PAUSE from a remote device. – Both—enables both the transmission/reception of <i>MAC</i> control frames used for PAUSE to/from a remote device. NOTE: The PAUSE mode can be configured, only if the negotiation Mode is set as NoNegot for the <i>MAU</i> attached to the interface. The PAUSE mode is automatically configured to the mode to which the interface will automatically revert once auto-negotiation is disabled, if the negotiation Mode is set as Auto for the Medium Attachment Unit (<i>MAU</i>) attached to the interface. This mode is applied only for the interface operating in full Duplex mode. Otherwise, the value set in this mode is ignored. The PAUSE mode cannot be set as Transmit and Receive on interfaces that operate at 100 Megabits per second or less. • FlowControl Oper Status—displays the PAUSE mode currently used in the interface. If the negotiation Mode is set as Auto for the <i>MAU</i> attached to the interface, then the value is set based on the auto-negotiation function. The list contains: – Invalid—denotes that the flow control operational status is invalid. – Disabled—denotes that the flow control mechanism (that is, PAUSE) is disabled. This value is returned by interfaces operating in half Duplex mode and interfaces on which auto negotiation process is not yet completed. – Transmit—denotes that the transmission of <i>MAC</i> control frames used for PAUSE to a remote device is enabled. This value is never returned by interfaces operating at 100 Megabits per second or less. – Receive—denotes that the reception of <i>MAC</i> control frames used for PAUSE to a remote device is enabled. This value is never returned by interfaces operating at 100 Megabits per second or less. – Both—denotes that both the transmission/reception of <i>MAC</i> control frames used for PAUSE to/from a remote device is enabled.

Fields (cont)	• HOL-Block Prevention—select whether the Head-Of-Line (<i>HOL</i>) blocking should be prevented on a port. <i>HOL</i> blocking happens when <i>HOL</i> packet of a buffer cannot be switched to an output port (i.e. <i>HOL</i> occurs when a line of packets is held up by the first packet). The default option is Enabled. The list contains: – Enabled—prevents <i>HOL</i> blocking from occurring on the port. The high priority packets are placed in a separate queue and the low priority packets are discarded. The applications or TCP protocol keeps track of necessity to retransmit discarded packets. – Disabled—does not prevent v blocking on the port. • CPU Controlled Learning—select whether the Head-Of-Line (<i>HOL</i>) blocking should be prevented on a port. <i>HOL</i> blocking happens when <i>HOL</i> packet of a buffer cannot be switched to an output port (i.e. <i>HOL</i> occurs when a line of packets is held up by the first packet). The default option is Enabled. The list contains: – Enabled—enables the software learning of <i>MAC</i> Address. – Disabled—disables the software learning of <i>MAC</i> Address. NOTE: When <i>CPU</i> controlled learning is enabled, for the first time, a packet is copied to <i>CPU</i>—source <i>MAC</i> address learning does not happen in the hardware. When packet is received at <i>PNAC</i>, and if the source <i>MAC</i> address is authorized, the packet is allowed to go through further processing; else, the packet is dropped. When packets from authorized <i>MAC</i> address are received at <i>VLAN</i>, <i>MAC</i> learning happens at <i>VLAN</i> and the same entry is programmed in the hardware. Once the <i>MAC</i> address is learnt, further forwarding happens at driver itself. When software learning is enabled, rate limiting to the port needs to be configured. • Pause High Water Mark—enter the ingress rate equal to or above which PAUSE frames are transmitted. The value is from 1 to 80000000 kbps with default of 0. • Pause Low Water Mark—enter the ingress rate equal to or above which PAUSE frames are stopped. The value is from 1 to 80000000 kbps with default of 0. NOTE: This value should be less than Pause High Water Mark (kbps). This value should be configured as 0 only if Flow Control Oper Status is disabled. • Auto MDI/ MDIX Capability—select the Auto-<i>MDIX</i> mode for the interface. The default option is Auto. The list contains: – Auto—enables <i>MDI/MDIX</i> auto crossover of the interface. NOTE: This configuration is effective only if the speed of the port is auto negotiable – <i>MDI</i>—sets the port to <i>MDI</i> 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. – <i>MDIX</i>—sets the port to <i>MDIX</i> 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. <i>MDIX</i> is the vice versa of <i>MDI</i>.
Buttons	• Apply—modifies attributes and saves the changes.

8.5. Storm Control

Figure 5: Storm Control

Storm Control

Select	Port	Ingress Storm Control			Egress Rate Limiting	
		DLF Level	Broadcast Level	Multicast Level	Egress-Port Rate-Limit	Port Burst-Size
☐	Gi0/1	0	0	0	0	0
☐	Gi0/2	0	0	0	0	0
☐	Gi0/3	0	0	0	0	0
☐	Gi0/4	0	0	0	0	0
☐	Gi0/5	0	0	0	2	2
☐	Gi0/6	0	0	0	0	0
☐	Gi0/7	0	0	0	0	0
☐	Gi0/8	0	0	0	0	0
☐	Gi0/9	0	2	0	0	0
☐	Gi0/10	0	0	0	0	0
☐	Gi0/11	0	0	0	0	0
☐	Gi0/12	0	0	0	0	0
☐	Gi0/13	0	0	0	0	0
☐	Gi0/14	0	0	0	0	0
☐	Gi0/15	0	0	0	0	0
☐	Gi0/16	0	0	0	0	0
☐	Gi0/17	0	0	0	0	0
☐	Gi0/18	0	0	0	0	0
☐	Gi0/19	0	0	0	0	0
☐	Gi0/20	0	0	0	0	0
☐	Gi0/21	0	0	0	0	0
☐	Gi0/22	0	0	0	0	0
☐	Gi0/23	0	0	0	0	0
☐	Gi0/24	0	0	0	0	0
☐	Ex0/1	0	0	0	0	0
☐	Ex0/2	0	0	0	0	0
☐	Ex0/3	0	0	0	0	0
☒	Ex0/4	0	0	0	0	0

Screen Objective	This screen allows the user to control the rate limiting parameters for all interfaces in the switch. The rate control feature protects the switch from packet flooding from malicious users. This feature allows the user to set threshold traffic rate so that the traffic exceeding the threshold rate is dropped. Rate control can be applied on unknown unicast, multicast, and broadcast traffic.
Navigation	Layer 2 Management > Port Manager > Storm Control
Fields	• Select—click to select the port for which the configuration needs to be done. • Port—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and port number (slot number/port number). • DLF Level—enter the limiting value for the maximum number of <i>DLF</i> (Destination Lookup Failure) packets that can be transmitted per second over the interface. The value range is limited by the underlying hardware. The value 0 disables rate limiting for destination look up failure packets on the interface. This value ranges from 0 to 262143. The default value is 0. • Broadcast Level—enter the limiting value for the maximum number of broadcast packets that can be transmitted per second over the interface. The value range is limited by the underlying hardware. The value 0 disables rate limiting for broadcast packets on the interface. This value ranges from 0 to 262143. The default value is 0. • Multicast Level—enter the limiting value for the maximum number of multicast packets that can be transmitted per second over the interface. The value range is limited by the underlying hardware. The value 0 disables rate limiting for multicast packets on the interface. This value ranges from 0 to 262143. The default value is 0. • Egress-Port Rate-Limit—enter the rate limit value that represents the maximum number of packets to be transferred per second on a port. The rate limit is applied based on the operating speed of the port. It affects the interface speed and is affected by the metering feature. The value 0 disables rate limiting; that is, it sets the port to the configured speed. This value ranges from 0 to 80000000. The default value is 0. <i>The window resolution is 256 μsec. So, to get a resolution of 100 ms, the window is programmed with a value of 389. (i.e. $389 \times 256 \mu\text{sec} = 99584 \mu\text{sec} = 99.584\text{msec} \approx 100\text{ms}$).</i> <i>Example:</i> <i>To have rate-limit at 1500 packets per second, this means that in 100ms resolution, packets that shall be allowed will be: $(100\text{ms} \times 1500)/1\text{sec} = 150$ packets. With rate-limit resolution as 64 packets, the value that will be programmed in the rate limiter field is: $150/64 = 2.34 \approx 2$.</i> NOTE: The value 0 disables rate limiting for the port. It sets the port to full speed.

Fields (cont)	• Port Burst-Size—enter the burst size that represents the maximum number of packet burst to be transferred per second on a port. The burst size is applied based on the operating speed of the port. It affects the interface speed and is affected by the metering feature. The value 0 disables burst rate limiting; that is, it sets the port burst rate limit to the configured speed. This value ranges from 0 to 80000000. The default value is 0.
Buttons	• Apply—modifies attributes and saves the changes.

8.6. Port Role

Figure 6: Port Role

Port Role

Select	Port	Link Status	Port Role
☐	Gi0/1		Downlink ▾
☐	Gi0/2		Downlink ▾
☐	Gi0/3		Downlink ▾
☐	Gi0/4		Downlink ▾
☐	Gi0/5		Downlink ▾
☐	Gi0/6		Downlink ▾
☐	Gi0/7		Downlink ▾
☐	Gi0/8		Downlink ▾
☐	Gi0/9		Downlink ▾
☐	Gi0/10		Downlink ▾
☐	Gi0/11		Downlink ▾
☐	Gi0/12		Downlink ▾
☐	Gi0/13		Downlink ▾
☐	Gi0/14		Downlink ▾
☐	Gi0/15		Downlink ▾
☐	Gi0/16		Downlink ▾
☐	Gi0/17		Downlink ▾
☐	Gi0/18		Downlink ▾
☐	Gi0/19		Downlink ▾
☐	Gi0/20		Downlink ▾
☐	Gi0/21		Downlink ▾
☐	Gi0/22		Downlink ▾
☐	Gi0/23		Downlink ▾
☐	Gi0/24		Downlink ▾
☐	Ex0/1		Downlink ▾
☐	Ex0/2		Downlink ▾
☐	Ex0/3		Downlink ▾
☒	Ex0/4		Downlink ▾

Figure 29-6: Port Role

Screen Objective	This screen allows the user to configure the port role related parameters.
Navigation	Layer 2 Management > Port Manager > Port Role

Fields	• Select—click to select the port for which the configuration needs to be done. • Port—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and port number (slot number/port number). • Link Status—displays the status of the link using graphics. The link represents a physical connection established between the switches or switch and device in a network. The graphical representation is: – Green up arrow—denotes that the link is working. That is, a physical connection established for the port is active and ready for exchange of traffic. – Red down arrow—denotes that the link is not working. That is, no physical connection is established for the port or the established physical connection is not active and is a faulty one. • Port Role—select the port role for the interface for which the configuration is to be applied. The list contains: – Uplink—sets the port role for an interface as uplink. – Downlink—sets the port role for an interface as downlink. – Designated Uplink—sets the port role for an interface as designated uplink.
Buttons	• Apply—modifies attributes and saves the changes.

VLAN Map

9. VLAN Section

This section describes the *VLAN* interfaces.

9.1. VLAN

This section describes how to configure *VLANs*.

VLAN (Virtual *LAN*) module logically segments the shared media *LAN* to form virtual workgroups. It fully utilizes the forwarding support available in the switch hardware. It redefines and optimizes the basic transparent bridging functionalities, such as learning, forwarding, filtering, flooding, etc.

VLAN operates in the following modes. They are:

- Transparent bridging—allows the user to connect two similar network segments to each other at the data link layer in a manner transparent to end stations, so the end stations do not participate in the bridging algorithm.
- *VLAN* aware bridging—allows the end stations at different *LAN* segments to be interconnected and to communicate with each other using *VLANs*. It provides the following optional capabilities that are not available for the transparent bridging mode of operation:
 - High availability (*HA*)—a feature for enhancing the network resiliency by minimizing the network downtime by integrating failover systems. *VLAN* in active node synchronizes the database with standby node(s).
 - Multiple instances—multiple switch instances can be created within a physical switch. Different instances are identified using context ID.
- Provider bridging—supports IEEE 802.1ad standard.

To access **VLAN** Screens, click **Layer 2 Management > VLAN**.

The **VLAN** parameters are configured through the screens displayed by the following tabs:

[VLAN Basic Settings](#)

[VLAN Port Settings](#)

[Static VLAN Configuration](#)

[VLAN Protocol Group Settings](#)

[Port VLAN Protocol Settings](#)

[VLAN Port Mac Map](#)

[FDB Flush](#)

VLAN Basic Settings

By default, the tab **Basic Settings** displays the **VLAN Basic Settings** screen.

Figure 1: VLAN Basic Settings

VLAN Basic Settings

Select	Context	Learning Mode	Subnet Based On All Ports	MAC Based On All Ports	Port and Protocol Based On All Ports	Global Mac Learning Status	Default Vlan Hybrid Type	MAC-Address-Table Aging Time
☒	0	IVL ▾	Disabled ▾	Disabled ▾	Enabled ▾	Enabled ▾	IVL ▾	300

Note 1: Default VLAN hybrid type can be configured only when learning mode is hybrid.

Note 2: Dynamic unicast mac limit set for the switch cannot be less than unicast mac limit of vlan and should not exceed the device capability.

Note 3: Pre-requisite for setting "Base bridge mode" to **DOT_1D_BRIDGE_MODE** is to shutdown protocols such as GARP, **Snooping**, **Pnac**, **Link Aggregation**, **LLDP**, **MSTP/RSTP** and all interfaces except physical interfaces should be deleted.

VLAN Basic Settings

MAC-Address-Table Aging Time	Unicast MAC Learning Limit	Base Bridge Mode	Dynamic Vlan Oper Status	Dynamic Multicast Oper Status	Maximum VLAN ID	Maximum Supported VLANs	Number of VLANs in the System	User Defined TPID
300	0	DOT_1Q_VLAN_MODE ▾	Disabled ▾	Disabled ▾	4094	4094	1	0

Screen Objective	This screen allows the user to configure, for all available virtual contexts, the <i>VLAN</i> details that are used globally in the switch for all ports available in the switch. It allows the user to set the parameters such as <i>VLAN</i> type, which are fundamental for the <i>VLAN</i> configuration in the switch.
NOTE: When all <i>VLAN</i> type-related fields subnet based on all ports, <i>MAC</i>-based on all ports, and port and protocol based on all ports are set as Enabled, the <i>VLAN</i> membership classification is done in the following order: • <i>MAC</i>-based <i>VLAN</i> classification • Subnet-based <i>VLAN</i> classification • Port and protocol based <i>VLAN</i> classification	
Navigation	Layer 2 Management > VLAN > Basic Settings
Fields	• Select—click to select the context ID to configure the <i>VLAN</i> Basic settings for the virtual context. • Context—displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This value ranges from 0 to 65535. The default value is 0. • Learning Mode—select the type of <i>VLAN</i> learning mode to be applied for all ports. This mode defines the forwarding database modes of operation to be implemented by the switch. The default option is <i>IVL</i> (Independent <i>VLAN</i> Learning). The list contains: – <i>IVL</i>—separate forwarding database is created for each <i>VLAN</i>. The information learnt from a <i>VLAN</i> is not shared among other relative <i>VLANs</i> during forwarding decisions. This mode is suitable in situations where the database size is not a constraint and end stations operate over multiple <i>VLANs</i> with the same <i>MAC</i> address. – <i>SVL</i>—for Shared <i>VLAN</i> Learning (<i>SVL</i>), single forwarding database is created for all <i>VLANs</i>. The information learnt from a <i>VLAN</i> is shared among all other relative <i>VLANs</i> during forwarding decision. This mode is suitable in situations where the learning database size is a constraint. – <i>HYBRID</i>—same forwarding database is created for some <i>VLANs</i> and separate forwarding database is used for some <i>VLANs</i>. The usage of same or separate forwarding database for the <i>VLAN</i> is decided based on the configuration done in the L2 Unicast Filter Configuration screen. NOTE: When the learning mode is changed: – The static <i>FID-VLAN</i> mapping and static unicast entries should be reconfigured respectively in the screens port <i>VLAN</i> protocol settings and Static <i>VLAN</i> configuration, and – Static unicast configurations associated with old <i>FID</i> (Filtering ID) will be deleted

Fields (cont)	• Subnet Based On All Ports—select whether the classification of <i>VLAN</i> membership should be done based on subnet on all available ports. <i>VLAN</i> membership classification is done by matching the source IP address in the packet to a <i>VLAN</i>-ID using an administrator configured table if the subnet based <i>VLAN</i> classification is enabled. The default option is Disabled. The list contains: – Enabled—enables the subnet based <i>VLAN</i> membership classification on all ports of the switch. – Disabled—disables the subnet based <i>VLAN</i> membership classification on all ports of the switch • MAC Based on All Ports—select whether the classification of <i>VLAN</i> membership should be done based on <i>MAC</i> on all available ports. <i>VLAN</i> membership classification is done based on the source <i>MAC</i>-address of the received frame if the <i>MAC</i> based <i>VLAN</i> classification is enabled. For this type, the <i>VLAN</i> membership should be assigned initially. The default option is Disabled. The list contains: – Enabled—enables <i>MAC</i>-based <i>VLAN</i> membership classification on all ports of the switch. – Disabled—disables <i>MAC</i>-based <i>VLAN</i> membership classification on all ports of the switch. • Port and Protocol Based on All Ports—select whether the classification of <i>VLAN</i> membership should be done based on port and protocol on all available ports. <i>VLAN</i> membership classification is done for all untagged and priority-tagged frames based on the port-protocol group / higher layer protocol for the port if the port and protocol based <i>VLAN</i> classification is enabled. The default option is Enabled. The list contains: – Enabled—enables Port and Protocol Based <i>VLAN</i> membership classification on all ports of the switch. – Disabled—disables Port and Protocol Based <i>VLAN</i> membership classification on all ports of the switch. • Default Vlan Hybrid Type—select the default <i>VLAN</i> Hybrid Type to be applied for all ports of the switch if learning mode is set to HYBRID. The default option is IVL. The list contains: – IVL—separate forwarding database is created for each <i>VLAN</i>. The information learnt from a <i>VLAN</i> is not shared among other relative <i>VLAN</i>s during forwarding decisions. This mode is suitable in situations where the database size is not a constraint and end stations operate over multiple <i>VLAN</i>s with the same <i>MAC</i> address. – SVL—single forwarding database is created for all <i>VLAN</i>s. The information learnt from a <i>VLAN</i> is shared among all other relative <i>VLAN</i>s during forwarding decision. This mode is suitable in situations where the learning database size is a constraint.

Fields (cont)	NOTE: Once the learning mode is changed: – The static <i>FID-VLAN</i> mapping and static unicast entries should be reconfigured respectively in the screens Port <i>VLAN</i> Protocol Settings and Static <i>VLAN</i> Configuration. – Static unicast configurations associated with old <i>FID</i> will be deleted. • MAC-Address-Table Aging Time—enter the timeout period (in seconds) to age out the dynamically learned forwarding database entries. This timer is started once the switch identifies the <i>MAC</i> address. This value ranges from 10 to 1000000 seconds. The default value is 300. • Unicast MAC Learning Limit—enter the maximum number of unicast <i>MAC</i> addresses that can be learned in the virtual context. This value ranges from 0 to 4294967295. The maximum number of unicast <i>MAC</i> addresses that can be learnt is 950. The maximum number of unicast <i>MAC</i> addresses that can be learnt is 950. NOTE: The upper limit value depends upon the underlying hardware. The unicast <i>MAC</i> learning limit cannot be configured greater than the default value. This value should be greater than the value set in the field <i>MAC</i> Limit for the <i>VLAN</i> and should not exceed the switch capability. • Base Bridge Mode—select the base bridge-mode in which the switch should operate. The list contains: – DOT_1D_BRIDGE_MODE—makes the switch to behave according to IEEE 802.1d implementation. – DOT_1Q_VLAN_MODE—makes the switch to behave according to IEEE 802.1q implementation. NOTE: The base bridge mode can be set as DOT_1D_BRIDGE_MODE, only if the <i>GARP</i>, <i>IGS</i>, <i>MLDS</i>, <i>PNAC LA</i>, <i>LLDP</i>, <i>RSTP</i> and <i>MSTP</i> modules are shut down and logical interfaces are deleted. This configuration should be done in the following order: – Shut down <i>GARP</i>. The Dynamic <i>VLAN</i> and Dynamic Multicast should be disabled in the Dynamic <i>VLAN</i> Global Configuration and Dynamic Multicast Global Configuration screens before shutting down <i>GARP</i>. – Shut down IGMP snooping module using the field System Control in the IGMP Snooping Configuration screen. Go to Multicast > IGMP Snooping > Basic Settings. – Shut down <i>MSTP</i> module using the field System Control in the Global Configuration screen. Go to Layer2 Management > MSTP > Basic Settings. – Shut down <i>RSTP</i> module using the field System Control in the Global Configuration screen. Go to Layer2 Management > RSTP > Global Settings. – Shut down <i>PNAC</i> module using the field System Control in the 802.1x Basic Settings screen. Go to Layer2 Management > 802.1x > Basic Settings. – Shutdown Link Aggregation module using the field System Control in the Link Aggregation Basic Settings screen. Go to Layer2 Management > Link Aggregation > Basic Settings.

Fields (cont)	• Base Bridge Mode (cont) NOTE: (cont) – Shutdown LLDP module using the field Global Status in the <i>LLDP</i> Global Configurations screen under the path Layer2Management > LLDP > Global Setting. – Shutdown <i>MLDS</i> module using the field System Control in the MLD Snooping Configuration screen. Go to Multicast > MLD Snooping > Basic Settings. The DOT_1D_BRIDGE_MODE operates over the physical interface alone, so all other VLAN / tunnel interfaces should be deleted. – If the Web interface is connected through the Layer3 IP interface, then first create a router port and assign IP address for that router port to re-establish the Web connectivity through the newly created router port. The existing Layer 3 IP interfaces can then be deleted, and base bridge mode can be set as DOT_1D_BRIDGE_MODE • Dynamic Vlan Oper Status—displays the operational status of the Dynamic <i>VLAN</i> (<i>GVRP</i> module). <i>GVRP</i> uses the services of <i>GARP</i> to propagate <i>VLAN</i> registration information to other <i>VLAN</i> aware bridges in the <i>LAN</i>. This information allows <i>GVRP</i> aware devices to dynamically establish and update the information about the existence of the <i>VLANs</i> in the topology. The <i>GVRP</i> module registers the created <i>VLANs</i> with <i>GARP</i> and de-registers the deleted <i>VLANs</i> from the <i>GARP</i>. The default option is Enabled. The list contains: – Enabled—denotes that the <i>GVRP</i> module is enabled in the switch. – Disabled—denotes that the <i>GVRP</i> module is disabled in the switch. • Dynamic Multicast Oper Status—displays the operational status of the <i>GMRP</i> module. <i>GMRP</i> uses the services of <i>GARP</i> to propagate multicast registration information to the bridges in the <i>LAN</i>. This information allows <i>GMRP</i> aware devices to reduce the transmission of multicast traffic to the <i>LANs</i>, which do not have any members of that multicast group. <i>GMRP</i> registers and de-registers the group membership information and group service requirement information with the <i>GARP</i>. The default option is Enabled. The list contains: – Enabled—denotes that the <i>GMRP</i> module is enabled in the switch. – Disabled—denotes that the <i>GMRP</i> module is disabled in the switch. • Maximum VLAN ID—displays the largest valid <i>VLAN</i> / VFI ID accepted in the system. This value ranges from 1 to 65535. – <vlan -id>—this is a unique value that represents the specific <i>VLAN</i>. This value ranges from 1 to 4094 – <vfi-id>—VFI ID is a <i>VLAN</i> created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical <i>LAN</i> for the VPLS service. This value ranges from 4096 to 65535.

Fields (cont)	NOTE: The <i>VLAN</i> ID 4095 is reserved and may be used to indicate a wildcard match for the <i>VLAN</i> ID in management operations or Filtering Database entries. <i>VFI</i> IDs 4096 and 4097 are reserved identifiers used in MPLS PW. The theoretical maximum for the maximum number of <i>VFI</i> is 65535 but the actual number of <i>VFI</i> supported is a sizing constant. Based on this, the maximum number of <i>VFI</i> ID accepted in the management interface is restricted. For example if 100 <i>VFI</i>s are supported, the maximum number of <i>VFI</i> supported will be restricted to maximum number of <i>VLAN</i>s + 100. An error message is displayed for any value beyond this range. The <i>VLAN</i> ID cannot be configured greater than the value displayed in the field. • Maximum Supported VLANs—displays the maximum number of <i>VLAN</i>s the switch can support. • Number of VLANs in the System—displays the total number of <i>VLAN</i>s currently active in the device. By default, <i>VLAN</i> 1 is active in the system, and hence, this value is set as 1. • User Defined <i>TPID</i>—enter the value for the user defined <i>TPID</i> configurable for an ingress port or for a <i>VLAN</i> egress Ethertype. The value ranges from 0 to 65535. The default value is 0. NOTE: A value 0 (ZERO) deletes the configured entry.
Buttons	• Apply—modifies attributes for the selected entry and saves the changes. • Configure VLAN Trace Options—accesses <i>VLAN</i> Traces screen.

VLAN Port Settings

Figure 2: VLAN Basic Settings

VLAN Port Settings

Select	Port	MAC Based VLAN	Port and Protocol Based VLAN	Port Protected	Subnet Based VLAN	PVID	Acceptable Frame Types	Ingress Filtering	Ingress EtherType Prefix Hex values by 0x	Egress EtherType Prefix Hex values by 0x	Egress TPID Type	Allowable TPID1	Allowable TPID2	Allowable TPID3
☐	Gi0/1	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/2	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/3	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/4	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/5	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/6	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/7	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/8	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/9	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/10	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/11	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/12	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/13	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/14	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/15	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/16	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/17	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/18	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/19	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/20	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/21	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/22	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/23	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Gi0/24	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Ex0/1	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Ex0/2	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☐	Ex0/3	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0
☒	Ex0/4	Disabled ▾	Enabled ▾	False ▾	Disabled ▾	1	All ▾	Disabled ▾	8100	8100	Portbased ▾	0	0	0

Screen Objective

This screen allows the user to configure *VLAN* details such as *VLAN* membership classification type for the physical ports available in the device.

When all *VLAN* type related fields subnet based on all ports, *MAC*- based on all ports, and port and protocol based on all ports are set as enabled, the *VLAN* membership classification is done in the following order:

- *MAC*-based *VLAN* classification
- Subnet-based *VLAN* classification
- Port and protocol based *VLAN* classification

NOTE: This screen is different for BCM target, refer the BCM specific screens chapter for more details.

Navigation

Layer 2 Management > VLAN > Port Settings

Fields

- **Select**—click to select the port for which the configuration needs to be done.

Fields	• Port—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number / port number) • MAC Based VLAN—select whether the <i>MAC</i>-based <i>VLAN</i> membership classification is supported in the port. <i>VLAN</i> membership classification is done based on the source <i>MAC</i> address of the received packets if the <i>MAC</i> based <i>VLAN</i> classification is supported. By default, the <i>MAC</i> based <i>VLAN</i> classification is set similar to that of the <i>MAC</i> Based on All Ports. The list contains: – Enabled—enables <i>MAC</i>-based <i>VLAN</i> classification in the port. – Disabled—disables <i>MAC</i>-based <i>VLAN</i> classification in the port. NOTE: This field can be configured independently without depending on the <i>VLAN</i> type configuration done globally in the switch. That is, this field does not depend upon the value set in the field <i>MAC</i>-based on All Ports. • Port and Protocol Based VLAN—select whether the port and protocol based <i>VLAN</i> membership classification is supported in the port. <i>VLAN</i> membership classification is done for all untagged and priority-tagged frames based on the port-protocol group / higher layer protocol for the port if the port and protocol based <i>VLAN</i> classification is supported. By default, the port and protocol based <i>VLAN</i> classification is set similar to that of the Port and Protocol Based on All Ports. The list contains: – Enabled—enables port and protocol based-<i>VLAN</i> classification in the port. – Disabled—disables port and protocol based-<i>VLAN</i> classification in port. NOTE: This field can be configured independently without depending on the <i>VLAN</i> type configuration done globally in the switch. So this field does not depend upon the value set in the field Port and Protocol Based on All Ports. • Port Protected—select whether the port should be configured as protected. The default option is False. The list contains: – true—sets the port as protected. the port will not forward frames received from another protected port on the same switch. – false—does not configure the port as protected. the port operates as a normal port. • Subnet Based VLAN—select whether the subnet based-<i>VLAN</i> membership classification is supported in the port. <i>VLAN</i> membership classification is done by matching the source IP address in the packet to a <i>VLAN</i>-ID using an administrator configured table if the subnet based-<i>VLAN</i> classification is supported. By default, the subnet based-<i>VLAN</i> classification is set similar to that of the subnet based on all ports. the list contains: – Enabled—enables subnet based-<i>VLAN</i> classification in the port. – Disabled—disables subnet based-<i>VLAN</i> classification in the port. NOTE: This field can be configured independently without depending on the <i>VLAN</i> type configuration done globally in the switch. That is, this field does not depend upon the value set in the field Subnet on All Ports.

Fields (cont)	• PVID—displays the <i>PVID</i> (Port <i>VLAN</i> ID), which represents the <i>VLAN</i> ID assigned to untagged frames or priority-tagged frames received on the port. The <i>PVID</i> is used for port based <i>VLAN</i> type membership classification. The default <i>VLAN</i> ID (that is, 1) is set as the <i>PVID</i>. This value ranges from 1 to 4094. • Acceptable Frame Types—select the type of <i>VLAN</i> dependent <i>BPD</i>U frames to be accepted by the port during the <i>VLAN</i> membership configuration. The default option is All. The list contains: – All—accepts tagged, untagged, and priority tagged frames received on the port and subjects the frames to Ingress Filtering setting. – Tagged—accepts only the tagged frames received on the port. It rejects untagged or priority tagged frames received on the port. – UnTagged and Priority Tagged—accepts only the untagged or priority tagged frames and rejects tagged frames received on the port. NOTE: This field does not affect <i>VLAN</i> independent <i>BPD</i>U frames such as GVRP <i>BPD</i>U and STP <i>BPD</i>U. It affects only the <i>VLAN</i> dependent <i>BPD</i>U frames such as GMRP <i>BPD</i>U. The frame type is always set as UnTagged and Priority Tagged if the Bridge Port Type is set to CustomerNwPort. • Ingress Filtering—select whether the filtering should be applied for the incoming frames received on the port. The default option is Disabled. The list contains: – Enabled—accepts only the incoming frames of the <i>VLAN</i>s that have this port in its member list. – Disabled—accepts all incoming frames received on the port. NOTE: This field does not affect <i>VLAN</i> independent <i>BPD</i>U frames such as GVRP <i>BPD</i>U and STP <i>BPD</i>U. It affects only the <i>VLAN</i> dependent <i>BPD</i>U frames such as GMRP <i>BPD</i>U. The filtering is always set as Enabled if the Bridge Port Type is set as CustomerNwPortStagged. The ingress filtering cannot be disabled for port whose Switch Port Mode is set as host or promiscuous • Ingress EtherType Prefix Hex values by 0x—enter the value for Ingress Ether-type. The value ranges from 1 to 65535. For the proprietary <i>PNPs</i> (Provider Network Ports), default value is 0x8100. For all other ports, default value is 0x88a8. NOTE: In Customer Bridge mode, this object indicates that the primary C-<i>VLAN</i> tag Ether-type used for the packets received on this port. Packets received on a port are considered tagged, when the packet Ether-type matches with the port Ether-type configured. Otherwise, they are considered untagged. By default, on all ports, 0x8100 will be configured as Ether-type. In Provider-Edge Bridge Mode, this object indicates the primary S-<i>VLAN</i> tag Ether-type used for the packets received on this port. Packets received on a port are considered tagged, when the packet Ether-type matches with the port Ether-type configured. Otherwise, they are considered untagged. By default, on all ports, 0x88a8 will be configured to be Ether-type. On Proprietary <i>PNPs</i>, 0x8100 is configured to be the ingress Ether-type.

Fields (cont)	• Egress EtherType Prefix Hex values by 0x—enter the value for Egress EtherType. The value ranges from 1 to 65535. For CEPs (Customer Edge Ports) and proprietary PNPs, default value is 0x8100. For all other ports, default value is 0x88a8. NOTE: In Customer Bridge Mode, this object indicates the Ethertype of the C-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 configured in this object. By default, 0x8100 will be used for packets transmitted with C-VLAN on the ports. NOTE: In Provider-Edge Bridge Mode, 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 configured in this object. By default, 0x88a8 will be used for packets transmitted with S-VLAN on the ports. On Proprietary PNPs and Customer Edge Ports, 0x8100 is used as the Ethertype for outgoing packets. • Egress TPID Type—select the egress <i>TPID</i> (Tag Protocol Identifier) type for the port. The default option is Portbased. The list contains: – Portbased—specifies the egress <i>TPID</i> type for a port. If the value is Portbased, the egress <i>TPID</i> of the packet is selected from Egress Port Table. – Vlanbased—specifies the egress <i>TPID</i> type for a port. When the value is Vlanbased, the Egress <i>TPID</i> is selected from Egress VLAN Table. • Allowable TPID1—enter the value for <i>TPID1</i>. This specifies the secondary Ether-type that is allowable for a port. The configurable value for this object is 0x8100 or 0x8808. This value ranges from 0 to 65535. The default value is 0. NOTE: When this value is set to zero, the secondary Ethertype configurations are deleted from Hardware. The <i>TPID1</i> value should be configured as a value different from the default ingress Ethertype. If the ingress Ethertype is 0x8808, then <i>TPID1</i> should be configured as 0x8100; and if the ingress Ethertype is 0x8100, <i>TPID1</i> should be configured as 0x8808. • Allowable TPID2—enter the value for <i>TPID2</i>. This specifies the secondary Ether-type that is allowable for a port. The configurable value for this object is 0x8100 or 0x8808. This value ranges from 0 to 65535. The default value is 0. NOTE: When this value is set to zero, the additional standard Ethertype configurations are deleted from Hardware. • Allowable TPID3—enter the value for <i>TPID3</i> to specify secondary Ether-type allowable for a port with configurable value of 0x8100 or 0x8808. This value ranges from 0 to 65535. The default value is 0. NOTE: When this value is set to zero, the additional standard Ethertype configurations are deleted from Hardware.
Buttons	• Apply—modifies attributes for the selected entry and saves the changes.

Static VLAN Configuration

Figure 3: Static VLAN Configuration

Static VLAN Configuration

VLAN ID *
VLAN Name
Member Ports *
Untagged Ports
Forbidden Ports
Vlan Egress Ethertype
☐ VLAN ACTIVE

Add Reset

Select	VLAN ID	VLAN Name	Member Ports	Untagged Ports	Forbidden Ports	VLAN ACTIVE	Vlan Egress Ethertype
☒	1		Gi0/1,Gi0/2,Gi0/3,G	Gi0/1,Gi0/2,Gi0/3,G		ACTIVE	0x8100

Apply Delete

Screen Objective	This screen allows the user to create / delete VLANs in the switch and statically configure details such as member port for the VLANs in the switch. These static configuration details are permanent and can be restored after the switch is reset. NOTE: The default VLAN entry, VLAN ID 1, cannot be deleted.
Navigation	Layer 2 Management > VLAN > Static VLANs
Fields	Select—click to select the vlan id for which the configuration needs to be modified or deleted. VLAN ID—enter the VLAN ID that uniquely identifies a specific VLAN. This value ranges from 1 to 4094. VLAN Name—enter an administratively assigned string, which is used to identify the VLAN. This value is a string of maximum size of 32. Member Ports—enter a port or a set of ports, which need to be part of the VLAN identified by the VLAN ID. Use comma as a separator between the ports while configuring a list of ports. This list includes both tagged and untagged members of the VLAN. NOTE: The format of this entry is <interface type><slot number/port number> for Gigabit Ethernet ports. For pseudowire and attachment circuit interfaces, the format is just the interface ID. There is no space needed between these two entries. For an example: Gi0/1,Gi0/2,pw1,ac1, where Gi is interface type Gigabit Ethernet, Pw is pseudowire interface, and AC is the attachment circuit interface. 0 is a slot number and 1 is a port number.

Fields (cont)	• Untagged Ports—enter port or set of ports, which should transmit egress packets for the <i>VLAN</i> as untagged packets. Use comma as a separator between the ports while configuring a list of ports. Ports which are attached to <i>VLAN</i>-unaware devices should be configured as untagged-ports for a given <i>VLAN</i>. The untagged ports list should be a sub-set of the <i>VLAN</i> Member Ports. NOTE: The format of this entry is <interface type><slot number/port number> for Gigabit Ethernet ports. For pseudowire and attachment circuit interfaces, the format is just the interface ID. There is no space needed between these two entries. For an example: Gi0/1,Gi0/2,pw1,ac1, where Gi is interface type Gigabit Ethernet, Pw is pseudowire interface, and AC is the attachment circuit interface. 0 is a slot number and 1 is port number. The port can be configured to be an untagged port only if the Switch Port Mode of the port is not set as trunk. The ports configured as untagged ports should be a subset of Member Ports. • Forbidden Ports—enter port or set of ports which should never receive packets from the <i>VLAN</i> mentioned in the <i>VLAN</i> ID. Use comma as a separator between the ports while configuring a list of ports. The ports configured in the Forbidden Ports list should be mutually exclusive to the Member Ports list field. NOTE: The format of this entry is <interface type><slot number/port number> for gigabitethernet ports. For pseudowire and attachment circuit interfaces, the format is just the interface ID. There is no space needed between these two entries. For an example: Gi0/1,Gi0/2,pw1,ac1, where Gi is interface type Gigabit Ethernet, Pw is pseudowire interface, and AC is the attachment circuit interface. 0 is a slot number and 1 is a port number. • Vlan Egress Ethertype—enter the value for egress ether type of a packet. The value set for this object is applicable for a port present in this <i>VLAN</i> only when the value of <i>VLAN</i> PortEgressTPID type is set as Vlanbased for an egress port. The value ranges from 0 to 65535. The default value is 33024. • VLAN ACTIVE—select this check-box to make the configured <i>VLAN</i> active.
Buttons	• Add—adds and saves new configuration • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes. • Delete—deletes the selected entry.

VLAN Protocol Group Settings

Figure 4: VLAN Protocol Group Settings

VLAN Protocol Group Settings

Frame Type *
 Protocol Value *
 Group Identifier *

Select	Frame Type	Protocol Value	Group Identifier
Apply Delete			

Screen Objective	This screen allows the user to create a protocol group with a specific 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.
Navigation	Layer 2 Management > VLAN > Protocol Group
Fields	• Select—click to select the Frame Type for which the Group Identifier needs to be modified or deleted. • Frame Type—select the data-link encapsulation format to be applied in a protocol template. The default option is Ethernet. The list contains: – Ethernet—applies the standard IEEE 802.3 frame format. This format contains the following • 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.

Fields (cont)	• Frame Type—(cont): – SNAP—applies the sub network access protocol (SNAP) 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 Organization Unique Identifier (OUI) 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. – SNAP802.1H—applies 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. – SNAP_OTHER—applies 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 either of the ranges used for RFC_1042 (SNAP) or SNAP 802.1H. – LLC_OTHER—applies 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 for determining the protocol used for the upper layer. • SSAP—1-byte value representing source service access point for determining the protocol used for the upper layer. • Control—1-byte value that is used by certain protocols for administration. NOTE: The option SNAP_OTHER can be used, only if the Protocol Value is set as OTHER.

Fields (cont)	Protocol Value—select the protocol to be applied above the data-link layer in a protocol template. The default option is IP. The protocol identification is internally handled using octet string. The list contains: - IP—sets the protocol as IP, which is used for communicating data across network using <i>TCP/IP</i>. The corresponding octet string is 08:00 - NOVELL—sets the protocol as Novell Netware protocol suite, which is developed by Novell Inc. The corresponding octet string is ff:ff. - NETBIOS—sets the protocol as NetBIOS over <i>TCP/IP</i>, which allows legacy application relying on the NetBIOS API to be used on modern <i>TCP/IP</i> networks. The corresponding octet string is f0:f0. NOTE: This option can be set only for the Frame Type set as LLC_OTHER. - APPLETALK—sets the protocol as AppleTalk, which is a proprietary suite of protocols developed by Apple Inc. The corresponding octet string is 80:9b. - OTHER—sets the protocol as some other protocol other than IP, NOVELL, NETBIOS, and APPLETALK. NOTE: The octet string for the respective protocol can be entered in the text box placed next to this field. This text box is greyed out and cannot be configured if an option other than OTHER is selected. This value is set as 16-bit (2 octet) IEEE 802.3 type field if the field Frame Type is set as Ethernet, SNAP, and SNAP802.1H. This value is set as 40-bit (5 octet) PID if the field Frame Type is set as SNAP_OTHER. This value is set as 2-octet IEEE 802.2 LSAP pair if the field Frame Type is set as LLC_OTHER. The first octet is used for DSAP and the second octet is used for SSA. Group Identifier—enter the group ID that represents a specific group of protocols that are associated together when assigning a VID to a frame. This value ranges from 0 to 2147483647.
Buttons	Add—adds and saves new configuration Reset—resets to default value for respective fields and discards all user inputs. Apply—modifies attributes for the selected entry and saves the changes. Delete—deletes the selected entry.

Port VLAN Protocol Settings

Figure 5: Port VLAN Protocol Settings

Port VLAN Protocol Settings

Port Gi0/1 v
 Group ID *
 VLAN ID *

Add
Reset

Gi0/1 1

Select	Port	Group ID	VLAN ID	Status
☒	1.3.6.1.4	1	1	Up v

Apply
Delete

Note : Please Enter valid Group ID, VLAN ID. To configure Group ID use [ProtocolGroup](#) Page.

Screen Objective	This screen allows the user to configure the VLANID set for a particular port for Port and Protocol Based VLAN classification. Only existing group ID can be assigned for the port. A VLAN ID which is not yet configured can be assigned for a port. When the VLAN is configured, forwarding will take place according to the VID set for the particular port.
Navigation	Layer 2 Management > VLAN > Port Protocol
Fields	Select—click to select the Port for which the Group ID and VLAN ID mapping needs to be modified or deleted Port—select the port to which the VLAN ID and group ID should be mapped. This is a combination of interface type and interface ID. The interface ID is a combination of slot number and port number (slot number/port number). Group ID—enter the group 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. This value ranges from 0 to 2147483647. NOTE: The Group Id entered should have already been created using the Layer 2 Management > VLAN > VLAN Protocol Group Setting Screen VLAN ID—enter the VLAN ID that uniquely identifies a specific VLAN. This VLAN ID is associated with a specific group of protocols for the specific port. This value ranges from 1 to 4094. Status—displays the status of the respective row / entry. This list contains: - Up—denotes the entry is created and operationally up. - Down—denotes the entry is created but operationally down. - Under Creation—denotes the entry is being created and not available for operation / usage.

Buttons	• Add—adds and saves new configuration • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes. • Delete—deletes the selected entry.

VLAN Port Mac Map

Figure 6: VLAN Port Mac Map

VLAN Port mac Map

Port No *
 Port Mac-Map Addr *
 Port Mac-Map Vid *
 Bcast Option ▾

Select	Port No.	Port Mac-Map Addr	Port Mac-Map Vid	Bcast option
☒	Gi0/1	00:11:22:33:44:55	1	Allow ▾

Screen Objective	This screen allows the user to map the <i>VLAN</i> and <i>MAC</i> address for <i>MAC</i> -based <i>VLAN</i> classification.
Navigation	Layer 2 Management > VLAN > Port MAC Map
Fields	• Port No —enter the port to which <i>MAC</i> and <i>VLAN</i> should be mapped. This is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number. The format is <interface type><slot number/port number>. There is no space between these two entries. For an example: Gi0/1, where Gi is interface type Gigabit Ethernet interface, 0 is a slot number, and 1 is a port number. • Port MAC Map Addr—enter the port to which <i>MAC</i> and <i>VLAN</i> should be mapped. This is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number. The format is <interface type><slot number/port number>. There is no space between these two entries. For an example: Gi0/1, where Gi is interface type Gigabit Ethernet interface, 0 is a slot number, and 1 is a port number. • Port MAC Map Vid—enter the <i>VLAN</i> ID that uniquely identifies a specific <i>VLAN</i> to which the <i>MAC</i> address of the port should be mapped. This <i>VLAN</i> ID is associated with a group of protocols for the specific port and it ranges from 1 to 4094. • Bcast Option—select whether the multicast / broadcast untagged frames should be allowed / discarded. The default option is Allow. The list contains:

Fields (cont)	– Allow—drops all multicast / broadcast untagged frames that contain source MAC address belonging to the address configured in the field Port Mac-Map Addr if the <i>MAC Based VLAN</i> is enabled on the port. – Discard—processes all multicast / broadcast untagged frames that contain source <i>MAC</i> address belonging to the address configured in the field Port Mac-Map Addr if the <i>MAC Based VLAN</i> is enabled on the port.
Buttons	• Add—adds and saves new configuration • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes. • Delete—deletes the selected entry.

FDB Flush

Figure 7: FDB Flush

Screen Objective	This screen allows the user to flush all dynamically generated <i>MAC</i> addresses.
NOTE: The output for <i>FDB</i> (File Data Buffer) flush cannot be verified in Web UI as viewing <i>FDB</i> is not implemented there. This can be seen only in <i>CLI</i> .	
Navigation	Layer 2 Management > VLAN > FDB Flush
Fields	• Context Id—enter the virtual context ID for which the <i>MAC</i> addresses need to be flushed. This represents uniquely a virtual switch created in the system. This value ranges from 0 to 65535. The default value is 0. NOTE: The user can create new virtual contexts from the Switch Creation screen (Context Manager—> Switch Creation) • Interface Id—enter the interface ID for which the <i>FDB</i> entries need to be flushed. This is a combination of slot number and the port number. The format is <interface type> <slot number/port number>. There is no space between these two entries. • VLAN ID—enter the VLAN ID for which the <i>FDB</i> entries need to be flushed. This value ranges from 1 to 4094.
Buttons	• Flush—flushes the dynamically generated <i>MAC</i> addresses for a specified interface.

9.2. GARP

This section describes how to configure *GARP* on the switch.

GARP (Generic Attribute Registration Protocol) is used to synchronize attribute information between the bridges in the LAN. It allows to register and de-register attribute values, which are disseminated into the backbone of the *GARP* participants.

To access **GARP** screens, go to **Layer 2 Management > GARP**.

GARP Configuration

Figure 8: GARP Configuration

Select	Context	GARP Status
☒	0	Start

Apply

Configure GARP Trace Options

Note: To Shutdown *GARP*, Dynamic Vlan & Dynamic Multicast should be disabled.

Screen Objective	This screen allows the user to enable <i>GARP</i> status in the Virtual contexts created in the system.
NOTE: To shutdown the <i>GARP</i> functionality: - Dynamic <i>VLAN</i> should be disabled in the Layer 2 Management > Dynamic VLAN > Dynamic Vlan Global Configuration screen - Dynamic Multicast should be disabled using Multicast > GMRP > GMRP Global Configuration screen	
Navigation	Layer 2 Management > GARP

Fields	• Select—click to select the context for starting or shutting down <i>GARP</i> module. • Context—displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This value ranges from 0 to 65535. The default value is 0.
Fields (cont)	• GARP Status—select status requested by management for <i>GARP</i>. The default option is Start for the default context ID (0) and Shutdown for other context IDs. The list contains: – Start—enables <i>GARP</i> in the switch on all ports. <i>GMRP</i> and <i>GVRP</i> are enabled explicitly, once the disabled <i>GARP</i> is enabled. – Shutdown—disables <i>GARP</i> in the switch on all ports NOTE: To shutdown <i>GARP</i> functionality, Dynamic VLAN and Multicast should be disabled in the Dynamic VLAN and GMRP Global Configuration screens.
Buttons	• Apply—modifies attributes and saves the changes. • Configure GARP Trace Option—click to access the <i>GARP</i> Traces ..

GARP Traces

Figure 9: GARP Traces

GARP Traces

GARP Global Trace DISABLE ▾
Submit

Select	Context	Debug Trace Options								Debug Module Options			
		Init-Shut	Management	Memory	Bpdu	Events	Timer	All-Failures	Buffer	GARP	GMRP	GVMRP	Redundancy
☒	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Apply
Configure Global Options

Screen Objective	This screen allows the user to enable the required debug statements required during debug operation.
NOTE: Dynamic VLAN should be disabled in the Layer 2 Management > Dynamic VLAN > Dynamic Vlan Global Configuration screen	
Navigation	Layer 2 Management > GARP > GARP Configuration screen. Click Configure GARP Trace Options button.

Fields	• GARP Global Trace—select the global status of the <i>GARP</i> trace to set the <i>VLAN</i> trace status for all virtual switches in the switch. The list contains: – ENABLE—enables the <i>GARP</i> traces in the switch for all virtual switches. The debug statement is generated for the selected traces. – DISABLE—disables the <i>GARP</i> traces in the switch for all virtual switches. The debug statement is not generated for any of the traces, even if the specific trace is selected. • Select—click to select the context for which the trace levels need to be set. • Context—displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This value ranges from 0 to 65535. The default value is 0. • Debug Trace Options—select traces for which debug statements is needed: – Init-Shut—generates debug statements for init and shutdown traces. This trace is generated on failed initialization and shutting down of <i>GARP</i> related entries. – Management—generates debug statements for management traces. This trace is generated during failure in configuration of any of the <i>GARP</i> features. – Memory—generates debug statements for data path traces. This trace is generated during failure in packet processing. – BPDU—generates debug statements for <i>BPDU</i> traces. This trace is generated during failure in modification or retrieving of <i>GARP</i> entries. – Events—generates debug statements for packet dump traces. This trace is currently not used in <i>GARP</i> module. – Timer—generates debug statements for OS resource related traces. This trace is generated during failure in message queues. – All-Failures—generates debug statements for all failure traces of the above-mentioned traces. – Buffer—generates debug statements for <i>GARP</i> buffer related traces. This trace is currently not used in <i>GARP</i> module. • Debug Module Options—select the module for which debug statements is to be generated. The options are: – GARP—Generates the debug statements for the <i>GARP</i> module. – GMRP—Generates the debug statements for the <i>GMRP</i> module. – GVMRP—Generates the debug statements for the <i>GVRP</i> module. – Redundancy—Generates the debug statements for the <i>GARP</i> redundancy module
Buttons	• Submit—selects the status of the Global Trace and saves the changes. • Apply—modifies attributes and saves the changes. • Configure GARP Trace Option—accesses the <i>GARP</i> Configuration screen.

9.3. Dynamic VLAN

This section describes the Dynamic *VLAN* or *GVRP* features on the switch.

Dynamic VLAN feature (*GVRP*) allows *GVRP* aware devices to dynamically establish and update the information about the existence of the *VLANs* in the topology. It uses the services of *GARP* to propagate *VLAN* registration information to other *VLAN* aware bridges in the LAN. *GVRP* learnt dynamic *VLAN* memberships are stored in *VLAN* current database.

The dynamic *VLAN* feature cannot run in the C-*VLAN* component of a provider edge bridge.

To access **Dynamic VLAN** screens, go to **Layer2 Management > Dynamic VLAN**.

The **Dynamic VLAN** related parameters are configured through the screens displayed by the following tabs:

[Dynamic VLAN Global Configuration](#)

[Dynamic VLAN Port Configuration](#)

[GARP Timers Configuration](#)

[GARP Clear Statistics](#)

Dynamic VLAN Global Configuration

By default, the tab **Dynamic VLAN** displays the **Dynamic VLAN Global Configuration** Screen.

Figure 10: Dynamic VLAN Global Configuration



Screen Objective	This screen allows the user to globally enable/disable dynamic <i>VLAN</i> feature (<i>GVRP</i>) for the virtual contexts available in the switch. To shut down <i>GARP</i> for the specific context, the Dynamic <i>VLAN</i> feature should be disabled
Navigation	Layer 2 Management > Dynamic VLAN > Dynamic VLAN
Fields	Select—click to select the context for which the configuration needs to be done. Context—displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This value ranges from 0 to 65535. The default value is 0.

Fields	• Dynamic VLAN Status—select the administrative status requested by management for <i>GVRP</i>. The default option is Enabled for the default context ID (0) and Disabled for other context IDs. The list contains: – Enabled—enables <i>GVRP</i> on the switch, on all ports for which <i>GVRP</i> is not specifically disabled in the Dynamic <i>VLAN</i> Port Configuration screen. – Disabled—disables <i>GVRP</i> on all ports of the switch and transparently forwards all <i>GVRP</i> packets. NOTE: The administrative status affects all <i>GVRP</i> applicant and registrar state machine. All <i>GVRP</i> state machines on all ports are idle when status is changed from Disabled to Enabled.
Buttons	• Apply—modifies attributes and saves the changes.

Dynamic VLAN Port Configuration

Figure 11: Dynamic VLAN Port Configuration

Dynamic Vlan Port Configuration

Select	Port	Dynamic Vlan Status	Restricted VLAN Registration
☐	Gi0/1	Disabled ▾	Disabled ▾
☐	Gi0/2	Disabled ▾	Disabled ▾
☐	Gi0/3	Disabled ▾	Disabled ▾
☐	Gi0/4	Disabled ▾	Disabled ▾
☐	Gi0/5	Disabled ▾	Disabled ▾
☐	Gi0/6	Disabled ▾	Disabled ▾
☐	Gi0/7	Disabled ▾	Disabled ▾
☐	Gi0/8	Disabled ▾	Disabled ▾
☐	Gi0/9	Disabled ▾	Disabled ▾
☐	Gi0/10	Disabled ▾	Disabled ▾
☐	Gi0/11	Disabled ▾	Disabled ▾
☐	Gi0/12	Disabled ▾	Disabled ▾
☐	Gi0/13	Disabled ▾	Disabled ▾
☐	Gi0/14	Disabled ▾	Disabled ▾
☐	Gi0/15	Disabled ▾	Disabled ▾
☐	Gi0/16	Disabled ▾	Disabled ▾
☐	Gi0/17	Disabled ▾	Disabled ▾
☐	Gi0/18	Disabled ▾	Disabled ▾
☐	Gi0/19	Disabled ▾	Disabled ▾
☐	Gi0/20	Disabled ▾	Disabled ▾
☐	Gi0/21	Disabled ▾	Disabled ▾
☐	Gi0/22	Disabled ▾	Disabled ▾
☐	Gi0/23	Disabled ▾	Disabled ▾
☐	Gi0/24	Disabled ▾	Disabled ▾
☐	Ex0/1	Disabled ▾	Disabled ▾
☐	Ex0/2	Disabled ▾	Disabled ▾
☐	Ex0/3	Disabled ▾	Disabled ▾
☒	Ex0/4	Disabled ▾	Disabled ▾

Screen Objective	This screen allows the user to configure the dynamic <i>VLAN</i> feature related parameters for every physical port available in the switch.
Navigation	Layer 2 Management > Dynamic VLAN > Port Settings
Fields	• Select—click to select the context for which the configuration needs to be done. • Context—displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This value ranges from 0 to 65535. The default value is 0. • Dynamic VLAN Status—select the state of <i>GVRP</i> operation in the port. This state affects all <i>GVRP</i> applicant and registrar state machines in the port. All <i>GVRP</i> state machines in the port are reset once the state is changed from Disabled to Enabled. The default option is Enabled on all physical ports. The list contains: – Enabled—enables <i>GVRP</i> in the port, only if Dynamic <i>VLAN</i> Status is globally enabled. Otherwise <i>GVRP</i> is not enabled in the port. Once the Dynamic <i>VLAN</i> Status is globally disabled, <i>GVRP</i> enabled in the port is also disabled. – Disabled—disables <i>GVRP</i> in the port, even if the dynamic <i>VLAN</i> feature (Dynamic <i>VLAN</i> Status) is globally enabled. Silently discards any received <i>GVRP</i> packets and does not propagate <i>GVRP</i> registrations from other ports. • Restricted VLAN Registration—displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This value ranges from 0 to 65535. The default value is 0. – Enabled—enables restricted <i>VLAN</i> registration. That is, the creation or modification of a dynamic <i>VLAN</i> entry is permitted only for <i>VLAN</i> for which static <i>VLAN</i> registration entries exist. – Disabled—disables restricted <i>VLAN</i> registration. That is, the creation or modification of a dynamic <i>VLAN</i> entry is permitted for all <i>VLAN</i>s.
Buttons	• Apply—modifies attributes and saves the changes.

GARP Timers Configuration

Figure 12: GARP Timers Configuration

Garp Timers Configuration

Select	Port No	GarpJoinTime (msecs)	GarpLeaveTime (msecs)	GarpLeaveAllTime (msecs)
☐	Gi0/1	200	600	10000
☐	Gi0/2	200	600	10000
☐	Gi0/3	200	600	10000
☐	Gi0/4	200	600	10000
☐	Gi0/5	200	600	10000
☐	Gi0/6	200	600	10000
☐	Gi0/7	200	600	10000
☐	Gi0/8	200	600	10000
☐	Gi0/9	200	600	10000
☐	Gi0/10	200	600	10000
☐	Gi0/11	200	600	10000
☐	Gi0/12	200	600	10000
☐	Gi0/13	200	600	10000
☐	Gi0/14	200	600	10000
☐	Gi0/15	200	600	10000
☐	Gi0/16	200	600	10000
☐	Gi0/17	200	600	10000
☐	Gi0/18	200	600	10000
☐	Gi0/19	200	600	10000
☐	Gi0/20	200	600	10000
☐	Gi0/21	200	600	10000
☐	Gi0/22	200	600	10000
☐	Gi0/23	200	600	10000
☐	Gi0/24	200	600	10000
☐	Ex0/1	200	600	10000
☐	Ex0/2	200	600	10000
☐	Ex0/3	200	600	10000
☒	Ex0/4	200	600	10000

Apply

Screen Objective	This screen allows the user the user to configure the timer used in <i>GARP</i> on physical ports available in the switch. <i>GARP</i> uses these timer values to control transmission of <i>GARP</i> PDUs used in synchronizing the attribute information between the switches and in registering and de-registering of attribute values.
Navigation	Layer 2 Management > Dynamic VLAN > GARP Timers
Fields	• Select—click to select the port for which the configuration needs to be done. • Port No—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number). • GarpJoinTime (msecs)—enter the time duration till which a <i>GARP</i> participant must 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 timer is started when the initial join message is sent. The join message is sent by a <i>GARP</i> participant to another <i>GARP</i> participant for registering: – Its attributes with another participant – Its manually configured attributes – Attributes received from a third <i>GARP</i> participant This value is represented in milliseconds. The default value is 200. The value can only be set as multiple of tens (e.g., 210, 220, 230 and so on). This value should satisfy the condition: $\text{GarpJoinTime} > 0$ and $(2 * \text{GarpJoinTime}) < \text{GarpLeaveTime}$ • GarpLeaveTime (msecs)—enter the time duration till which a <i>GARP</i> participant must 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 timer is started when a leave message is sent to de-register the attribute details. The leave messages are sent from one <i>GARP</i> participant to another one as follows: – Its attributes should be de-registered – Its attributes are manually de-registered – leave messages are received from a third <i>GARP</i> participant • GarpLeaveAllTime (msecs)—enter the time period during 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 <i>GARP</i> participant to other <i>GARP</i> participants, after this time interval. This timer is started once a <i>GARP</i> participant started or re-registration is done. The leaveall messages are sent from a <i>GARP</i> participant to other participants for: – De-registering all registered attributes – Re-registering all attributes with each of the participants. This value is represented in milliseconds. The default value is 10000. You can set the value as multiple of tens (that is, as 10010, 10020, and so on). – The leave all time should be greater than 0 and greater than GarpLeaveTim
Buttons	• Apply—modifies attributes and saves the changes.

GARP Clear Statistics

Figure 13: GARP Clear Statistics

GARP CLEAR STATISTICS

Clear garp Statistics ☐ All
☒ Interface

Interface Gi0/1 ▼

Apply

Screen Objective	This screen allows the user to clear the <i>GARP</i> statistics for a specified interface or all interfaces
Navigation	Layer 2 Management > Dynamic VLAN > Garp Clear Stats
Fields	• Clear garp Statistic—click to select which <i>GARP</i> statistics have to be cleared. – All—clears the <i>GARP</i> statistics for all port information in the switch – Interface—clears the <i>GARP</i> statistics for the specified interface in the switch • Interface—select the interface which clears the <i>GARP</i> counters on the switch. NOTE: This field is greyed out when the Clear <i>GARP</i> Statistics option is All.
Buttons	• Apply—modifies attributes and saves the changes.

Spanning Tree Map

10. Spanning Tree Protocols

This section describes the Web Interfaces for *RSTP*, *MSTP* and *PVRSTP* protocols.

10.1. RSTP

This section describes how to configure Rapid Spanning Tree Protocol (*RSTP*) on the switch.

RSTP (Rapid Spanning Tree Protocol) is 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 for reconfiguring the active topology of the network when physical topology or topology configuration parameters change. It provides increased availability of *MAC* service when there is a reconfiguration or failure of components in a bridged *LAN*. It can inter-operate with legacy *STP* bridges without any change in the configuration. This is the switch's default spanning tree algorithm.

The *RSTP* provides an optional capability for:

- High availability
- Executing multiple instances of the protocol
- Provider bridging

To access **RSTP** screens, go to **Layer2 Management > RSTP**.

The **RSTP** related parameters are configured through the screens displayed by the following tabs:

[Global Information](#)

[RSTP Traces](#)

[RSTP Configuration](#)

[Port Status Configuration](#)

[RSTP Port Status](#)

Global Information

By default, the tab **Global Settings** displays the **Global Configuration** screen.

Global Information

Global Configuration

Select	Context Id	System Control	Status	Dynamic Path Cost Calculation	Speed Change Path Cost Calculation	Flush Interval	Flush Indication Threshold	BPDU Guard
☒	0	Start ▾	Enabled ▾	False ▾	False ▾	0	0	Disable ▾

Apply

Configure Trace Options

Note : To enable RSTP Functionality, **MSTP** and **PVRST** should be disabled.

Screen Objective	This screen allows the user to configure for each available virtual context the MST module parameters that are used globally in the switch for all ports.
NOTE: To enable RSTP, MSTP and PVRSTP should be disabled in the selected context.	
Navigation	Layer 2 Management > RSTP > Global Settings

Fields	• Select—click to select the context for which the configuration needs to be done. • Context—displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This is a read-only field. This value ranges from 0 to 65535. The default value is 0. • System Control—select the administrative shutdown status requested by management for the <i>RSTP</i> feature. The default option is Shutdown. The list contains: – Start—specifies that all resources required by <i>RSTP</i> should be allocated and <i>RSTP</i> should be supported in the device on all ports. – Shutdown—specifies that <i>RSTP</i> should be shutdown in the device on all ports and all allocated memory must be released. NOTE: The administrative status can be set as Shutdown, only if the <i>RSTP</i> Status is set as Disabled. The status can be set as Start, only if the <i>MSTP</i> System Control and <i>PVRST</i> System Control are set as Shutdown using the Layer 2 Management > <i>MSTP</i> > Global Configuration and Layer 2 Management > <i>PVRST</i> > Global Configuration screen respectively. • Status—select the administrative module status requested by management for the <i>RSTP</i> module. <i>RSTP</i> provides rapid recovery of connectivity following the failure of a bridge/bridge port or a <i>LAN</i>. The default option is Disabled. The list contains: – Enabled—enables the <i>RSTP</i> in the device on all ports. – Disabled—disables the <i>RSTP</i> in the device on all ports. NOTE: <i>RSTP</i> can be enabled globally in the switch, only if the <i>RSTP</i> System Control status is set as Start. • Dynamic Path Cost Calculation—select whether the dynamic path cost calculation is allowed. The path cost represents the distance between the root port and designated port. The path cost is based on a guideline established as part of 802.1d. According to the specification, path cost is calculated by dividing the speed with bandwidth of the segment connected to the port. The default option is False. The list contains: – True—dynamically calculates path cost based on the speed of the ports whose Admin State is set as Up at that time. The path cost is not changed based on the operational status of the ports once calculated. – False—dynamically calculates path cost based on the link speed at the time of port creation. NOTE: The manually assigned path cost is used irrespective of the status (True or False) of the dynamic path cost calculation. This field cannot be configured if the <i>RSTP</i> System Control is shut down or Status is set as Disabled.

Fields (cont)	• Speed Change Path Cost Calculation—select whether the speed change path cost calculation is allowed or not. The speed change path cost is to be calculated for ports whose speed changes dynamically. This feature is mainly used for Link Aggregation ports whose speed changes due to the addition and deletion of ports from the port channel. The default option is False. The list contains: – True—specifies that path cost is dynamically calculated for ports based on their speed at that time. It is calculated if the speed of the port changes. – False—specifies that path cost is not dynamically calculated for ports based on their speed at that time. NOTE: This field can be configured only if System Control is set as Start. The manually assigned path cost is used irrespective of the status (True or False) of the dynamic path cost calculation. • Flush Interval—enter the value that controls the number of flush indications invoked from spanning-tree module per instance basis. This value ranges from 0 to 500 centi-seconds. The default value is 0. NOTE: This field can be configured only if System Control is set as Start. If the flush interval timer is set to zero, port based flushing occurs (default functionality). If it is set to non-zero, global / port based flushing occurs and is dependent on the flush-indication-threshold value. • Flush Indication Threshold—enter the number of flush indications to go before the flush-interval timer method triggers. This value ranges from 0 to 65535. The default value is 0. NOTE: This field can be configured only if System Control is set as Start. 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. • BPDU Guard—select the administrative status for the <i>BPDU</i> guard feature in the port. This feature configures <i>BPDU</i> guard globally in <i>MSTP</i>. This global <i>BPDU</i> is applicable if and only no port specific <i>BPDU</i> Guard is configured. The default option is Disable. The list contains: – Enabled—enables <i>BPDU</i> Guard feature on edge ports globally and moves the port to disabled discarding state when <i>BPDU</i> is received on the edge ports – Disabled—disables <i>BPDU</i> Guard feature on edge ports globally.
Buttons	• Apply—modifies attributes and saves the changes. • Configure Trace Options—click to access the <i>RSTP</i> Traces screen

RSTP Traces

Figure 1: RSTP Traces

RSTP Traces

Traces

☐ Init-Shut

☐ Management

☐ Memory

☐ Bpdu

☐ Events

☐ Timer

☐ Redundancy

☐ Semaphore

☐ Errors

State Machine

☐ Port-Info

☐ Port-Receive

☐ Port-Role-Select

☐ Role-Transition

☐ State-Transition

☐ Protocol-Migration

☐ Topology-Change

☐ Port-Transmit

☐ Bridge-Detection

☐ Pseudo-Info

Screen Objective	This screen allows the user to enable the required debug statements for <i>RSTP</i> module that will be useful during debug operation.
Navigation	Layer 2 Management > RSTP > Global Settings > Global Configuration screen. Click Configure Trace Options .
Fields	Traces—select the traces for which debug statements is to be generated. The options are: - Init-Shut—generates debug statements for init and shutdown traces. This trace is generated on failed and successful initialization and shutting down of <i>STP</i> related module and memory. - Management—generates debug statements for management traces. - Memory—generates debug statements for memory related traces. This trace is generated on failed and successful allocation of memory for <i>STP</i> process. - BPDU—generates debug statements for <i>BPDU</i> related traces. This trace is generated on failed and successful reception, transmission and processing of <i>BPDU</i>s. - Events—generates debug statements for event handling traces. This trace is generated to denote events that are posted to <i>STP</i> configuration queue whenever you configure any of the <i>STP</i> features.

Fields (cont)	• Traces—the options are (cont): – Timer—generates debug statements for timer module traces. This trace is generated on failed and successful start, stop and restart of <i>STP</i> timers. The different <i>STP</i> timers are: • Forward delay timer • Hello timer • Migration delay timer • Recent backup while timer • Received information while timer • Recent root while timer • Topology change timer • Hold timer • Edge delay timer • Rapid age duration timer • Pseudo information hello timer – Redundancy—generates debug statements for redundancy code flow traces. This trace is generated in standby node <i>STP</i> while taking backup of configuration information from active node. – Semaphore—generates debug statements for state machine variable changes traces. This trace is generated on failed and successful creation and deletion of semaphore. – Errors—generates debug statements for all failure traces of the traces. • State Machine—select the <i>SEMs</i> (State Event Machines) for which debug statements are to be generated to denote the event and state of the selected <i>SEM</i>. The options are: – Port-Info—generates debug statements for port information <i>SEM</i>. – Port-Receive—generates debug statements for port receive <i>SEM</i>. – Port-Role-Select—generates debug statements for role selection <i>SEM</i>. – Role-Transition—generates debug statements for role transition <i>SEM</i>. – State-Transition—generates debug statements for state transition <i>SEM</i>. – Protocol-Migration—generates debug statements for protocol migration <i>SEM</i>. – Topology-Change—generates debug statements for topology change <i>SEM</i>. – Port-Transmit—generates debug statements for port transmit <i>SEM</i>. – Bridge-Detection—generates debug statements for bridge detection <i>SEM</i>. – Pseudo-Info—generates debug statements for port receive pseudo information <i>SEM</i>.
Buttons	• Apply—modifies attributes and saves the changes. • Configure Global Options—accesses Global Configuration screen

RSTP Configuration

Figure 2: RSTP Configuration

RSTP Configuration

Select	Context Id	Priority	Version	Tx Hold Count	Max Age	Hello Time	Forward Delay
☒	0	32768	RSTP Compatible ▾	6	20	2	15

Screen Objective	This screen allows the user to configure the bridge priority to be assigned to the specified <i>VLAN</i> .
NOTE: Bridge Priority can be configured only if <i>MSTP</i> Instance is created using the <i>VLAN Mapping</i> screen	
Navigation	Layer 2 Management > RSTP > Basic Settings
Fields	• Select—select the <i>MSTP</i> Instance ID for which the configuration needs to be applied. • Context Id—displays the context ID. • Priority—enter the priority value that is assigned to the switch. In <i>RSTP</i>, this value is used during the election of root. This value ranges from 0 to 61440. The default value is 32768. The values set for the priority must be in increments of 4096, e.g., 4096, 8192, 12288, etc • Version—select the mode of <i>STP</i> in which the port is currently operating. The compatibility version allows the switch to operate temporarily (that is, till this configuration is reset manually) in other <i>STP</i> versions even though the spanning tree mode is set as some other version. This configuration is useful during cases where spanning tree mode itself is not required to be changed. The default option is <i>RSTP</i> Compatible. The list contains: – <i>STP</i> Compatible—specifies that the mode is set as <i>STP</i> compatible i.e. it transmits Config/TCN BPDUs. – <i>RSTP</i> Compatible—specifies that the mode is set as <i>RSTP</i> compatible i.e. it transmits RST BPDUs. • Tx Hold Count—enter the transmit hold count which is the number of RST BPDUs that can be transmitted in a given interval. This value is configured to avoid flooding. Port transmit state machine uses this value to limit the maximum transmission rate. This value ranges from 1 to 10. The default value is 6.

Fields	• Max Age—enter the maximum expected arrival time (in seconds) of Hello <i>BPDUs</i>. <i>STP</i> 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. This value ranges from 6 to 40 seconds. The default value is 20. NOTE: The maximum age should be lesser than or equal to 2*(Forward Delay—1.0) and should be greater than or equal to 2*(HelloTime + 1.0). • Hello Time—enter the amount of time between the transmission of configuration bridge PDUs by this node. This value can be either 1 or 2 seconds. The default is 2. • Forward Delay—enter the value that all bridges use for ForwardDelay when the bridge is acting as the root. This value is the number of seconds for which a port waits before changing from the blocking state to the forwarding state. This value ranges from 4 to 30 seconds. The default value is 15.
Buttons	• Apply—modifies attributes and saves the changes.

Port Status Configuration

Figure 3: Port Status Configuration

Port Status Configuration																		
Select	Port	Port Role	Port Priority	RSTP Status	Path Cost	Protocol Migration	Admin Edge Port	Admin Point To Point	Auto Edge Detection	Restricted Role	Restricted TCN	Bpdu Receive	Bpdu Transmit	Layer2 Gateway Port	Loop Guard	Root Guard	Bpdu Guard	Error Recovery
☐	Gi0/1	Root	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/2	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/3	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/4	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/5	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/6	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/7	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/8	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/9	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/10	Designated	128	Enable	200000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/11	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/12	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/13	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/14	Designated	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/15	Designated	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/16	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/17	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/18	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/19	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/20	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/21	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/22	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/23	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Gi0/24	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Ex0/1	Disabled	128	Enable	2000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Ex0/2	Disabled	128	Enable	2000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☐	Ex0/3	Disabled	128	Enable	2000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000
☒	Ex0/4	Disabled	128	Enable	2000	False	False	Auto	True	False	False	True	True	False	False	False	None	30000

Screen Objective	This screen allows the user to configure the port information for <i>RSTP</i> used during computation of loop-free topology.
Navigation	Layer 2 Management > RSTP > Port Settings
Fields	• Select—click to select the port for which the configuration needs to be applied. • Port—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of a slot number and a port number (slot number/port number). NOTE: Only the ports whose Admin State is set as Up are displayed. • Port Role—displays the current role of the port for the spanning tree. The values can be: – Disabled—specifies that the port is disabled manually (<i>RSTP</i> Status) or automatically (Link). It does not take part in the spanning tree process. – Alternate—specifies that the port is acting as an alternate path to the root bridge. It is blocked and not used for traffic. It is enabled and declared as the root port if the root port is blocked. – Backup—specifies that the port is acting as a backup path to a segment where another bridge port already connects. The port is blocked and not used for traffic, and it is enabled and declared as the designated port if the active designated port is blocked. – Root—specifies that the port is used to forward data to root bridge directly or through an upstream <i>LAN</i> segment. – Designated—specifies that the port is used to send and receive packets to/from a specific downstream <i>LAN</i> segment/device. Only one designated port is assigned for every segment. • Port Priority—enter the priority value that is assigned to the port. This value is used during the Port Role selection process. This value ranges from 0 to 240. The default value is 128. This value should be set in steps of 16, e.g., 0, 16, 32, 48, etc. • RSTP Status—select the administrative module status requested by management for the <i>RSTP</i> Module on the port. This enables or disables <i>RSTP</i> status of the port. The default option is Enable. The list contains: – Enable—enables <i>RSTP</i> in the device on the port. The port participates in the <i>STP</i> process and is ready to transmit/receive <i>BPDUs</i> and data. – Disable—disables <i>RSTP</i> in the device on the port. The port does not participate in the <i>STP</i> process and is not ready to transmit / receive <i>BPDUs</i> and data. • Path Cost—enter the path cost that contributes to the path cost of paths containing the 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. This value ranges from 0 to 2000000000. The default value is 200000 for all physical ports and 199999 for port channels.

Fields	NOTE: The default value is used as the path cost if this field is not configured, and the Dynamic Path Cost Calculation and Speed Change Path Cost Calculation are set as False. The dynamically calculated path cost is used if the path cost is not manually configured, and one of these Fields is set as True. The configured value is used as the path cost irrespective of the status (True or False) of the Dynamic Path Cost Calculation and Speed Change Path Cost Calculation. The path cost value is calculated automatically based on the port speed maintained by CFA module if the value is set as 0. • Protocol Migration—select the protocol migration state of the port. This is used for controlling of the protocol migration mechanism that enables the module to interoperate with legacy 802.1D switches. The default option is False. The list contains: – True—specifies that the port transmits <i>BPDUs</i> based on the spanning tree protocol supported by the receiving switch. The port is forced to transmit <i>RSTP BPDUs</i>. – False—specifies that the port does not perform protocol migration mechanism. The port always transmits the standard <i>RSTP BPDUs</i>. NOTE: This field cannot be configured if the <i>RSTP Status</i> is set as Disable. The protocol migration triggers the transmission of <i>RSTP BPDUs</i> only once when set as True. The protocol migration changes automatically as False, once the <i>RSTP BPDUs</i> is transmitted. • Admin Edge Port—select the administrative status of the Edge Port parameter. The default option is False. The list contains: – True—sets the port as an edge port. The Port State is immediately set as forwarding. It is connected directly to a single end station. It allows <i>RSTP</i> to converge faster and does not wait to receive <i>BPDUs</i>. – False—sets the port as a non-Edge port. The spanning tree process is performed using the <i>RSTP</i>. It is connected to a routing device such as switch. NOTE: The value of the Edge Port parameter is automatically updated if the Auto Edge Detection is set as True • Admin Point-to-Point—select the administrative point-to-point status of the LAN segment attached to the port. The default option is Auto. The list contains: – Forcetrue—specifies that port is connected to a point-to-point link. – Forcefalse—specifies that port is having a shared media connection. – Auto—specifies that the ports as having a shared media connection, or a point-point link based on the prevailing conditions. NOTE: Port is considered to have a point-to-point link if: – It is an aggregator and all its members can be aggregated. – The <i>MAC</i> entity is configured for full Duplex operation, either manually or through auto negotiation process (negotiation Mode is set as Auto).

Fields (cont)	• Auto Edge Detection—select whether the Edge Port parameter of the port is detected automatically or configured manually. The default option is True. The list contains: – True—specifies that detection of port as Edge Port happens automatically. The port is set as edge port, if no <i>BPDU</i> is received on the port. The port is set as non-edge port, if any <i>BPDU</i> is received by that port. This overrides the value set in the field Admin Edge Port, based on the reception of <i>BPDU</i>. – False—specifies that automatic detection of edge port is disabled. This uses the manually configured value for the Edge Port parameter. • Restricted Role—select whether the selection of port Role as root can be blocked during the role Selection process. This feature allows the user to block switches external to a core region of the network from influencing the spanning tree active topology. The default option is False. The list contains: – True—blocks the port from being selected as root port for the topology even if it has the best spanning tree priority vector. It is selected as an alternate port after the root port is selected. NOTE: The blocking of port from being selected as a root port may cause lack of spanning tree connectivity. – False—includes all available ports of the topology, in the root selection process to select the port. • Restricted TCN—select the status of transmission of the received topology change notifications and topology changes to the other ports in the network. This feature allows the user to block switches external to a core region of the network from causing address flushing in the region. The default option is False. The list contains: – True—blocks the port from propagating the received topology change notifications and topology changes to other ports. NOTE: The blocking of port may cause temporary loss of connectivity after changes in a spanning tree active topology as a result of persistent incorrectly learnt station location information. – False—allows the port to propagate the received topology change notifications and topology changes to other ports. • BPDU Receive—select the processing status of the received <i>RSTP BPDUs</i>. The default option is True. The list contains: – True—normally processes the <i>RSTP BPDUs</i> received on the port. – False—discards the <i>RSTP BPDUs</i> received on the port. • BPDU Transmit—select the <i>BPDU</i> transmission status of the port. The default option is True. The list contains: – True—specifies that <i>RSTP BPDUs</i> are transmitted from the port. – False—specifies that <i>RSTP BPDUs</i> transmission is blocked from the port. NOTE: This field should be set as False for ports to be configured as Layer-2 Gateway Port.

Fields (cont)	• Layer 2-Gateway Port—select whether the port acts as a normal port or as a L2GP. The default option is False. The list contains: – True—specifies that the port operates as a Layer 2 Gateway Port. – False—specifies that the port operates as a normal port. NOTE: <i>BPDUs</i> Transmit, Restricted Role and Restricted <i>TCN</i> should be set as False before configuring the port as a Layer 2 gateway port. L2GP operates similarly to that of the normal port operation but pretends to continuously receive <i>BPDUs</i> when Admin State is set to Up. • Loop Guard—select the status of loop guard. The Loop Guard does age out the information even if the peer does not send information. If the port continues to receive information through <i>BPDUs</i>, the operation on this port will be normal. This is useful when the neighbor bridge is faulty; that is, the bridge cannot send <i>BPDUs</i> but continues to send data traffic. The default option is False. The list contains: – True—enables the loop guard in the port. – False—disables the loop guard in the port. • Root Guard—select the administrative status for the root guard feature in the port. When enabled, this feature causes the port not to be selected as Root Port for the topology, even if it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. The default option is Disabled, and this can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology; possibly because those bridges are not under the full control of the administrator. – Enabled—enables root guard feature in the port. – Disabled—disables root guard feature in the port. NOTE: The root guard feature can be enabled only for the ports whose Switch Port Mode is configured as Trunk using Layer 2 Management > Port Manager > Port Basic Settings screen. • BPDUs Guard—the administrative status for the <i>BPDUs</i> guard feature in the port. This feature configures <i>BPDUs</i> guard globally in <i>RSTP</i> and this global <i>BPDUs</i> is applicable if and only if no port specific <i>BPDUs</i> Guard is configured. The default option is Disable. The list contains: – Enabled—enables <i>BPDUs</i> Guard feature on edge ports globally and moves the port to disable discarding state when <i>BPDUs</i> is received on the edge ports – Disabled—disables <i>BPDUs</i> Guard feature on edge ports globally. • Error Recovery—enter the amount of time to bring the interface out of the error-disabled (err-disabled) state. This value ranges from 30 to 65535 seconds. The default value is 30.
Buttons	• Apply—modifies attributes and saves the changes.

RSTP Port Status

Figure 4: RSTP Port Status

RSTP Port Status							
Port	Designated Root	Designated Cost	Designated Bridge	Designated Port	Type	Role	Port State
Gi0/1	80:00:e8:e8:75:00:07:db	0	80:00:e8:e8:75:00:07:db	80:10	Point-to-Point	Root	Forwarding
Gi0/2	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/3	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/4	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/5	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/6	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/7	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/8	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/9	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	Point-to-Point	Disabled	Discarding
Gi0/10	80:00:e8:e8:75:00:07:db	20000	80:00:e8:e8:75:90:25:81	80:0a	Point-to-Point	Designated	Forwarding
Gi0/11	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/12	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/13	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/14	80:00:e8:e8:75:00:07:db	20000	80:00:e8:e8:75:90:25:81	80:0e	Point-to-Point	Designated	Forwarding
Gi0/15	80:00:e8:e8:75:00:07:db	20000	80:00:e8:e8:75:90:25:81	80:0f	Point-to-Point	Designated	Forwarding
Gi0/16	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/17	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/18	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/19	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/20	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/21	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/22	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/23	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Gi0/24	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Ex0/1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	Point-to-Point	Disabled	Discarding
Ex0/2	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	Point-to-Point	Disabled	Discarding
Ex0/3	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	Point-to-Point	Disabled	Discarding
Ex0/4	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	Point-to-Point	Disabled	Discarding

Screen Objective	This screen allows the user to view information maintained by every port of the switch for <i>RSTP</i> .
Navigation	Layer 2 Management > RSTP > Port Status
Fields	• Port—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of a slot number and a port number (slot number/port number). • Designated Root—displays the unique identifier of the bridge recorded as the CIST root in the transmitted configuration BPDUs. This value is an 8-byte octet string. For example, 80:00:00:01:02:03:04:05 • Designated Cost—displays the Path Cost of the Designated Port of the segment connected to the port. This value ranges from 1 to 200000000. • Designated Bridge—displays the unique identifier of the bridge, which the port considers to be the designated bridge for the port's segment. The designated bridge is the only bridge allowed to forward frames to and from the segment. This value is an 8-byte octet string. For example, 80:00:00:01:02:03:04:05.

Fields (cont)	• Designated Port—displays the identifier of the port on the Designated Bridge for the port's segment and represents the port through which the Designated Bridge forwards frames. This value is a 2-byte octet string e.g. 80:05. • Type—displays the operational Admin Point to Point of the LAN segment attached to the port. The values can be: – Point-to-point—specifies that the port is treated as if it is connected to a point-to-point link.. – SharedLan—specifies that the port is treated as if it is having a shared media connection. NOTE: The values can be set directly or as Auto for the switch to decide about the point-to-point status, in the field Admin Point to Point provided in the screen Port Status Configuration. • Role—displays the current role of the port for the spanning tree instance. The values can be: – Disabled—specified that the port is disabled manually (Port State) or automatically (Link status in Layer 2 Management > Port Manager > Basic Settings). It does not take part in the spanning tree process. – Alternate—specifies that the port is acting as an alternate path to the root bridge (i.e. it is blocked and not used for traffic). The alternate port is enabled and declared as a root port if the current root port is blocked. – Backup—specifies that the port is acting as a backup path to a segment where another bridge port already connects (i.e. it is blocked and not used for traffic). The backup port is enabled and declared as a designated port if the active designated port is blocked. – Root—specifies that the port is used to forward data to root bridge directly or through an upstream LAN segment. – Designated—specifies that the port is used to send and receive packets to/from a specific downstream LAN segment/device. Only one designated port is assigned for each segment. • Port State—displays the current state of the port as defined by the common STP. The values can be: – Disabled—specifies that the port is disabled manually (Port State) or automatically (Link). It does not take part in the spanning tree process. – Discarding—specifies that the port is in Discarding state i.e. No user data is sent over the port. – Learning—specifies that the port is in the Learning state i.e. the port is not forwarding frames yet, but is populating its MAC-address-table by learning source addresses from received frames and storing them in the switching database for using these details while sending and receiving data. – Forwarding—specifies that the port is in Forwarding state i.e. the port is operational by sending and receiving data based on the formed spanning tree topology which is loop-free.

10.2. MSTP

This section describes how to configure Multiple Spanning Tree Protocol (*MSTP*) on the switch.

MSTP (Multiple Spanning Tree Protocol) is used to configure spanning tree on per *VLAN* basis or multiple *VLANs* per spanning tree. It allows the user to build several *MST* over *VLAN* trunks and a 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.

The *MSTP* provides an optional capability for:

- High availability
- Executing multiple instances of the protocol
- Provider bridging

To access **MSTP** screens, go to **Layer2 Management > MSTP**.

The **MSTP** related parameters are configured through the screens displayed by the following tabs:

[Global Information](#)

[MSTP Traces](#)

[MSTP Timers](#)

[Port Configuration - CIST Settings](#)

[VLAN Mapping](#)

[Port Settings](#)

[MSTP CIST Port Status](#)

[Bridge Priority](#)

Global Information

By default, the tab **Basic Settings** displays the **Global Configuration** screen.

Figure 5: Global Information

Global Configuration

Select	Context Id	System Control	MSTP Status	Maximum MST Instances	Bridge Priority	Protocol Version	Region Name	Region Version	Dynamic Path Cost Calculation	Speed Change Path Cost Calculation	Flush Interval	Flush Indication Threshold	BPDU Guard
☒	0	Shutdown ▾	Disabled ▾	0	0	MSTP ▾		0	▾	▾	0	0	▾

Note : To enable *MSTP* Functionality, *RSTP* and *PVRST* should be disabled.

Screen Objective

This screen allows the user to configure for each available virtual context the *MST* module parameters that are used globally in the switch for all ports.

NOTE: To enable *MSTP*, *RSTP* and *PVRSTP* should be disabled in the selected context.

Navigation	Layer 2 Management > MSTP > Basic Settings
Fields	• Select—click to select the context for which the configuration needs to be done. • Context Id—displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This value ranges from 0 to 65535. The default value is 0. • System Control—select the administrative shutdown status requested by management for the <i>MSTP</i> module. The default option is Start for the default context and shutdown for the other contexts. The list contains: – Start—specifies that <i>MSTP</i> is active in the device on all ports. – Shutdown—specifies that <i>MSTP</i> is shutdown in the device on all ports, and all allocated memory is release NOTE: The administrative status can be set as Shutdown, only if the <i>MSTP</i> Status is set as Disabled. The status can be set as Start, only if the <i>RSTP</i> System Control and <i>PVRST</i> System Control are set as Shutdown using the Layer 2 Management > <i>RSTP</i> > Global Configuration and Layer 2 Management > <i>PVRST</i> > Global Configuration screen respectively. <i>MSTP</i> System Control cannot be shutdown if <i>MSTP</i> status is enabled. • MSTP Status—select the administrative status requested by management for the <i>MST</i> feature. <i>MSTP</i> is used to configure spanning tree on per <i>VLAN</i> basis or multiple <i>VLANs</i> per spanning tree. It provides multiple forwarding paths for data traffic and enables load balancing. The default option is Enabled for the default context and Disabled for the other contexts. The list contains: – Enabled—enables <i>MST</i> in the device on all ports. – Disabled—disables <i>MST</i> in the device on all ports NOTE: To enable <i>MSTP</i> globally in the switch, the <i>MSTP</i> System Control status should be set as Start. All fields in this screen (except System Control) are greyed out and cannot be configured, once the <i>MSTP</i> status is set as Disabled. • Maximum MST Instances—enter the maximum number of spanning trees to be allowed in the switch. This value represents the maximum number of active <i>MSTIs</i> (<i>MST</i> Instances) that can be created. This allows the user to limit the number of spanning tree instances to be allowed in the switch. This does not count the special <i>MSTID</i> such as <i>PTETID</i> (Provider Backbone Bridging—Traffic Engineering Multiple Spanning Tree ID), which is used to identify <i>VIDs</i> used by Ethernet switched paths (<i>ESPs</i>). This value ranges from 1 to 64. The default value is 64. NOTE: The maximum available number of instances is 16 (values from 0–15 where 0 being <i>CIST</i>). • Bridge Priority—enter the priority value that is assigned to the switch. This value is used during the election of <i>CIST</i> root, <i>CIST</i> regional root and, <i>IST</i> root. This value ranges from 0 to 61440. The default value is 32768. The values set for Bridge Priority must be in steps of 4096.

Fields (cont)	• Protocol Version—select the version of <i>STP</i> in which the switch is currently running. This allows the user to set the type of <i>STP</i> to be used by the switch to form loop-free topology. The default option is <i>MSTP</i>. The list contains: – <i>STP</i>—sets the version as <i>STP</i> specified in IEEE 802.1D. – <i>RSTP</i>—sets the version as <i>RSTP</i> as specified in IEEE 802.1w. – <i>MSTP</i>—sets the version as <i>MSTP</i> as specified in IEEE 802.1s. NOTE: The Fields Region Name and Region Version are greyed out and cannot be configured, if the protocol version is set as <i>STP</i> or <i>RSTP</i>. • Region Name—enter the name for the region’s configuration to identify the specific <i>MST</i> region. Each <i>MST</i> region contains multiple spanning tree instances and runs special instance of spanning tree known as <i>IST</i> for disseminating of <i>STP</i> topology information for other <i>STP</i> instances. The default value is same as that of the Switch Base MAC Address configured in the Factory Default Settings screen. This value is an octet string of maximum size 32. NOTE: This field can be configured only if the protocol version is selected as <i>MSTP</i>. • Region Version—enter the version that represents the specific <i>MST</i> region. The default value is 0. This value ranges from 0 to 65535. NOTE: This field can be configured only if the protocol version is selected as <i>MSTP</i>. • Dynamic Path Cost Calculation—select whether the dynamic path cost calculation is allowed or not. The path cost represents the distance between the root port and designated port. The path cost is based on a guideline established as part of 802.1d. The path cost is dynamically calculated using port speed, when the operational status of the port changes from down to up or link speed at the time of port creation. The default option is False. The list contains: – True—dynamically calculates path cost based on the speed of the ports whose Admin State is set as Up at that time. The path cost is not changed based on the operational status of the ports, once calculated. – False—dynamically calculates path cost based on the link speed at the time of port creation NOTE: The manually assigned path cost is used irrespective of the status (True or False) of the dynamic path cost calculation. • Speed Change Path Cost Calculation—select whether the speed change path cost calculation is allowed or not. The speed change path cost is to be calculated for ports whose speed changes dynamically. This feature is mainly used for Link Aggregation ports whose speed changes due to the addition and deletion of ports from the port channel. The default option is False. The list contains: – True—specifies that path cost is dynamically calculated for ports based on their speed at that time. It is calculated if the speed of the port changes. – False—specifies that path cost is not dynamically calculated for ports based on their speed at that time. NOTE: The manually assigned path cost is used irrespective of the status (True or False) of the path cost calculation if Path Cost for the port is manually assigned.

Fields (cont)	Flush Interval—enter the value that controls the number of flush indications invoked from spanning-tree module per instance basis. This value ranges from 0 to 500 centi-seconds. The default value is 0. NOTE: 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). Flush Indication Threshold—enter the number of flush indications to go before the flush-interval timer method triggers. This value ranges from 0 to 65535. The default value is 0. NOTE: The flush indication threshold value can be configured only when flush interval value is other than default value. 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. BPDU Guard—select the administrative status for the <i>BPDU</i> guard feature in the port. This feature configures <i>BPDU</i> guard globally in <i>MSTP</i>. This global <i>BPDU</i> is applicable if and only no port specific <i>BPDU</i> Guard is configured. The default option is Disable. The list contains: - Enabled—enables <i>BPDU</i> Guard feature on edge ports globally and moves the port to disabled discarding state when <i>BPDU</i> is received on the edge ports - Disabled—disables <i>BPDU</i> Guard feature on edge ports globally.
Buttons	Apply—modifies attributes and saves the changes. Configure Trace Options—click to access the <i>MSTP</i> Traces screen.

MSTP Traces

Figure 6: MSTP Traces

MSTP Traces

Traces

☐ Init-Shut
☐ Memory
☐ Events
☐ Redundancy
☐ Errors

☐ Management
☐ Bpdu
☐ Timer
☐ Semaphore

State Machine

☐ Port-Info
☐ Port-Role-Select
☐ State-Transition
☐ Topology-Change
☐ Bridge-Detection

☐ Port-Receive
☐ Role-Transition
☐ Protocol-Migration
☐ Port-Transmit
☐ Pseudo-Info

Screen Objective	This screen allows the user to clear the GARP statistics for a specified interface or all interfaces
Navigation	Layer 2 Management > MSTP > Basic Settings > Global Configuration screen. Click Configure Trace Options .
Fields	Traces—select the traces for which debug statements is to be generated. The options are: - Init-Shut—generates debug statements for init and shutdown traces. This trace is generated on failed and successful initialization and shutting down of <i>STP</i> related module and memory. - Management—generates debug statements for management traces. - Memory—generates debug statements for memory related traces. This trace is generated on failed and successful allocation of memory for <i>STP</i> process. - BPDUs—generates debug statements for <i>BPDUs</i> related traces. This trace is generated on failed and successful reception, transmission and processing of <i>BPDUs</i>. - Events—generates debug statements for event handling traces. This trace is generated to denote events that are posted to <i>STP</i> configuration queue whenever you configure any of the <i>STP</i> features.

Fields (cont)	• Traces—the options are (cont): – Timer—generates debug statements for timer module traces. This trace is generated on failed and successful start, stop and restart of <i>STP</i> timers. The different <i>STP</i> timers are: • Forward delay timer • Hello timer • Migration delay timer • Recent backup while timer • Received information while timer • Recent root while timer • Topology change timer • Hold timer • Edge delay timer • Rapid age duration timer • Pseudo information hello timer – Redundancy—generates debug statements for redundancy code flow traces. This trace is generated in standby node <i>STP</i> while taking backup of configuration information from active node. – Semaphore—generates debug statements for state machine variable changes traces. This trace is generated on failed and successful creation and deletion of semaphore. – Errors—generates debug statements for all failure traces of the traces. • State Machine—select the <i>SEMs</i> (State Event Machines) for which debug statements are to be generated to denote the event and state of the selected <i>SEM</i>. The options are: – Port-Info—generates debug statements for port information <i>SEM</i>. – Port-Receive—generates debug statements for port receive <i>SEM</i>. – Port-Role-Select—generates debug statements for role selection <i>SEM</i>. – Role-Transition—generates debug statements for role transition <i>SEM</i>. – State-Transition—generates debug statements for state transition <i>SEM</i>. – Protocol-Migration—generates debug statements for protocol migration <i>SEM</i>. – Topology-Change—generates debug statements for topology change <i>SEM</i>. – Port-Transmit—generates debug statements for port transmit <i>SEM</i>. – Bridge-Detection—generates debug statements for bridge detection <i>SEM</i>. – Pseudo-Info—generates debug statements for port receive pseudo information <i>SEM</i>.
Buttons	• Apply—modifies attributes and saves the changes. • Configure Global Options—accesses Global Configuration screen

MSTP Timers

Figure 7: MSTP Timers Configuration

Timers Configuration

Select	Context Id	Maximum Hop Count	Max Age	Forward Delay	Transmit Hold Count	Hello Time
☒	0	0	0	0	0	0

Apply

Screen Objective	This screen allows the user to configure the timers used in <i>MSTP</i> protocol for controlling the transmission of BPDUs during the computation of loop free topology. This configuration is applied globally in the switch on all ports.
NOTE: This screen displays the default configuration details only for the context for which the <i>MSTP</i> System Control status is set as Start. For the contexts for which <i>MSTP</i> is shutdown, it displays the value as 0 for all fields.	
Navigation	Layer 2 Management > MSTP > Timers
Fields	Select—click to select the context for which the configuration needs to be applied. Context Id—displays the context ID. Maximum Hop Count—enter the maximum hop count value that represents the maximum number of switches that a packet can cross before it is dropped. This value is used by the switch to avoid infinite looping of the packets, if it is selected as the root switch in the topology. This value ranges from 6 to 40. The default value is 20. The root switch always transmits a <i>BPDU</i> with the maximum hop count value. The receiving switch decrements the value by one and propagates the <i>BPDU</i> with modified hop count value. The <i>BPDU</i> is discarded and the information held is aged out, when the count reaches 0. Max Age—enter the amount of time a port waits for <i>STP/RSTP</i> information. This value is used by <i>MSTP</i> while interacting with <i>STP/RSTP</i> domains on the boundary ports. This value ranges from 6 to 40 seconds. The default value is 20. NOTE: The maximum age should be lesser than or equal to $2 * (\text{Forward Delay} - 1.0)$ and should be greater than or equal to $2 * (\text{HelloTime} + 1.0)$. Forward Delay—enter the number of seconds a port waits before changing from the learning/listening state to the forwarding state. This value ranges from 4 to 30 seconds. The default value is 15. Transmit Hold Count—enter the value used by the port transmit state machine for limiting the maximum transmission rate i.e. the number of packets that can be sent for a given interval. This value is configured to avoid flooding. Port transmit state machines use this value to limit the maximum transmission rate. This value ranges from 1 to 10. The default value is 6.

Fields (cont)	Hello Time—enter the amount of time between the transmission of configuration bridge PDUs by this node. This value can be either 1 or 2 seconds. The default value is 2.
Buttons	Apply—modifies attributes and saves the changes.

Port Configuration - CIST Settings

Figure 8: CIST Settings

CIST Settings

Select	Port	Path Cost	Priority	PointToPoint Status	Edge Port	MSTP Status	Protocol Migration	Hello Time	AutoEdge Status	Restricted Role	Restricted TCN	BPDU Receive	BPDU Transmit	Layer2-Gateway Port	Loop Guard	Root Guard	Bpdu Guard	Error Recovery

Apply

Screen Objective	This screen allows the user to configure the timers used in <i>MSTP</i> protocol for controlling the transmission of BPDUs during the computation of loop free topology. This configuration is applied globally in the switch on all ports.
Navigation	Layer 2 Management > MSTP > Port Configuration
Fields	Select—click to select the port for which the configuration needs to be applied. Port Id—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of a slot number and a port number (slot number/port number). Path Cost—enter the value that contributes to the path cost of paths towards the <i>CIST</i> Root which includes this port. The paths' path cost is used during calculation of shortest path to reach the <i>CIST</i> root. The path cost represents the distance between the root port and designated port. This value ranges from 1 to 200000000. The default value is 200000 for all physical ports and 199999 for port channels. NOTE: The default value is used as path cost if this field is not configured and the Dynamic Path Cost Calculation and Speed Change Path Cost Calculation are set as False. The dynamically calculated path cost is used if the path cost is not manually configured and one of these Fields is set as True. The configured value is used as the path cost irrespective of the status (True or False) of the Dynamic Path Cost Calculation and Speed Change Path Cost Calculation. Priority—enter the priority value that is assigned to the port. This value is used during the role selection process. The four most significant bits of the Port Identifier of the Spanning Tree instance can be modified by setting the <i>CIST</i> Port Priority value. The values that are set for Port Priority must be in steps of 16. The Priority value ranges from 0 to 240. The default value is 128.

Fields (cont)	• Point-to-Point Status—select the point-to-point status of the LAN segment attached to the port. The default option is Auto. The list contains. – ForceTrue—specifies that port is connected to a point-to-point link. – ForceFalse—specifies that port is having a shared media connection. – Auto—specifies that the ports as having a shared media connection, or a point-point link based on the prevailing conditions. NOTE: Port is considered to have a point-to-point link if: – It is an aggregator and all of its members can be aggregated. – The <i>MAC></i> entity is configured for full Duplex operation, either manually or through auto negotiation process (that is, negotiation Mode is set as Auto). • Edge Port—select the administrative value of the Edge Port parameter. The default option is False. The list contains: – True—sets the port as an edge port (then Port State is immediately set as forwarding). It is connected directly to a single end station. It allows <i>MSTP</i> to converge faster and does not wait to receive BPDUs. – False—sets the port as a non-Edge port (the spanning tree process is performed using the <i>MSTP</i>). It is connected to a routing device such as a switch. • MSTP Status—select the <i>MSTP</i> status of the port for all spanning tree instances. This value will override the port's status in the MSTI contexts. The default option is Enable. The list contains: – Enable—enables <i>MST</i> in the port. <i>MAC</i> frames are forwarded, and their source addresses are learnt. – Disable—disables <i>MST</i> in the ports. <i>MAC</i> frames are not forwarded, and their source addresses are not learnt. • Protocol Migration—select the protocol migration state of the port. This is used to control the protocol migration mechanism that enables the module to interoperate with legacy 802.1D switches. The default option is False. The list contains: – True—specifies that the port transmits <i>BPDUs</i> based on the spanning tree protocol supported by the receiving switch. The port is forced to transmit <i>MSTP BPDUs</i> without instance information. – False—specifies that the port does not perform protocol migration mechanism. The port always transmits the standard <i>MSTP BPDUs</i>. NOTE: The protocol migration is greyed out and cannot be configured, if the <i>MSTP Status</i> is set as Disable. • Hello Time—enter the amount of time between the transmission of Configuration bridge PDUs by this node in units of hundredths of a second. This value can be either 1 or 2 seconds. The default value is 2.

Fields (cont)	• Auto Edge Status—select whether the Edge Port parameter of the port is detected automatically or configured manually. The default option is True. The list contains: – True—specifies that detection of port as Edge Port happens automatically. • The port is set as edge port if no <i>BPDU</i> is received on the port. • The port is set as non-edge port, if any <i>BPDU</i> is received by that port. NOTE: This overrides the value set in the field Edge Port, based on the reception of <i>BPDU</i>. – False—specifies that the auto edge feature is disabled and the manually configured value for the Edge Port parameter is used. • Restricted Role—select whether the selection of port Role as root can be blocked during the role Selection process. This feature allows the user to block switches external to a core region of the network from influencing the spanning tree active topology. The default option is False. The list contains: – True—blocks the port from being selected as root port for the <i>CIST</i> or any <i>MSTI</i>, even if it has the best spanning tree priority vector. It is selected as an alternate port after the root port is selected. NOTE: The blocking of port from being selected as a root port may cause lack of spanning tree connectivity. – False—includes all available ports of the topology, in the root selection process to select the root for <i>CIST</i> or any <i>MSTI</i>. • Restricted TCN—select the status of transmission of the received topology change notifications and topology changes to the other ports in the network. This feature allows the user to block switches external to a core region of the network from causing address flushing in the region. The default option is False. The list contains: – True—blocks the port from propagating the received topology change notifications and topology changes to other ports. NOTE: The blocking of port may cause temporary loss of connectivity after changes in a spanning tree active topology as a result of persistent incorrectly learnt station location information. – False—allows the port to propagate the received topology change notifications and topology changes to other ports. • BPDU Receive—select the processing status of the received <i>MSTP BPDUs</i>. The default option is True. The list contains: – True—normally processes the <i>MSTP BPDUs</i> received on the port. – False—discards the <i>MSTP BPDUs</i> received on the port. • BPDU Transmit—select the <i>BPDU</i> transmission status of the port. The default option is True. The list contains: – True—specifies that <i>MSTP BPDUs</i> are transmitted from the port. – False—specifies that <i>MSTP BPDUs</i> transmission is blocked from the port

Fields (cont)	NOTE: This field should be set as False for ports to be configured as Layer-2 Gateway Port. • Layer 2-Gateway Port—select whether the port acts as a normal port or as a <i>L2GP</i>. The default option is False. The list contains: – True—specifies that the port operates as a Layer 2 Gateway Port. – False—specifies that the port operates as a normal port. NOTE: <i>BPDUs</i> Transmit, Restricted Role and Restricted <i>TCN</i> should be set as False before configuring the port as a Layer 2 gateway port (<i>L2GP</i>). <i>L2GP</i> should not be enabled on ports whose Bridge Port Type is set as <i>PIP</i> (Provider Instance Port)s or <i>CBP</i> (Customer Backbone Port)s, as the effect is unknown. <i>L2GP</i> operates similarly to that of the normal port operation but pretends to continuously receive <i>BPDUs</i> when Admin State is set as Up. <i>L2GP</i> cannot be enabled on ports with Switch Instance Shared Port (<i>SISP</i>) enabled interfaces. The Port State of the <i>L2GP</i> is always set as Discarding. • Loop Guard—select the status of loop guard. The Loop Guard does age out the information even if the peer does not send information. If the port continues to receive information through <i>BPDUs</i>, the operation on this port will be normal. This is useful when the neighbor bridge is faulty; that is, the bridge cannot send <i>BPDUs</i> but continues to send data traffic. The default option is False. The list contains: – True—enables the loop guard in the port. – False—disables the loop guard in the port. • Root Guard—select the administrative status for the root guard feature in the port. When enabled, this feature causes the port not to be selected as Root Port for the <i>CIST</i> or any <i>MSTI</i>, even if it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. The default option is Disabled, and this can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology; possibly because those bridges are not under the full control of the administrator. – Enabled—enables root guard feature in the port. – Disabled—disables root guard feature in the port. • BPDUs Guard—the administrative status for the <i>BPDUs</i> guard feature in the port. This feature configures <i>BPDUs</i> guard globally in <i>MSTP</i> and this global <i>BPDUs</i> guard is applicable if and only if no port specific <i>BPDUs</i> Guard is configured. The default option is Disable. The list contains: – Enabled—enables <i>BPDUs</i> Guard feature on edge ports globally and moves the port to disable discarding state when <i>BPDUs</i> is received on the edge ports – Disabled—disables <i>BPDUs</i> Guard feature on edge ports globally. • Error Recovery—enter the amount of time to bring the interface out of the error-disabled (err-disabled) state. This value ranges from 30 to 65535 seconds. The default value is 30.
Buttons	• Apply—modifies attributes and saves the changes.

VLAN Mapping

Figure 9: LAN Mapping

VLAN Mapping

MSTP Instance ID *
 Add VLAN ▼
 Delete VLAN ▼

Select	Instance ID	Mapped VLANs
Delete		

Screen Objective	This screen allows the user to map / unmap VLANs for each instance of <i>MSTP</i> and to create / delete instance specific information for the member ports of the <i>VLAN</i> . The instance specific information for the port in one instance is independent of its information in another instance.
Navigation	Layer 2 Management > MSTP > VLAN Mapping
Fields	• Select—select the instance Id for which the mapping is to be deleted. • MSTP Instance ID—enter an integer value that is used to uniquely identify an instance of the <i>MSTP</i>. This value ranges from 1 to 64. The special value 4094 is used in a switch that supports PBB-TE. This special value represents PTETID that identifies VID used by Ethernet switched paths (ESPs). NOTE: The <i>MSTP</i> Instance ID depends on the Maximum <i>MSTP</i> instance configured in the Global Configuration page. Any external agent can separately provide ESPs. The ESPs do not use spanning tree. • Add VLAN—select the <i>VLAN</i> that should be mapped to the <i>MSTP</i> instance. The list contains <i>VLAN</i> Name of all <i>VLANs</i> available in the switch. The mapping of <i>VLAN</i> to the <i>MSTP</i> instance is not done again if the <i>VLAN</i> is already mapped to that instance. • Delete VLAN—select the <i>VLAN</i> that should be unmapped from the <i>MSTP</i> instance. The list contains <i>VLAN</i> Name for the <i>VLANs</i> available in the switch. The unmapping of <i>VLAN</i> from the <i>MSTP</i> instance cannot be done if the <i>VLAN</i> is already unmapped from that instance. • Mapped VLANs—displays the <i>VLAN</i> ID mapped to the spanning tree instance specified. All Instance Specific information for the member ports of the <i>VLAN</i> will be created.
Buttons	• Add—adds and saves new configuration • Reset—resets to default value for respective fields and discards all user inputs • Deleted—deletes the selected entry

Port Settings

Figure 10: Port Settings

Port Settings							
Select	Port	MSTP Instance ID	Port State	Priority	Cost	PseudoRootId Priority	PseudoRootId Address
Apply							
Screen Objective	This screen allows the user to map / unmap VLANs for each instance of <i>MSTP</i> and to create / delete instance specific information for the member ports of the <i>VLAN</i> . The instance specific information for the port in one instance is independent of its information in another instance.						
Navigation	Layer 2 Management > MSTP > Port Settings						
Fields	Select—click to select the port for which the configuration needs to be applied. Port—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of a slot number and a port number (slot number/port number). MSTP Instance ID—enter an integer value that is used to uniquely identify an instance of the <i>MSTP</i>. This value ranges from 1 to 64. The special value 4094 is used in a switch that supports PBB-TE. This special value represents PTETID that identifies VID used by Ethernet switched paths (ESPs). NOTE: This field displays the Instance ID created using the <i>VLAN Mapping</i> screen. The maximum available number of instances will be 16 (values from 0–15 where 0 being <i>CIST</i>). Port State—select the status of the <i>MSTP</i> in the port. The list contains: - Enabled—enables <i>MSTP</i> in the port. The port participates in the <i>STP</i> process and is ready to transmit/receive BPDUs and data. - Disabled—disables <i>MSTP</i> in the port. The port does not participate in the <i>STP</i> process and is not ready to transmit/receive BPDUs and data Priority—enter the priority value that is assigned to the port. This value is used during the role selection process. The four most significant bits of the Port Identifier of the Spanning Tree instance can be modified by setting the <i>CIST</i> Port Priority value. The values that are set for Port Priority must be in steps of 16. This value ranges from 0 to 240. The default value is 128. Cost—enter the value that contributes to the path cost of paths towards the <i>CIST</i> Root which includes this port. The paths' path cost is used during calculation of shortest path to reach the MSTI root. The path cost represents the distance between the root port and designated port. This value ranges from 0 to 200000000. The default value is 200000 for all physical ports and 199999 for port channels.						

Fields (cont)	NOTE: The default value is used as the path cost if this field is not configured and the Dynamic Path Cost Calculation and Speed Change Path Cost Calculation are set as False. The dynamically calculated path cost is used if the path cost is not manually configured and one of these Fields is set as True. The configured value is used as the path cost irrespective of the status (True or False) of the Dynamic Path Cost Calculation and Speed Change Path Cost Calculation. • PseudoRootId Priority—enter the priority of the pseudo root. This value is used by a port configured as <i>L2GP</i>, and the field Layer 2-Gateway Port is set as True. This value ranges from 0 to 61440. The default value is 32768. 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 Address—enter the unicast MAC address of the pseudo root. This value is used by port configured as <i>L2GP</i> (the field Layer 2-Gateway Port is set as True). The default value is 00:08:02:03:04:01.
Buttons	• Apply—modifies attributes and saves the changes.

MSTP CIST Port Status

Figure 11: MSTP CIST Port Status

MSTP CIST Port Status

Port	Designated Root	Root Priority	Designated Bridge	Designated Port	Designated Cost	Regional Root	Regional Root Priority	Regional Path Cost	Type	Role	Port State
Screen Objective	This screen allows the user to view information maintained by every port of the switch for <i>CIST</i> .										
Navigation	Layer 2 Management > MSTP > CIST Port Status										
Fields	• Port—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of a slot number and a port number (slot number/port number). • Designated Root—displays the unique identifier of the bridge recorded as the <i>CIST</i> root in the transmitted configuration BPDUs. This value is an 8-byte octet string. For example, 80:00:00:01:02:03:04:05 • Root Priority—displays the Bridge Priority configured in Global Configuration Screen that represents the priority of the bridge recorded as the <i>CIST</i> root in the configuration BPDUs transmitted. This value ranges from 0 to 61440. The default value is 32768. • Designated Bridge—displays the unique identifier of the bridge, which the port considers to be the designated bridge for the port's segment. The designated bridge is the only bridge allowed to forward frames to and from the segment. This value is an 8-byte octet string. For example, 80:00:00:01:02:03:04:05.										

Fields (cont)	• Designated Port—displays the identifier of the port on the Designated Bridge for the port's segment. This represents the port through which the Designated Bridge forwards frames to and from the segment. This value is a 2-byte octet string. For example, 80:05. • Designated Cost—displays the identifier of the port on the Designated Bridge for the port's segment. This represents the port through which the Designated Bridge forwards frames to and from the segment. This value is a 2-byte octet string. For example, 80:05. • Regional Root—displays the unique identifier of the bridge recorded as the <i>CIST</i> regional root in the configuration BPDUs transmitted. This value is an 8-byte octet string. For example, 80:00:00:01:02:03:04:05 • Regional Root Priority—displays the Bridge Priority that represents the priority of the bridge recorded as the <i>CIST</i> regional root in the configuration BPDUs transmitted. This value ranges from 0 to 61440. The default value is 32768. • Regional Path Cost—displays the port's Path Cost that contributes to the cost of paths (including the port) towards the <i>CIST</i> Regional Root. This value ranges from 1 to 200000000. • Type—displays the operational Point-to-Point Status of the LAN segment attached to the port. The values can be: – Point-to-point—port is treated as if it is connected to a point-to-point link. – SharedLan—port is treated as if it is having a shared media connection. NOTE: The User can set the values directly or can set as Auto for the switch to decide about the point-to-point status, in the field Point-to-Point Status provided in the screen <i>CIST</i> Settings. • Role—displays the current role of the port for the spanning tree instance. The values can be: – Disabled—specified that the port is disabled manually (Port State) or automatically (Link status in Layer 2 Management > Port Manager > Basic Settings). It does not take part in the spanning tree process. – Alternate—specifies that the port is acting as an alternate path to the root bridge (i.e. it is blocked and not used for traffic). The alternate port is enabled and declared as a root port if the current root port is blocked. – Backup—specifies that the port is acting as a backup path to a segment where another bridge port already connects (i.e. it is blocked and not used for traffic). The backup port is enabled and declared as a designated port if the active designated port is blocked. – Root—specifies that the port is used to forward data to root bridge directly or through an upstream LAN segment. – Designated—specifies that the port is used to send and receive packets to/from a specific downstream LAN segment/device. Only one designated port is assigned for each segment.

Fields (cont)	• Port State—displays the current state of the port as defined by the common <i>STP</i>. The values can be: – Disabled—specifies that the port is disabled manually (Port State) or automatically (Link). It does not take part in the spanning tree process. – Discarding—specifies that the port is in Discarding state i.e. No user data is sent over the port. – Learning—specifies that the port is in the Learning state i.e. the port is not forwarding frames yet, but is populating its <i>MAC</i>-address-table by learning source addresses from received frames and storing them in the switching database for using these details while sending and receiving data. – Forwarding—specifies that the port is in Forwarding state i.e. the port is operational by sending and receiving data based on the formed spanning tree topology which is loop-free.

Bridge Priority

Figure 12: Bridge Priority

Bridge Priority

Select	MSTP Instance ID	Root	Bridge Priority	Bridge Cost	Root Port

Apply

Note : Add mstp instance from [VLAN Mapping](#) page.

Screen Objective	This screen allows the user to configure the bridge priority to be assigned to the specified <i>VLAN</i> .
NOTE: Bridge Priority can be configured only if <i>MSTP</i> Instance is created using the <i>VLAN</i> Mapping screen	
Navigation	Layer 2 Management > MSTP > Bridge Priority
Fields	• Select—select the <i>MSTP</i> Instance ID for which the configuration needs to be applied. • MSTP Instance ID—displays the integer value that uniquely identifies an instance of the <i>MSTP</i>. This value ranges from 1 to 64. The special value 4094 is used in a switch that supports PBB-TE. This special value represents PTETID that identifies VID, which can be used by ESPs. NOTE: This value is the instance ID created using the <i>VLAN</i> Mapping screen. Any external agent can separately provide ESPs. The ESPs do not use spanning tree.

Fields	• Root—select the root type for the given <i>VLAN</i> interface. The list contains: – primary—configures the switch to become root for a given <i>VLAN</i>. The priority of the switch is lowered until it becomes root – secondary—configures the switch to become backup root for a given <i>VLAN</i>. 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. • Bridge Priority—denter the priority value that is assigned to the switch. This value is used during the election of <i>CIST</i> root, <i>CIST</i> regional root, and <i>IST</i> root. This value ranges from 0 to 61440. The default value is 32768. NOTE: The value should be set in increments of 4096. For example, 0, 4096, 8192, 12288, and so on. • Bridge Cost—displays the Cost of the path to the MSTI Regional Root seen by this bridge. This is a read-only field • Root Port—displays the port number of the port which offers the lowest path cost from this bridge to the <i>CIST</i> Root Bridge. This is a read-only field
Buttons	• Apply—modifies attributes and saves the changes.

10.3. PVRST

This section describes how to configure Per VLAN Spanning Tree Protocol (*PVRSTP*) on the switch.

PVRST (Per VLAN Rapid Spanning Tree) 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*.

To access **PVRST** screens, go to **Layer 2 Management > PVRST**

The **PVRST** related parameters are configured through the screens displayed by the following tabs:

[Global Configuration](#)

[Port Configurations](#)

[Instance Bridge Configurations](#)

[Instance Port Configurations](#)

[Instance Port Status](#)

Global Configuration

By default, the tab **Basic Settings** displays the **Global Configuration** screen.

Figure 13: PVRST Global Configuration

Global Configuration

Select	Context Id	System Control	Module Status
☒	0	Shutdown ▾	Disabled ▾

Apply

Note : To enable PVRST Functionality, MSTP, RSTP and GVRP should be disabled.

Screen Objective	This screen allows the user to configure for each available virtual context the <i>PVRST</i> basic details that are used globally in the switch for all ports available in the switch.
NOTE: To enable <i>PVRST</i> , the following should be disabled in the selected context <i>MSTP</i> <i>RSTP</i> <i>GVRP</i>	
Navigation	Layer 2 Management > PVRST > Basic Settings
Fields	Select—click to select the context for which the configuration needs to be done.

Fields (cont)	• Context ID—displays the context ID. Currently <i>PVRST</i> can be enabled only for the Context ID of 0. • System Control—select the administrative system control status requested by management for the <i>PVRST</i>. This status allows the user to set availability of the <i>PVRST</i> feature on all ports in the switch. The default option is Shutdown. The list contains: – Start—specifies that <i>PVRST</i> is active on all ports of the device. The required memory is allocated for the feature. – Shutdown—specifies that <i>PVRST</i> is shut down on all ports of the device. The allocated memory is released on all ports. NOTE: The system control status can be set as Start, only if the MSTP System Control is set as Shutdown, <i>RSTP</i> System Control is set as Shutdown, and Dynamic VLAN Status is set as Disabled. The system control status can be set as Shutdown, only if the <i>PVRST</i> Module Status is set as Disabled. Currently <i>PVRST</i> can be enabled only for the Context ID of 0. • Module Status—select the administrative module status requested by management for the <i>PVRST</i>. The default option is Disabled. The list contains: – Enabled—enables the <i>PVRST</i> feature on all ports in the switch. – Disabled—disables the <i>PVRST</i> feature on all ports in the switch. NOTE: The module status is grayed out and cannot be configured, if the <i>PVRST</i> System Control is set as Shutdown. The module status can be set as Enabled, only if the <i>PVRST</i> System Control is set as Start.
Buttons	• Apply—modifies attributes for the selected entry and saves the changes.

Port Configurations

Figure 14: Port Configurations

Port Configurations

Select	Port	Status	Point to Point	Root Guard	BPDU Guard	Encap Type	Row Status	Loop Guard

Apply

Screen Objective	This screen allows the user to configure, on per port basis, the <i>PVRST</i> port information that is used during computation of loop-free topology.
NOTE: The parameters in the screen are not populated with the values (the screen is blank) if the <i>PVRST</i> System Control status is set as Shutdown for the context selected using the Context Selection screen.	
Navigation	Layer 2 Management > PVRST > Port Settings
Fields	• Select—click to select the port for which the configuration needs to be done.

Fields (cont)	• Port—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number). NOTE: Only the ports whose Admin State is set as Up are displayed. • Status—select the <i>PVRST</i> status for the port. The default option is Enabled. The list contains: – Enabled—enables <i>PVRST</i> in the port. The port participates in the STP process and is ready to transmit/receive <i>BPDUs</i> and data. – Disabled—disables <i>PVRST</i> in the port. The port does not participate in the STP process and will not transmit/receive <i>BPDUs</i> and data. • Point to Point—select the administrative point-to-point status of the LAN segment attached to the port. The default option is Auto. The list contains: – ForceTrue—specifies that the port is connected to a point-to-point link. – ForceFalse—specifies that the port is connected to shared media connection. – Auto—specifies that the port is connected to point-to-point link or it is configured as a <i>MAC</i> entity. NOTE: The port is considered to have a point-to-point link if it is an aggregator and all of its members can be aggregated. The <i>MAC</i> entity is configured for full Duplex operation, either manually or through auto negotiation process (Negotiation Mode is set as Auto). • Root Guard—select the administrative status for the root guard feature in the port. The root guard feature prevents the port from becoming root port or blocked port. The port changes to the root-inconsistent state if the port receives a superior <i>BPDUs</i>. The port automatically reverts back to forwarding state, once the superior <i>BPDUs</i> are not received. The default option is Disabled. The list contains: – Enabled—enables the root guard feature in the port. – Disabled—disables the root guard feature in the port. NOTE: The root guard feature can be enabled only for the ports whose Switch Port Mode is configured as Trunk using Layer 2 Management > Port Manager > Port Basic Settings screen. • BPDUs Guard—select the administrative status for the <i>BPDUs</i> guard feature in the port. The <i>BPDUs</i> guard feature prevents the port from receiving a <i>BPDUs</i> for providing security from invalid configurations. The default option is None. The list contains: – None—sets the <i>BPDUs</i> Guard status as None. This removes the <i>BPDUs</i> Guard functionality on this port. Global <i>BPDUs</i> guard configuration will take effect if this port is edge port. – Enabled—enables <i>BPDUs</i> guard feature in the port. This prevents temporary loops and moves the port to disabled discarding state when <i>BPDUs</i> is received on this port.

Fields (cont)	– Disabled—disables <i>BPDU</i> guard feature in the port. The port state is maintained till is manually enabled • Encap Type—select type of encapsulation to be used in the port. Encapsulation defines the <i>VLAN</i> services available and identifies/tags frames transmitted between switches. The default option is dot1Q. The list contains: – dot1Q—specifies that the encapsulation type is dot1Q. This indicates that the port sends <i>BPDUs</i> to the native <i>VLAN</i> as normal IEEE <i>RSTP BPDUs</i>. <i>BPDUs</i> for other <i>VLAN</i> are sent with proprietary tunneled address. The <i>PVRST</i> unaware bridge considers these <i>BPDUs</i> as data packets and forwards them through <i>VLAN</i>. NOTE: The encapsulation type is always set as dot1Q and cannot be changed if the Switch Port Mode is set as Access using Layer 2 Management > Port Manager > Port Basic Settings screen. – isl—specifies that the encapsulation type is isl. This indicates that the port sends <i>BPDUs</i> for all <i>VLANs</i> as normal <i>RSTP BPDUs</i> (including the IEEE Ethernet header) encapsulated within an additional proprietary ISL Ethernet header that contains the <i>VLAN ID</i>. NOTE: The encapsulation type can be configured as isl, only if the Switch Port Mode is configured as Trunk using Layer 2 Management > Port Manager > Port Basic Settings screen. • Row Status—select the status of the row to create or delete interfaces at <i>PVRST</i> module level. Ports can be created at <i>PVRST</i> module level only for ports that have been created in Interface Manager. NOTE: This field is greyed out since it is applicable only when Automatic Port Create Feature is Disabled. Automatic Port Create Feature can be configured using CLI. • Loop Guard—select the status of Loop Guard. The Loop Guard does not age out the information even if the peer does not send information. If the port continues to receive information through <i>BPDUs</i>, the operation on this port will be normal. This is useful when the neighbor bridge is faulty, that is, the bridge cannot send <i>BPDUs</i> but continues to send data traffic. The default option is False. The list contains: – True—enables the Loop Guard in the port. – False—disables the Loop Guard in the port.
Buttons	• Apply—modifies attributes for the selected entry and saves the changes.

Instance Bridge Configurations

Figure 15: Instance Bridge Configuration

Instance Bridge Configurations

Select	ContextId	InstanceId	Max-Age(Secs)	HelloTime(Secs)	ForwardDelay (Secs)	Tx HoldCount	BridgePriority

Apply

Note :

To set the parameters Forward Delay and Max Age, the following relation is to be satisfied :

$$2 * (\text{Forward Delay} - 1.0) \geq \text{Max Age}.$$

To set the parameters Hello Time and Max Age, the following relation is to be satisfied :

$$\text{Max Age} \geq 2 * (\text{Hello Time} + 1.0).$$

Screen Objective	This screen allows the user to configure bridge information specific to spanning tree instance, for virtual contexts available in the switch. This configuration is applied globally to all ports in the switch.
NOTE: The parameters in the screen are not populated with the values (the screen is blank) if the PVRST System Control status is set as Shutdown for the context selected using the Context Selection screen.	
Navigation	Layer 2 Management > PVRST > Instance Bridge Settings
Fields	Select—click to select the context for which the configuration needs to be done. Context ID—displays the context ID. Currently PVRST is enabled only for the Context ID of 0. Instance ID—displays the spanning tree instance to which the bridge information belongs. The instance represents the VLAN ID created in the Static VLAN Configuration screen. For example, the instance IDs 1 and 3 are displayed if VLAN IDs 1 and 3 are created. These values range from 1 to 4094. The default value is 1. Max-Age (Secs)—enter the maximum age (in seconds) of the bridge information. This value represents the time interval after which the spanning tree protocol information learnt from the network for any port is discarded. This value ranges from 6 to 40 seconds. The default value is 20 seconds. NOTE: The maximum age should be lesser than or equal to $2 * (\text{Forward Delay} - 1.0)$ and should be greater than or equal to $2 * (\text{HelloTime} + 1.0)$ HelloTime (Secs)—enter the time interval (in seconds) between two successive configuration BPDUs generated by the root switch. This value ranges from 1 to 10 seconds. The default value is 2 seconds. ForwardDelay (Secs)—enter the ForwardDelay of the Root Bridge i.e. the time that is spent in the listening and learning state. This value ranges from 4 to 30 seconds. The default value is 15 seconds.

Fields (cont)	• Tx HoldCount—enter the value used by the Port Transmit state machine to limit the maximum transmission rate. This value is configured to avoid flooding and limit the maximum transmission rate. This value is from 1 to 10 with default of 6. • BridgePriority—enter the priority value that is assigned to the switch. This is used during the election of root. This value is from 0 to 61440, the default is 32768. NOTE: The value should be set in increments of 4096; that is, the value can be set as 0, 4096, 8192, 12288, and so on. The configured priority is added to the instance ID, and the total value is displayed. For example, the default priority value is displayed as 32769 if the instance ID is 1 (32768 + 1).
Buttons	• Apply—modifies attributes for the selected entry and saves the changes.

Instance Port Configurations

Figure 16: Instance Port Configurations

Instance Port Configurations

Select	Instance	Port	Module Status	Path Cost	Priority

Apply

Screen Objective	This screen allows the user to configure port specific information for all ports available in the switch on per port basis. It also allows the user to assign ports to specific instances so that the instances can make use of the port information.
NOTE: The parameters in the screen are not populated with the values (the screen is blank) if the <i>PVRST</i> System Control status is set as Shutdown for the context selected at the Context Selection screen.	
Navigation	Layer 2 Management > PVRST > Instance Port Settings
Fields	• Select—click to select the context for which the configuration needs to be done. • Instance—displays the spanning tree instance to which the bridge information belongs. The instance represents the <i>VLAN</i> ID created in the Static <i>VLAN</i> Configuration screen. For example, the instance IDs 1 and 3 are displayed if <i>VLAN</i> IDs 1 and 3 are created. This value ranges from 1 to 4094. The default value is 1. • Port—displays the port # identifying a port in the switch- from 1 to 65535. NOTE: Only the ports whose Admin State is set as Up are displayed. • Module Status—select the administrative status for the <i>PVRST</i> module. By default, the value is set same as the value shown in the field Status in Port Configuration screen. The list contains: – Enabled—enables <i>PVRST</i> in the device on all ports. The port participates in the STP process and is ready to transmit/receive <i>BPDUs</i> and data. – Disabled—disables <i>PVRST</i> in the device on all ports. The port does not participate in the STP process and is not ready to transmit/receive <i>BPDUs</i> / data.

Fields (cont)	NOTE: The module status can be set as Enabled, only if the Status in Port Configuration is set as Enabled. • Path Cost—enter the administratively assigned value for the contribution of this port to the path cost of paths toward the spanning tree root. The path cost represents the distance between the root port and designated port. The path cost is used during calculation of shortest path to reach the root. This value ranges from 0 to 200000000. The default value is 200000 for all physical ports and 199999 for port channels. NOTE: The configured value is applied, only if the Status in Port Configuration is set as Enabled. • Priority—enter the priority value that is assigned to the port. The four most significant bits of the port identifier for a given spanning tree instance can be modified independently for each spanning tree instance supported by the bridge. This value is used during the port role selection process. This value ranges from 0 to 240. The values that are set for Port Priority must be in steps of 16. The default value is 128. NOTE: The configured value is applied, only if the Status in Port Configuration is set as Enabled.
Buttons	• Apply—modifies attributes for the selected entry and saves the changes.

Instance Port Status

Figure 17: Instance Port Status

Instance Port Status

Instance	Port	Designated Root	Designated Bridge	Designated Port	Port State	Port Role

Screen Objective	This screen allows the user to view information maintained by every port of the switch for <i>PVRST</i> .
NOTE: The parameters in the screen are not populated with values (the screen is blank) if the <i>PVRST</i> System Control status is set as Shutdown for the context selected using the Context Selection screen.	
Navigation	Layer 2 Management > PVRST > Instance Port Status
Fields	• Instance—displays the spanning tree instance to which the bridge information belongs. The instance represents the <i>VLAN</i> ID created in the Static <i>VLAN</i> Configuration screen. For example, the instance IDs 1 and 3 are displayed if <i>VLAN</i> IDs 1 and 3 are created. This value ranges from 1 to 4094. The default value is 1. • Port—displays the port number that uniquely identifies the specific port in the switch. This value ranges from 1 to 65535. NOTE: Only the ports whose Admin State is set as Up are displayed.

Fields (cont)	• Designated Root—displays the unique identifier of the bridge recorded as the instance root in the transmitted configuration <i>BPDUs</i>. This value is an 8-byte octet string. For example, 80:01:00:01:02:03:04:01. • Designated Bridge—displays the unique identifier of the bridge, which the port considers to be the designated bridge for the port's segment. The designated bridge is the only bridge allowed to forward frames to and from the segment. This value is an 8-byte octet string. For example, 80:01:00:01:02:03:04:01. • Designated Port—displays the ID of the port on the Designated Bridge for the port's segment. This represents the port through which the Designated Bridge forwards frames to and from the segment. This is a 2-byte octet string (e.g. 80:05). • Port State—displays the current state of the port state as defined by the STP. The port states are: – Disabled—specifies that the port is disabled manually (<i>PVRST</i> Module Status) or automatically (Link). The port does not take part in the spanning tree process. – Discarding—specifies that the port is in the Discarding state i.e. no user data is sent over the port. – Learning—specifies that the port is in Learning state i.e. the port is not forwarding frames yet, but it is populating its <i>MAC</i>-address-table by learning source addresses from received frames and storing them in the switching database for using them while sending and receiving data. – Forwarding—specifies that the port is in the Forwarding state i.e. the port is operational by sending and receiving data based on the formed spanning tree topology which is loop free. • Port Role—displays the current role of the port for the spanning tree instance. The port roles are: – Disabled—specifies that the port is disabled manually (<i>PVRST</i> Module Status) or automatically (Link). The port does not take part in the spanning tree process. – Alternate—specifies that the port is acting as an alternate path to the root bridge which is blocked and not used for traffic. If the root port is blocked, the alternate port is enabled and declared as a root port. – Backup—specifies that the port is acting as a backup path to a segment to which another bridge port already connects and which is blocked and not used for traffic. If the active designated port is blocked, the backup drive is enabled and declared as a designated port. – Root—specifies that the port is used to forward data to root bridge directly or through an upstream LAN segment. – Designated—specifies that the port is used to send to and receive packets from a specific downstream LAN segment/device. Only one designated port is assigned for each segment.

11. MRP WebUI Interface

This section describes how to configure Media Redundancy Protocol (*MRP*) on the switch using the WebUI.

MRP (Media Redundancy Protocol) 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.

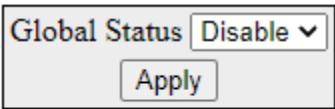
The ring size may consist of up to 50 devices while still meeting the 200 ms reconfiguration requirement. To access **MRP** screens, go to **Layer2 Management > MRP**.

11.1. Global Settings

The **Global Settings** screen is used to enable or disable *MRP* on the switch.

Global Settings

MRP Global Settings



Screen Objective	This screen allows the user to enable or disable <i>MRP</i> .
Navigation	Layer 2 Management > MRP > Global Settings
Fields	Global Status— select Disable or Enable to change the status of the protocol.
Buttons	Apply—modifies attributes and saves the changes.

11.2. MRP Configuration

Figure 1: MRP Configuration

MRP Configuration

Ring ID

*

Mode

Disabled

▼

Ring Port 1

▼

*

Ring Port 2

▼

*

Priority

UUID

Vlan ID(1-4094)

Name

Add

Reset

Select	Ring ID	Mode	Ring Port 1	Ring Port 2	Priority	UUID	Vlan ID	Name
☒	1	Manager ▼	Gi0/3 ▼	Gi0/2 ▼	32768	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	7	

Modify

Delete

Fields	• Ring ID—the ring identifier of the <i>MRP</i> instance. This is a numeric value with a range of 1 through 2. • Mode—a drop-down list with the following options: – Disabled – Client—enter this to configure <i>MRP</i> instance as client (<i>MRC</i>) in the <i>MRP</i> ring, which forwards the test frames between the ring ports. – Manager—enter this to configure <i>MRP</i> instance as manager (<i>MRM</i>) in the <i>MRP</i> ring, which generates the test frames on both ring ports and handles/avoid the loop. – Manager-Autocomp—enter this to configure <i>MRP</i> instance as manager auto (<i>MRA</i>) in the <i>MRP</i> ring. It competes with the other <i>MRA</i> nodes in the ring to become <i>MRM</i> based on priority. If priority is the highest, it turns to act as <i>MRM</i> else turn <i>MRC</i>. • Ring Port 1—this is a drop-down selector for the port to be selected as Port 1 of the ring. • Ring Port 2—this is a drop-down selector for the port to be selected as Port 2 of the ring. • Priority—this is a value between 0 and 65535, Enter to configure <i>MRP</i> priority to be manager (<i>MRM</i>) in the ring, in case auto manager is enabled. • UUID—enter this to configure <i>MRP UUID</i> as 32 octet string (hex). The <i>UUID</i> is a 128-bit identifier unique to a domain/ring. All <i>MRP</i> instances belonging to the same ring must have the same domain ID. • Vlan ID (1-4094)—enter a number from 1 to 4094 to assign a Vlan ID to a ring instance. • Name—an optional field that assigns a name to the ring configuration.
Buttons	• Add—adds the configuration to the switch. • Reset—clears the fields in the form • Modify—by selecting a configuration with the radial button and then clicking modify, the user will be able to edit a configuration. • Delete—the user first selects a configuration with the radial button and then clicks delete to remove it.

11.3. MRP Status

Figure 2: MRP Status Screen

MRP Status

Ring ID	Admin Mode	Oper Mode	Ring Port 1	Port 1 State	Ring Port 2	Port 2 State	Ring State	Multiple MRM Error	Single Side Error
1	MANAGER	MANAGER	Gi0/12	FORWARDING	Gi0/21	DOWN	OPEN	FALSE	FALSE
Refresh									

Screen Objective	The status of the ring is displayed in the <i>MRP</i> status page. In addition to the status, the page also displays any errors in the received <i>MRP</i> packets.
Navigation	Layer 2 Management > MRP > Status
Fields	• Ring ID—displays the Ring ID. • Admin Mode—displays the admin mode of the ring. • Ring Port 1—displays the ring port of the ring. • Ring Port 2—displays the ring port of the ring. • Port 1 State —displays the port 1 state. • Port 2 State—displays the port 2 state. • Ring State—displays the ring state. • Multiple MRM Error—displays <i>MRM</i> Errors state. This error is indicated by an <i>MRM</i> when more than one <i>MRM</i> are active in the MRP ring. Possible values are as follows: – false—no multi-<i>MRM</i> error – true—more than one <i>MRM</i> present in the ring • Single Side Error—displays Single Side Error state. This error also indicated by an <i>MRM</i> when the test frames of an <i>MRM</i> have been seen, but only on one ring port. – false—no one Side Rx error – true—test frame received only on one ring port
Buttons	• Refresh—refreshes the table.

12. Link Aggregation

This section describes how to configure Link Aggregation (LA).

Link Aggregation (LA) implements the LA functionality as per the IEEE 802.3ad standard. LA feature allows the user to combine individual point-to-point links into a LA group. A MAC client treats the LA group as a single link. The total capacity of the LA group is the sum of the capacities of the individual links present in the group. The LA group provides increased bandwidth for the traffic between the hosts and the server, and it does not affect the traffic if any of the links are made down.

LA feature is supported only in point-to-point links, with MACs operating in full Duplex mode. All links in a LA group should work at the same data rate (i.e. speed should be same).

The switch supports up to 8 link aggregation groups, each link aggregation group may support up to a maximum of 8 ports.

To access **Link Aggregation** screens, click **Layer 2 Management > Link Aggregation**.

The **Link Aggregation** link parameters are configured through the screens displayed by the following tabs:

[Basic Settings](#)

[Port Channel Interface Basic Settings](#)

[Port Channel Settings](#)

[Link Aggregation Port Settings](#)

[Link Aggregation Port State Machine Information](#)

[Link Aggregation Load Balancing Policy](#)

[DLAG Remote Port Channel Information](#)

[DLAG Remote Ports Information](#)

12.1. Basic Settings

By default, the tab **Basic Settings** displays the **Link Aggregation Basic Settings** screen.

Figure 1: Link Aggregation Basic Settings

Link Aggregation Basic Settings

System Control	Start ▾
LA Status	Disabled ▾
System Priority	32768
System ID	00:00:00:00:00:00
LA Independent Mode	Disabled ▾
Apply	

Screen Objective	This screen allows the user to configure the Link Aggregation (LA) module parameters that are used globally in the switch for all ports available in it.
Navigation	Layer 2 Management > Link Aggregation > Basic Settings

Fields	• System Control—select the system control status of the <i>LA</i> in the switch. The default option is Start. The list contains: – Start—starts the <i>LA</i> module and allocates the resources required by the <i>LA</i>. – Shutdown—shuts down the Link Aggregation module and releases the allocated resources to the system. NOTE: All fields in this screen are greyed out when System Control is Shutdown. • LA Status—select the administrative status of the <i>LA</i> module. The <i>LA</i> feature allows the user to aggregate individual point-to-point links into a <i>LA</i> group. The default option is Disabled. The list contains: – Enabled—enables <i>LA</i> on all ports in the switch. The <i>LA</i> is enabled in the switch, only if the <i>LA</i> System Control is set as start. – Disabled—disables <i>LA</i> in the switch on all ports. • System Priority—enter the priority value associated with the system’s ID. This value ranges from 0 to 65535. The default value is 32768. • System ID—enter 6-octet unicast <i>MAC</i> address value that is used as a unique identifier for the switch containing the aggregator. The default value is 00:01:02:03:04:01. • LA Independent Mode—select the independent mode of the <i>LA</i> module. The default option is Disabled. The list contains: – Enabled—enables operation of the member ports of the port-channel as independent ports and allows the ports to be visible to higher layers. NOTE: If there is no remote partner information available in the system, then the port-channel becomes operationally down. – Disabled—disables the ports from being visible to higher layers and sets the member ports of the port-channel operationally up. NOTE: If there is no remote partner information available in the system, then the port-channel becomes operationally up based on the default values assigned for the partner.
Buttons	• Apply—modifies attributes and saves the changes.

12.2. Port Channel Interface Basic Settings

Figure 2: Port Channel Interface Basic Settings

Port Channel Interface Basic Settings

Select	Context	PortChannel ID	Admin State	Oper State	MTU
☒	0	2	Up	Down	1500

Screen Objective	This screen allows the user to create a port channel (aggregator) and configure the port channel related parameters. The port channel is treated as a logical port that is used to aggregate several ports. The port channel related parameters are configured on context basis.
NOTE: The port channel should be created, and its related parameters should be configured, before aggregating the ports. The port channel can be created, only if the System Control is set to Start in Link Aggregation Basic Settings.	
Navigation	Layer 2 Management > Link Aggregation > Interface Settings
Fields	Port Channel ID—enter the identifier that uniquely determines a port channel to be created in the switch. This value ranges from 1 to 65535. Context—select the context ID. Context of 0 is available for the current version. Admin Status—select the desired Admin status of the port channel. The default option is Up. The list contains: - Up—allows the port channel to be available for aggregating the ports and transmitting / receiving traffic. - Down—blocks the availability of the port channel for aggregating the ports and transmitting / receiving traffic. Operational State—select the context ID. Context of 0 is available for the current version. - Up—port channel is available for aggregating ports and transmitting / receiving traffic. - Down—port channel availability for aggregating ports and transmitting / receiving traffic is blocked.

Fields (cont)	MTU—enter the <i>MTU</i> for the port channel. This value defines the largest <i>PDU</i> that can be passed by the channel without any need for fragmentation. The default value is 1500. This value ranges from 46 to 9216. NOTE: enter the <i>MTU</i> for the port channel. This value defines the largest <i>PDU</i> that can be passed by the channel without any need for fragmentation. The default value is 1500. This value ranges from 46 to 9216.
Buttons	Add—adds and saves new configuration. Reset—resets to default value for respective fields and discards all user inputs. Apply—modifies attributes and saves the changes. Delete—deletes the selected entry.

12.3. Port Channel Settings

Figure 3: Port Channel Settings

Link Aggregation Port Channel Settings

Context	Port Channel	Ports	NoOf Ports Per Channel	NoOf HotstandBy Ports	Default Port	Aggregator MAC	Max Ports
0	2		0	0		e8:e8:75:90:0b:1d	8

Screen Objective	This screen allows the user to add or delete aggregation of ports, Distributed Link aggregation, and configure their related parameters for the port channels already created in the Port Channel Interface Basic Settings screen. NOTE: Only one entry can be created for each port channel. The parameters in the screen are not populated with values (the screen is blank) if the Link Aggregation's variable System Control is set as Shut-down
Navigation	Layer 2 Management > Link Aggregation > Port Channel Settings
Fields	Context—displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. NOTE: The user can create new virtual contexts from the Switch Creation screen. Go to Context Manager->Switch Creation. The user can create new virtual contexts from the Switch Creation screen.

Fields (cont)	• Port Channel ID—select the port channel identifier from the list already specified in the system, to which the ports should be aggregated or from which aggregated ports should be removed. The list contains the port channels created in the Port Channel Interface Basic Settings screen. • Aggregation Type—select the type of aggregation to be used in the port channel. The default option is Static for all ports and Dynamic for the port configured as a default port of the port channel. The list contains: – Static—allows the port to participate only in static aggregation; that is, the port is a member of only the port channel to which it is configured. The port channel should be manually assigned with its member ports. – Dynamic—allows the port to participate only in dynamic aggregation selection, that is, the port is made as a part of best aggregation selected based on System ID and Admin key (that is, Port Channel ID). • Action Type—select the action to be performed for the Ports configured in this screen. The default option is Add. The options are: – Add—aggregates the mentioned Ports and configures them as a member for the selected Port Channel ID. – Delete—removes the mentioned Ports from the member list created for the selected Port Channel ID. NOTE: The field is greyed out when the aggregation type is set as Dynamic. • Mode—select the operating mode to be set for the port channel. The default option is LACP. The list contains: – LACP—sets the port channel into passive negotiation state, in which the port channel waits for its peer to initiate negotiation. – Manual—sets/forces the port channel to enable channeling without waiting for its peer to start negotiation. – Disable—disables the channeling i.e. the <i>LACP</i> feature is disabled in the port channel. NOTE: The field is greyed out when the aggregation type is set as Dynamic. • Ports—enter port or set of ports, which should be aggregated and set as member of the selected port channel. Use a comma as a separator between the ports while configuring a list of ports. The format of this entry is <interface type><slot number/port number>. Note that here is no space needed between these two entries. Example: Gi0/1,Gi0/2 (Here Gi is interface type Gigabit Ethernet Interface, 0 is a slot number, and 1 is a port number). The maximum number of ports is 8. NOTE: The field is greyed out when the aggregation type is set as Dynamic. • No of Ports Per Channel—displays the number of ports that are bundled for the port channel. For example, this value would be set as 3, if the value for the field Ports is entered as gi0/4,gi0/7,gi0/8. • No of Hot Standby Ports—displays the number of ports that are bundled for the port channel. For example, this value would be set as 3, if the value for the field Ports is entered as gi0/4,gi0/7,gi0/8.

Fields (cont)	• Default Port—select the port that should be set as default port, which gets attached to the port channel and participates only in dynamic aggregation selection. NOTE: This field is disabled (that is greyed out) and cannot be configured, if the Aggregation Type is set as Static. • Aggregator MAC—displays the 6-octet <i>MAC</i> address that is assigned to the port channel. This MAC address is automatically assigned to the port channel. • Max Ports—enter the maximum number of ports that can be attached to the port-channel. This value ranges from 2 to 8. The default value is 8. If the total number of ports attached to the port-channel exceeds the configured value, the best ports are maintained in active state and other ports are maintained in standby state. The best ports are calculated based on the Port Identifier and Port Priority.
Buttons	• Apply—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs

12.4. Link Aggregation Port Settings

Figure 4: Link Aggregation Port Settings

Link Aggregation Port Settings

Select	Port	Port Priority	Port Identifier	Mode	Activity	Timeout	Wait Time (secs)	Bundle State	Aggregation Selection
☐	Gi0/1	128	1	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/2	128	2	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/3	128	3	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/4	128	4	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/5	128	5	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/6	128	6	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/7	128	7	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/8	128	8	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/9	128	9	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/10	128	10	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/11	128	11	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/12	128	12	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/13	128	13	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/14	128	14	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/15	128	15	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/16	128	16	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/17	128	17	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/18	128	18	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/19	128	19	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/20	128	20	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/21	128	21	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/22	128	22	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/23	128	23	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Gi0/24	128	24	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Ex0/1	128	25	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Ex0/2	128	26	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☐	Ex0/3	128	27	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾
☒	Ex0/4	128	28	Disable ▾	Active ▾	Long ▾	2	Down ▾	Static ▾

Apply

Screen Objective

This screen allows the user to configure the Link Aggregation control configuration parameters for each port in the switch. These parameters allow you to control the bundling of physical ports.

NOTE: The parameters in the screen are not populated with values (the screen is blank) if the Link Aggregation System Control is set as Shutdown.

Navigation	Layer 2 Management > Link Aggregation > Port Settings
Fields	• Select—click to select the port for which the configuration needs to be applied. • Port—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of a slot number and the port number (slot number/port number). • Port Priority—enter the priority value assigned to the aggregation port. This value is used in combination with Port Identifier during the identification of best ports in the port channel. This value ranges from 0 to 65535. The default value is 128. • Port Identifier—enter the port number that represents the concerned aggregation port. This number is communicated as the Actor_Port in LACPDUs. This value ranges from 1 to 65535. • Mode—displays the operating mode configured for the port. By default, the configuration set in the field Mode in the screen Link Aggregation Port Channel Basic Settings is displayed. The list contains: – LACP—places the port into passive negotiation state, in which the port waits for its peer to initiate negotiation. – On—forces the port to enable channeling without waiting for its peer to start negotiation. – Disable—disables the channeling; that is, the <i>LACP</i> feature is disabled in the port. NOTE: This field is greyed and cannot be configured. • Activity—select the <i>LACP</i> activity for the port. The list contains: – Active—generates <i>LACP PDUs</i> without waiting for any <i>LACPPDU</i> from the partner port. – Passive—generates <i>LACPPDU</i> only when an <i>LACPPDU</i> is received from the partner port. NOTE: This field is greyed and cannot be configured if the Mode is set as On or Disable. • Timeout—select the time within which <i>LACPPDUs</i> should be received on a port to avoid timing out of the aggregated link. The default option is Long. The list contains: – Short—sets the value as 3 seconds for the port to time out of the port channel. <i>LACP PDU</i> is sent every second. – Long—sets the value as 90 seconds for the port to time out of the port channel. <i>LACP PDU</i> is sent every 30 seconds. • Wait Time (secs)—enter the waiting time for a port after receiving partner information and before entering aggregation (i.e. the time taken to attach to the port channel). This value ranges from 0 to 10 seconds. The default value is 2.

Fields (cont)	• Bundle State—displays the current state of the port with respect to Link Aggregation. This field is read only. – Up In Bundle—specifies that the port is an active member of the port channel. The port is operationally up and actively takes part in aggregation. – Standby—specifies that the port is a member of the port channel but is currently in standby state. The port is capable of joining in the port channel, when any of the ports in the port channel goes down. – Down—specifies that the port is operationally down in lower layers or the port is operational in lower layers, but temporarily it is not able to participate in aggregation because of different partner information in the same group. – Up Individual—specifies that the port is operating individually and is not taking part in aggregation. • Aggregation Selection—displays the type of aggregation in which the port participates. The default option is Static for all ports and Dynamic for the port configured as a Default Port of the port channel. This field is read only. – Static—allows the port to participate only in static aggregation; that is, the port is a member of only the port channel to which it is configured, i.e. the port channel has to be assigned manually to its member ports in the Link Aggregation Port Channel Settings screen. – Dynamic—allows the port to participate only in dynamic aggregation selection; that is, the port is made as a part of best aggregation selection based on System ID and Admin key (i.e. Port Channel ID).
Buttons	• Apply—modifies attributes and saves the changes.

12.5. Link Aggregation Port State Machine Information

Figure 5: Link Aggregation Port State Machine Information

Link Aggregation Port State Machine Information

Port Channel	Port No	Aggregation State

Screen Objective	This screen allows the user to view the aggregation state of the port channels created in the switch through the Port Channel Interface Basic Settings screen.
NOTE: The parameters in the screen are not populated with values (the screen is blank) if the Link Aggregation System Control is set as Shutdown.	
Navigation	Layer 2 Management > Link Aggregation > Port State Machine Info

Fields	• Port Channel—displays the identifier that uniquely identifies a port channel created in the switch. This value ranges from 1 to 65535. • Port Id—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number). • Aggregation State—displays the Actor State as transmitted by the actor in LACPDUs. The state can be: – Aggregation—sets the port as a potential candidate for aggregation. – Individual—does not set the port from aggregation. It can be operated only as an individual link. – Sync—allocates the port to the correct Link Aggregation group which is associated with a compatible port channel whose identity is consistent with the Actor System ID and Admin key (Port Channel ID). The System ID and Admin Key are in sync with partner information. – Collecting—enables the port to collect incoming frames and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. – Distributing—enables the port to distribute outgoing frames. – Defaulted—sets the ports receive machine to use the default operational partner information that is administratively configured for the partner. – Expired—sets the ports receive machine in expired state. The receive machine state is changed as expired if the <i>PDU</i>s are not received from partner for certain time period.

12.6. Link Aggregation Load Balancing Policy

Figure 6: Link Aggregation Load Balancing Policy

Link Aggregation Load Balancing Policy

Select	Port Channel	Selection Policy
☐	2	☐ MAC Source ☐ MAC Destination ☒ MAC Source and Destination ☐ IP Source ☐ IP Destination ☐ IP Source and Destination ☐ Vlan ID ☐ ISID ☐ MAC Source Vlan ID ☐ MAC Destination Vlan ID ☐ MAC Source and Destination Vlan ID ☐ MPLS VC Label ☐ MPLS Tunnel Label ☐ MPLS VC and Tunnel Label ☐ Ipv6 Source ☐ Ipv6 Destination ☐ L3 Protocol ☐ Source L4 Port ☐ Destination L4 Port
Apply		

Screen Objective	This screen allows the user to configure the rule for distributing the Ethernet traffic among the aggregated links and establish load balancing.
NOTE: The parameters in the screen are not populated with values (the screen is blank) if the Link Aggregation System Control is set as Shutdown.	
Navigation	Layer 2 Management > Link Aggregation > Load Balancing

Fields	• Select—click to select the port channel for which the configuration needs to be done. • Port Channel—displays the identifier that uniquely identifies a port channel created in the switch. This value ranges from 1 to 65535. • Selection Policy—select the rule for distributing the Ethernet traffic. The default option is MAC Source and Destination. The options are: – MAC Source—uses the bits of the source <i>MAC</i> address in the packet to select the port in which the traffic should flow. – MAC Destination—uses the bits of the destination <i>MAC</i> address in the packet to select the port in which the traffic should flow. – MAC Source and Destination—uses the bits of the source and destination <i>MAC</i> address in the packet to select the port in which the traffic should flow. – IP Source—uses the bits of the source IP address in the packet to select the port in which the traffic should flow. – IP Destination—uses the bits of the destination IP address in the packet to select the port in which the traffic should flow. – IP Source and Destination—uses the bits of the source and destination IP address in the packet to select the port in which the traffic should flow. – VLAN ID—uses the <i>VLAN</i> ID in the packet to select the port in which the traffic should flow. – ISID—uses the ISID in the packet to select the port in which the traffic should flow. – MAC Source VLAN ID—uses the <i>VLAN</i> ID and source <i>MAC</i> address in the packet to select the port in which the traffic should flow. – MAC Destination VLAN ID—uses the <i>VLAN</i> ID and destination <i>MAC</i> address in the packet to select the port in which the traffic should flow. – MAC Source and Destination VLAN ID—uses the <i>VLAN</i> ID, source <i>MAC</i> address, and destination <i>MAC</i> address in the packet to select the port in which the traffic should flow. – MPLS VC Label—uses the <i>MPLS</i> VC label in the packet to select the port in which the traffic should flow. – MPLS Tunnel Label—uses the <i>MPLS</i> tunnel label in the packet to select the port in which the traffic should flow. – MPLS VC and Tunnel Label—uses the <i>MPLS</i> VC and tunnel labels in the packet to select the port in which the traffic should flow. – Ipv6 Source—uses the bits of the source IPv6 address in the packet to select the port in which the traffic should flow. – Ipv6 Destination—uses the bits of the destination Ipv6 address in the packet to select the port in which the traffic should flow. – L3 Protocol—uses the frames of the L3 IP header in the packet to select the port in which the traffic should flow.

Fields	• Selection Policy—The options are (cont): – L3 Protocol—uses the frames of the L3 IP header in the packet to select the port in which the traffic should flow. – Source L4 Port—uses the bits of L4 source port specified in L4 header (TCP/UDP port) in the packet to select the port in which the traffic should flow. – Destination L4 Port—uses the bits of L4 destination port specified in L4 header (TCP/UDP port) in the packet to select the port in which the traffic should flow.
Buttons	• Apply—modifies attributes and saves the changes.

12.7. DLAG Remote Port Channel Information

Figure 7: DLAG Remote Port Channel Information

DLAG Remote Port Channel Information

Port Channel Index	DLAG SystemID	DLAG System Priority	DLAG Role Played	DLAG Keep Alive Count

Screen Objective	This screen allows the user to view the details of all remote port channels that are part of same <i>D-LAG</i> (Distributed Link Aggregation).
NOTE: The parameters in the screen are not populated with values (the screen is blank) if the Link Aggregation System Control is set as Shutdown.	
Navigation	Layer 2 Management > Link Aggregation > DLAG Remote Port Channel Settings
Fields	• Port Channel Index—displays the Remote Aggregator's interface index. • DLAG System ID—displays the 6-octet MAC address value of each remote D-LAG node and the system ID in <i>D-LAG</i> nodes used for communicating with peer nodes. • DLAG System Priority—displays stored system priority of remote <i>D-LAG</i> nodes. • DLAG Role Played—displays system priority in <i>D-LAG</i> nodes which is to be used for communicating with the peer node when <i>D-LAG</i> status is enabled. The list contains: – none—specifies the role by the remote <i>D-LAG</i> node as none. – Master—specifies the role by the remote <i>D-LAG</i> node as master. – slave—specifies the role by the remote <i>D-LAG</i> node as slave. – backupmaster—specifies the role of a remote <i>D-LAG</i> node as backup-master
Fields	• DLAG Keep Alive Count—displays the Keep Alive Count when <i>D-LAG</i> status is enabled. Each <i>D-LAG</i> node will have a Max Keep alive count and each <i>D-LAG</i> node maintains separate keep alive counts for all other remote <i>D-LAG</i> nodes. The default value is 3.

12.8. DLAG Remote Ports Information

Figure 8: DLAG Remote Ports Information

DLAG Remote Ports Information

Port Channel Index	DLAG SystemID	DLAG Remote Port Index	DLAG Remote Port Bundle State	DLAG Remote Port Sync Status

Screen Objective	This screen is used to access the stored port list information of each remote <i>D-LAG</i> node
NOTE: The parameters in the screen are not populated with values (the screen is blank) if the Link Aggregation System Control is set as Shutdown.	
Navigation	Layer 2 Management > Link Aggregation > Settings > DLAG Remote Ports Settings
Fields	Port Channel Index—displays the Remote Aggregator's interface index. DLAG System ID—displays the 6-octet <i>MAC</i> address value of each remote <i>D-LAG</i> node, which uniquely identifies the remote. DLAG Remote Port Index—displays stored system priority of remote <i>D-LAG</i> nodes. DLAG Remote Port Bundle State—displays port bundle states of each port belonging to the remote <i>DLAG</i> node. The list contains: - upInBndl—sets the port operationally up and actively takes part in aggregation. - standby—sets the port that is capable of joining in aggregation group, when any of the ports in aggregation group goes down. - down—sets the port operationally down in lower layers, or the port is operational in lower layers but temporarily not able to participate in aggregation because of different partner information in the same group. - upIndividual—sets the port to operate individually and not take part in aggregation. DLAG Remote Port Index—displays the current sync status of each port belonging to the remote <i>DLAG</i> node. - inSync—sync status of the port belonging to <i>DLAG</i> node is inSync. - outofSync— sync status of the port belonging to <i>DLAG</i> node is out-of-sync.

13. LLDP

This section describes how to configure Link Layer Discovery Protocol (*LLDP*).

The **LLDP** (Link Layer Discovery Protocol) is a vendor-neutral Data Link Layer protocol used by network devices for advertising their identity, capabilities, and interconnections on an IEEE 802 LAN network. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery as specified in standards document 802.1AB.

LLDP performs functions similar to several proprietary protocols, such as Cisco Discovery Protocol, Extreme Discovery Protocol, Nortel Discovery Protocol (also known as SONMP), and Microsoft's LLTD (Link Layer Topology Discovery).

Information gathered with *LLDP* is stored in the device as a management information database (MIB) and can be queried with the Simple Network Management Protocol (SNMP) as specified in RFC 2922 Physical Topology MIB <https://tools.ietf.org/html/rfc2922>. "The Physical Topology MIB (PTOPO-MIB) provides a standard way to identify connections between network ports and to discover network addresses of SNMP agents containing management information associated with each port. The scope of the physical topology (PTOPO) mechanism is the identification of connections between two network ports. Network addresses of SNMP agents containing management information associated with each port can also be identified."

The topology of an *LLDP*-enabled network can be discovered by crawling the hosts and querying this database.

To access **LLDP** screens, go to **Layer 2 Management > LLDP**.

The **LLDP** link parameters are configured through the screens displayed by the following tabs:

[*LLDP Global Configurations*](#)

[*Configured Traces*](#)

[*LLDP Basic Settings*](#)

[*Interface Settings*](#)

[*Neighbor Information*](#)

[*LLDP Agent Information*](#)

[*LLDP Agent Details*](#)

13.1. LLDP Global Configurations

By default, the tab **Global Settings** displays the **LLDP Global Configuration** screen.

Figure 1: LLDP Global Configurations

LLDP Global Configurations

Global Status: Start

Module Status: Enabled

Version: v1

Apply

Configure Trace Options

Screen Objective	This screen allows the user to enable or disable <i>LLDP</i> module globally and set the <i>LLDP</i> version number.
Navigation	Layer 2 Management > LLDP > Global Settings
Fields	Global Status—select the administrative system control status of <i>LLDP</i>. The options are: - Start—indicates that all resources required by <i>LLDP</i> module should be allocated and <i>LLDP</i> should be supported in the devices on all ports. - ShutDown—indicates that <i>LLDP</i> should be shut down in the devices on all ports and all allocated memory must be released. NOTE: If the Global Status is set as ShutDown, the Module Status cannot be enabled. Module Status—select the administrative status of <i>LLDP</i> module. The list contains: - Enabled—indicates that <i>LLDP</i> is enabled in the device and can be enabled port-wise - Disabled—indicates that <i>LLDP</i> is disabled in the device and is also disabled on all ports. Version Status—select the version of <i>LLDP</i> to be used on the system. The default option is v1 (Version 1). The list contains: - v1—enables <i>LLDP</i> version 1 (2005) on the port. When v1 is enabled, only one MAC address can be assigned to the port. - v2—enables <i>LLDP</i> version 2 (2009) on the port. When v2 is enabled, MAC address can be assigned per port, i.e. the user can have multiple <i>LLDP</i> agents per port.
Buttons	Apply—modifies attributes and saves the changes. Configure Trace Options—accesses the Configured Traces screen

13.2. Configured Traces

Figure 2: Configured Traces

Configured Traces

Traces

☐ Init-Shut	☐ Management
☐ Datapath	☐ Control
☐ Packet Dump	☐ Resource
☐ All Fail	☐ Buf
☐ neigh-trace	
☐ vid-digest	☐ mgmt-vid
☒ critical	☐ redundancy
☐ chassis-id	☐ port-id
☐ ttl	☐ port-descr
☐ sys-name	☐ sys-descr
☐ sys-capab	☐ mgmt-addr
☐ port-vlan	☐ ppvlan
☐ vlan-name	☐ proto-id
☐ mac-phy	☐ pwr-mdi
☐ lagg	☐ max-frame

Apply

Configure Global Options

Screen Objective	This screen allows the user to enable the required debug statements which are useful during debug operations.
Navigation	Layer 2 Management > LLDP Global Settings > LLDP Global Configuration Click Configure Trace Options

Fields	• Traces Status—select the traces for which debug statements is to be generated. The default option is critical. The options are: – Init-Shut—generates debug statements for init and shutdown traces. This trace is generated on failed and successful initialization and shutting down of <i>LLDP</i> related module and memory. – Management—generates debug statements for management traces. This trace is generated when any of the <i>LLDP</i> features is configured. – Datapath—generates the debug statements for datapath traces. This trace is generated during failure in packet processing. – Control—generates debug statements for Control functionality traces. This trace is generated during failure in modification or retrieving of <i>LLDP</i> entries.

Fields (cont)	• Traces Status—the options are: – Packet Dump—generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets. – Resource—generates debug statements for traces with respect to allocation and freeing of all resource except the buffers. – All Fail—generates debug statements for all failure traces. – Buffer—generates debug statements for traces with respect to allocation and freeing of Buffer. – neigh-trace—generates debug statements for neighbour traces. – vid-digest—generates debug statements for <i>VLAN</i> identifier (Vid) digest type, length, and value (TLV) traces – mgmt-vid—generates debug statements for management vid tlv traces. – critical—generates debug statements for critical state machine (SEM). – redundancy—generates the debug statements for the <i>LLDP</i> redundancy module. – chassis-id—generates debug statements for chassis-id TLV traces. – port-id—generates debug statements for port-id TLV trace – ttl—generates debug statements for Time To Live (TTL) TLV trace. – port-descr—generates debug statements for the port description TLV traces. – sys-name—generates debug statements for the system name TLV traces. – sys-descr—generates debug statements for system description TLV traces. – sys-capab—generates debug statements for system capabilities TLV traces. – mgmt-addr—generates debug statements for management address TLV traces. – port-vlan—generates debug statements for port-vlan TLV traces. – ppvlan—generates debug statements for port-protocol-vlan TLV traces. – vlan-name—generates debug statements for vlan-name TLV traces. – proto-id—generates debug statements for protocol-id TLV traces. – mac-phy—generates debug statements for MAC or physical (PHY) TLV traces. – pwr-mdi—generates debug statements for power-through Media Dependent Interface (MDI TLV) traces. – lagg—generates debug statements for link aggregation TLV traces. – max-frame—generates debug statements for maximum frame size TLV traces.
Buttons	• Apply—modifies attributes and saves the changes. • Configure Global Options—accesses the LLDP Global Configuration screen.

13.3. LLDP Basic Settings

Figure 3: LLDP Basic Settings

LLDP Basic Settings

Transmit Interval	30
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
txCreditMax	1
MessageFastTx	30
TxFastInit	1
Apply	

Screen Objective	This screen allows the user to configure the <i>LLDP</i> basic parameters.
Navigation	Layer 2 Management > LLDP > Basic Settings
Fields	Transmit Interval—enter the time interval at which the <i>LLDP</i> frames are transmitted on behalf of this <i>LLDP</i> agent. The value should be restored from non-volatile storage after a re-initialization of the management system. The value ranges from 5 to 32768 seconds. The default value is 30. Holdtime Multiplier—enter the Holdtime Multiplier value, which is the amount of time for which the server should hold the <i>LLDP</i>. This value ranges from 2 to 10 seconds. The default value is 4. The actual time-to-live value used in <i>LLDP</i> frames, as transmitted on behalf of this <i>LLDP</i> agent, can be expressed by the following formula: $TTL = \min (65535, \text{Transmit Interval} * \text{Holdtime Multiplier}).$ - For example, if the value of <i>Transmit Interval</i> is 30 and value of <i>Holdtime Multiplier</i> is 4, then value '120' is encoded in TTL field of <i>LLDP</i> header. The value of this object must be restored from non-volatile storage after a re-initialization of the management system. Reinitialization Delay—enter the delay from when the port admin status becomes 'disabled' until re-initialization will be attempted. The value of this object must be restored from non-volatile storage after a re-initialization of the management system. This value ranges from 1 to 10 seconds. The default value is 2.

Fields (cont)	• Tx Delay—enter the delay between successive <i>LLDP</i> frame transmissions initiated by value / status changes in the <i>LLDP</i> local systems objects. This value ranges from 1 to 8192 seconds. The value should be lesser than or equal to (0.25 * Transmit Interval). The default value is 2. • Notification Interval—enter the time interval during which the local system generates a notification event. In this specific interval, generating more than one notification event is not possible. If additional changes in <i>lldpRemoteSystemsData</i> object groups occur within the indicated throttling period, then these trap events must be suppressed by the agent. The value of this object must be restored from non-volatile storage after a re-initialization of the management system. This value ranges from 5 to 3600 seconds. The default value is 5. • Chassis ID Subtype—select the source of a chassis identifier. The default is Mac Address. The options are: – Chassis Component— represents a chassis identifier based on the value of <i>entPhysicalAlias</i> object for a chassis component – Interface Alias—represents a chassis identifier based on the value of <i>ifAlias</i> for an interface on the containing chassis. – Port Component—represents a chassis identifier based on the value of <i>entPhysicalAlias</i> object for a port or backplane within the chassis. – MAC Address—represents a chassis identifier based on the value of a unicast source address, of a port on the containing chassis. – Network Address—represents a chassis identifier based on a 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 <i>AddressFamilyNumbers</i> value for the specific address type, and the second field is the network address value. – Interface Name—represents a chassis identifier based on the value of <i>ifName</i> object for an interface on the containing chassis. – Local—represents a chassis identifier based on a locally defined value. • Chassis ID—enter the chassis identifier string. This field is enabled only if the Chassis ID subtype is selected as anyone of the following: – Chassis Component—the octet string identifies a particular instance of the <i>entPhysicalAlias</i> object for a chassis component – Port Component—the octet string identifies an instance of the <i>entPhysicalAlias</i> object for a port or backplane component within the chassis. – Local—the Octet string identifies a locally assigned chassis ID. • txCreditMax—enter the maximum number of consecutive <i>LLDP PDUs</i> that can be transmitted any time by the port. This value ranges from 1 to 10. The default value is 1 for <i>LLDP v1</i> and 5 for <i>LLDP v2</i>. • MessageFastTx—enter the interval at which <i>LLDP</i> frames are transmitted on behalf of <i>LLDP</i> agent during fast transmission period. This value ranges from 1 to 3600 seconds. The default value is 30 for <i>LLDP v1</i> and 1 for <i>LLDP v2</i>.

Fields (cont)	TxFastInit—this command configures the value used to initialize the txFast variable which determines the number of transmissions that are made in fast transmission mode. This value ranges from 1 to 8. The default value is 1 for <i>LLDP</i> v1 and 4 for <i>LLDP</i> v2.
Buttons	Apply—modifies attributes and saves the changes.

13.4. Interface Settings

Figure 4: Interface Settings

Interface Settings								
Select	Port	Tx State	Rx State	Tx SEM State	Rx SEM State	Notification Status	Notification Type	Destination MAC
☐	Gi0/1	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/2	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/3	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/4	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/5	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/6	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/7	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/8	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/9	Enabled ▾	Enabled ▾	Idle ▾	Frame Rx ▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/10	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/11	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/12	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/13	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/14	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/15	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/16	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/17	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/18	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/19	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/20	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/21	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/22	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/23	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Gi0/24	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Ex0/1	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Ex0/2	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☐	Ex0/3	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e
☒	Ex0/4	Enabled ▾	Enabled ▾	Initialize ▾	▾	Disabled ▾	Mis-config ▾	01:80:c2:00:00:0e

Screen Objective

This screen allows the user to configure every port of the *LLDP*.

NOTE: The parameters in the screen are not populated with values (the screen is blank) if the *LLDP* Global Sates is set as Shutdown.

Navigation	Layer 2 Management > LLDP > Interface
Fields	• Select—click the port for which the <i>LLDP</i> parameters need to be configured. • Port—displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number). • Tx State—select the status of the <i>LLDP PDU</i> transmitter. The default option is Enabled. The options are: – Enabled—enables transmission of <i>LLDP PDU</i> from one of the ports of the server to the LLDP module – Disabled—disables transmission of <i>LLDP PDU</i> from one of the ports of the server to the LLDP module. • Rx State—select the status of the <i>LLDP PDU</i> receiver. The default option is Enabled. The options are: – Enabled—enables reception of <i>LLDP PDU</i> from one of the ports of the server to the LLDP module. – Disabled—enables reception of <i>LLDP PDU</i> from one of the ports of the server to the LLDP module. • Tx SEM State—displays current status of the Tx state event machine (<i>SEM</i>). • Rx SEM State—displays current status of the Rx <i>SEM</i>. • Notification Status—select the notification status to be set. The default option is Disabled. The options are: – Enabled—enables the notification status. – Disabled—disables the notification status. • Notification Type—select the notification type. The default option is Mis-config. The options are: – Remote-Table-Change—<i>LLDP</i> agent sends trap notification to <i>NMS</i> when a remote table change occurs. – Mis-Config—<i>LLDP</i> agent sends trap notification to <i>NMS</i> when mis-configuration is identified. – Both—<i>LLDP</i> agent sends trap notification to <i>NMS</i> when a remote table change occurs or/and whenever mis-configuration is identified. • Destination MAC—displays the destination <i>MAC</i> address to be used by the <i>LLDP</i> agent for transmission on this port.
Buttons	• Apply—modifies attributes and saves the changes.

13.5. Neighbor Information

Figure 5: Neighbor Information

Neighbor Information

Chassis ID	Local Interface	Hold Time	Capability	Port ID
54:e1:ad:07:0d:87	Gi0/11	3601	---	54:e1:ad:07:0d:87

Clear LLDP Neighbors

Screen Objective	This screen allows the user to obtain the information of the adjacent server connected to the LLDP.
Navigation	Layer 2 Management > LLDP > Neighbors
Fields	Chassis ID—displays the Chassis ID of the peer. This value is a string value with a maximum size of 255. Local Interface—displays the local port on which the peer information is learnt. This value is a string with maximum size 255. Hold Time—displays the destination <i>MAC</i> address to be used by the <i>LLDP</i> agent for transmission on this port. Capability—displays the Hold Time advertised by the peer. Port ID—displays the Port ID advertised by the peer.
Buttons	Clear LLDP Neighbors—clears the Neighbor information

13.6. LLDP Agent Information

Figure 6: LLDP Agent Information

LLDP Agent Info

Interface Id	
MAC Address	
Apply	

Screen Objective	This screen allows the user to configure the destination <i>MAC</i> address to be used by the LLDP agent for transmission on this port.
Navigation	Layer 2 Management > LLDP > Agent Info
Fields	Interface ID—enter the Interface ID for which the <i>LLDP</i> Agent info is to be configured. The Interface Id value ranges between 1 and 24. MAC Address—enter the <i>MAC</i> address to be used as <i>LLDP</i> agent <i>MAC</i> address by the <i>LLDP</i> agent on the specified port.

Fields (cont)	NOTE: When <i>LLDP</i> Version is set as V1, only one <i>MAC</i> address can be assigned for a port. NOTE: When <i>LLDP</i> Version is set as V2, multiple <i>MAC</i> addresses can be assigned per port, i.e. the user can have multiple <i>LLDP</i> agents per port.
Buttons	Apply—modifies attributes and saves the changes.

13.7. LLDP Agent Details

Figure 7: LLDP Agent Details

LLDP Agent Details

Interface Id	MAC Address	Port Descriptor TLV	System Name TLV	System Description TLV	System Capability TLV	Management Address TLV	Management Address Type	Management Address	Port Vlan Id TLV	Protocol Vlan Id TLV
Apply										

Protocol Vlan Id	Vlan Name TLV	Vlan Name	Vid Usage Digest TLV	Management Link Vid TLV	Link Aggregation TLV	MacPhy Config TLV	Max FrameSize TLV

Select	Port	Mac Address	Port Descriptor TLV	System Name TLV	System Description TLV	System Capability TLV	Management Address TLV	Management Address Type	Management Address	Port Vlan Id TLV	Protocol Vlan Id TLV	Protocol Vlan Id	Vlan Name TLV	Vlan Name	Vid Usage Digest TLV	Management Link Vid TLV	Link Aggregation TLV	MacPhy Config TLV	Max FrameSize TLV
☐	G0/1	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/2	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/3	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/4	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/5	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/6	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/7	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/8	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/9	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/10	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/11	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/12	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/13	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/14	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/15	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/16	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/17	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/18	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/19	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/20	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/21	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/22	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/23	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	G0/24	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	Ex0/1	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	Ex0/2	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	Ex0/3	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☒	Ex0/4	01:80:c2:00:00:0e	Enabled	Enabled	Enabled	Enabled	Enabled	IPv4	172.16.25.101	Disabled	Disabled	-	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

Screen Objective	This screen allows the user to configure the <i>LLDP</i> Agent details.
Navigation	Layer 2 Management > LLDP > Agent Details

Fields	• Interface ID—enter the Interface ID for which the <i>LLDP</i> Agent info is to be configured. The Interface Id value ranges between 1 and 24. • MAC Address—enter the <i>MAC</i> address to be used as <i>LLDP</i> agent <i>MAC</i> address by the <i>LLDP</i> agent on the specified port. NOTE: – When <i>LLDP</i> Version is set as V1, only one <i>MAC</i> address can be assigned for a port. – When <i>LLDP</i> Version is V2, multiple <i>MAC</i> addresses can be assigned per port, i.e. the user can have multiple <i>LLDP</i> agents per port. This screen can be configured for a specific <i>MAC</i> address only if an agent is created with a <i>MAC</i> Address using the <i>LLDP</i> Agent Info screen. • Port Descriptor TLV—select the transmit status for Port Description <i>TLV</i> (Type, Length, Value). The default option is Disabled. The list contains: – Enabled—Indicates that <i>LLDP</i> agent transmits Port Description <i>TLV</i>. – Disabled—Indicates that <i>LLDP</i> agent discards Port Description <i>TLV</i>. • System Name TLV—select the transmit status for System Name <i>TLV</i>. The default option is Disabled. The list contains: – Enabled—Indicates that <i>LLDP</i> agent transmits System Name <i>TLV</i>. – Disabled—Indicates that <i>LLDP</i> agent discards System Name <i>TLV</i>. • System Description TLV—select the transmit status for System Description <i>TLV</i>. The default option is Disabled. The list contains: – Enabled—Indicates that <i>LLDP</i> agent transmits System Description <i>TLV</i>. – Disabled—Indicates that <i>LLDP</i> agent discards System Description <i>TLV</i>. • System Capability TLV—select the address type for the Management address. This list contains: – Enabled—Indicates that <i>LLDP</i> agent transmits System Capability <i>TLV</i>. – Disabled—Indicates that <i>LLDP</i> agent discards System Capability <i>TLV</i>. • Management Address TLV—select the transmit status for System Description <i>TLV</i>. The default option is Disabled. The list contains: – All—selects the address type for the Management address as both <i>IPv4</i> and <i>IPv6</i> addresses. – <i>IPv4</i>—selects the address type for the Management address as <i>IPv4</i>. – <i>IPv6</i>—selects the address type for the Management address as <i>IPv6</i>. • Management Address—enter the Management IP address for the <i>TLV</i> as per the address type selected. • Port VLAN Id TLV—select the transmit status for Port <i>VLAN</i> ID <i>TLV</i>. The default option is Disabled. The list contains:

Fields	– Enabled—Indicates that <i>LLDP</i> agent transmits Port <i>VLAN ID TLV</i>. – Disabled—Indicates that <i>LLDP</i> agent discards Port <i>VLAN ID TLV</i>. • Protocol VLAN Id TLV—select the transmit status for Protocol VLAN Id <i>TLV</i>. The default option is Disabled. The list contains: – Enabled—Indicates that <i>LLDP</i> agent transmits Protocol VLAN ID <i>TLV</i>. – Disabled—Indicates that <i>LLDP</i> agent discards Protocol VLAN ID <i>TLV</i>. • Protocol VLAN Id—select the transmit status for Protocol VLAN ID. It indicates that <i>LLDP</i> agent should transmit Port VLAN ID <i>TLV</i>. – all—indicates that <i>LLDP</i> agent transmits all Protocol VLAN ID <i>TLV</i>. • VLAN Name TLV—select the <i>VLAN Name TLV</i> for enabling or disabling the transmission of the <i>LLDP</i> agent. The default option is Enabled. The list contains: – Enabled—Indicates that <i>LLDP</i> agent transmits VLAN Name <i>TLV</i>. – Disabled—Indicates that <i>LLDP</i> agent discards VLAN Name <i>TLV</i>. • VLAN Name—enter the specific <i>VLAN ID</i> for which the <i>LLDP</i> agent transmits PDUs. All indicates that <i>LLDP</i> agent transmits all <i>VLANs</i>. • Vid Usage Digest TLV—select the transmit status for Vid Usage Digest <i>TLV</i>. The default option is Disabled. The list contains: – Enabled—specifies that <i>LLDP</i> agent transmits Vid Usage Digest <i>TLV</i>. – Disabled—specifies that <i>LLDP</i> agent discards Vid Usage Digest <i>TLV</i>. • Management Vid TLV—select the transmit status for Management Vid <i>TLV</i>. The default option is Disabled. The list contains: – Enabled—specifies that <i>LLDP</i> agent transmits Management Vid <i>TLV</i>. – Disabled—specifies that <i>LLDP</i> agent discards Management Vit <i>TLV</i>. • Link Aggregation TLV—select the transmit status for Link Aggregation <i>TLV</i>. The default option is Disabled. The list contains: – Enabled—specifies that <i>LLDP</i> agent transmits Link Aggregation <i>TLV</i>. – Disabled—specifies that <i>LLDP</i> agent discards Link Aggregation <i>TLV</i>. • MacPhy Config TLV—select the transmit status for MacPhy Config <i>TLV</i>. The default option is Disabled. The list contains: – Enabled—specifies that <i>LLDP</i> agent transmits MacPhy Config <i>TLV</i>. – Disabled—specifies that <i>LLDP</i> agent discards MacPhy Config <i>TLV</i>. • Max Frame Size TLV—select the transmit status for Max Frame Size <i>TLV</i>. The default option is Disabled. The list contains: – Enabled—specifies that <i>LLDP</i> agent transmits Max Frame Size <i>TLV</i>. – Disabled—specifies that <i>LLDP</i> agent discards Max Frame Size <i>TLV</i>.
Buttons	• Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

Serial Management

14. Serial Communication

Serial communication is used to exchange information between two hosts. The most used serial communication standards are *RS-232*, *RS-422*, and *RS-485* and these are supported on the serial-card. An understanding of these communication standards is needed to ensure correct connectivity and application. Presented here is a summary of these standards and how they can be used on a physical level

14.1. Comparison of Serial Communication Standards

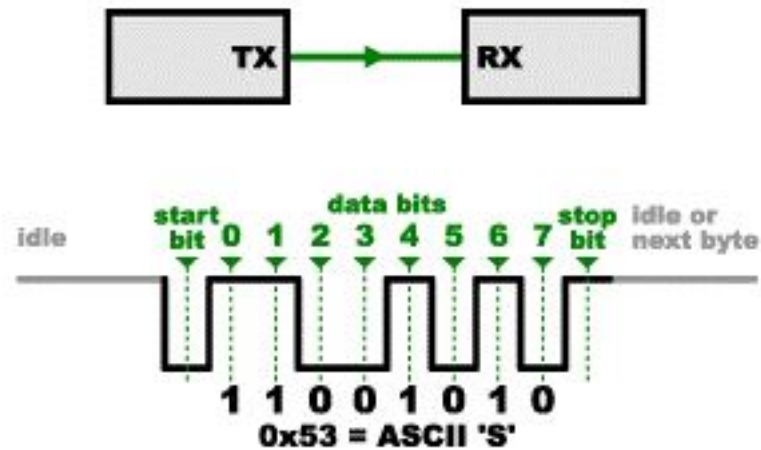
Table 1: Comparison of Serial Communication Standards

	<i>RS-232</i>	<i>RS-422</i>	<i>RS-485</i>
Cable	Single ended	Single ended multi-drop	Multi-drop
Number of Devices	1 transmitter 1 receiver	1 transmitter 10 receivers	32 transmitters 32 receiver
Communication Mode	Full duplex	Full duplex, Half duplex	Full duplex, Half duplex
Maximum Distance	50 feet at 19200 bps	4000 feet at 100 kbps	4000 feet at 100 kbps
Maximum Data Rate	1 Mbps	10 Mbps at 50 feet	10 Mbps at 50 feet

14.2. 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 *CTS* and *RTS* lines. The *RS-232* standard has been commonly used in computer serial ports and is still widely used in industrial communication devices.

Figure 1: RS-232



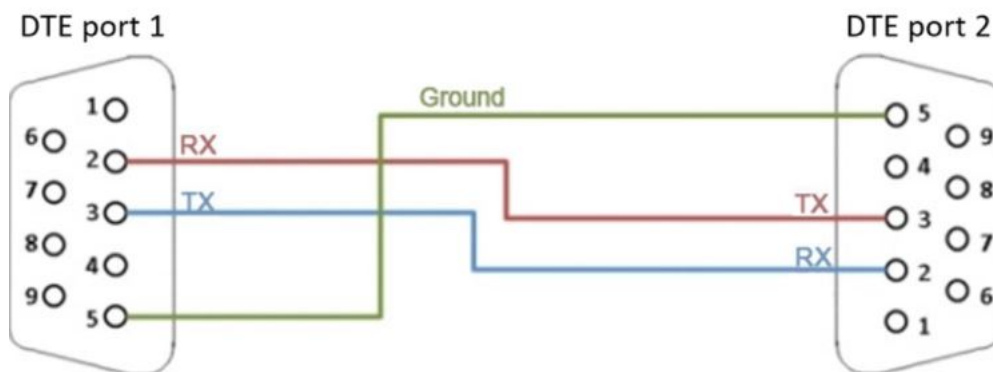
RS-232 Connectivity

A subset of the RS-232 standard signals are available on a serial card, and they allow for most use cases. The signals available are *TX*, *RX*, *RTS*, and *CTS* and can be used in different combinations to achieve different results.

3-wire Mode

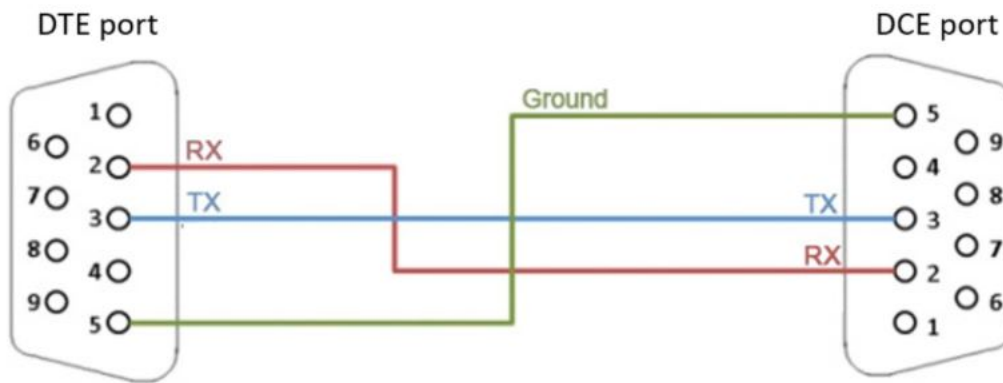
This is the simplest connection where two devices can communicate with each other which requires the use of the *TX*, *RX*, and ground lines. The *TX* line of one device is connected to the *RX* line of the other device (and visa versa). This allows one device to send a message to the other device and the other device to send a message back.

Figure 2: 3-wire Mode



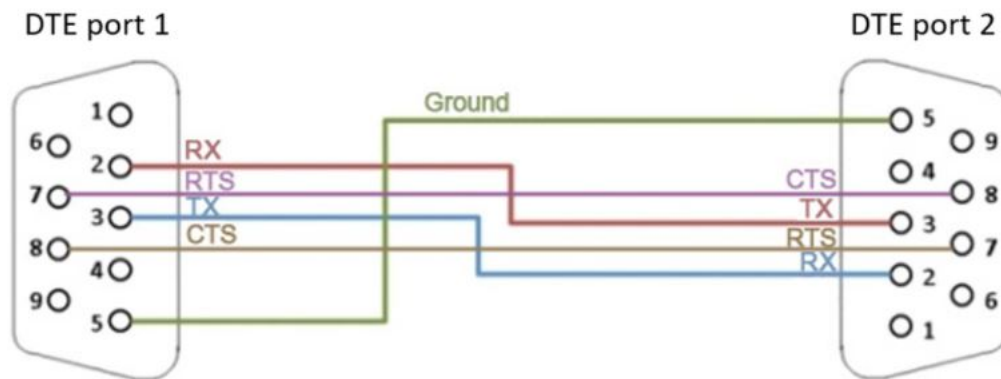
Simple Null Modem Cable Route

In some cases, the communication takes place through another device, such as a modem. In this case, the *RX* and *TX* signals are not swapped.

Figure 3: Simple Null Modem Cable Route

Simple Straight Through Cable Route - 5-wire Mode

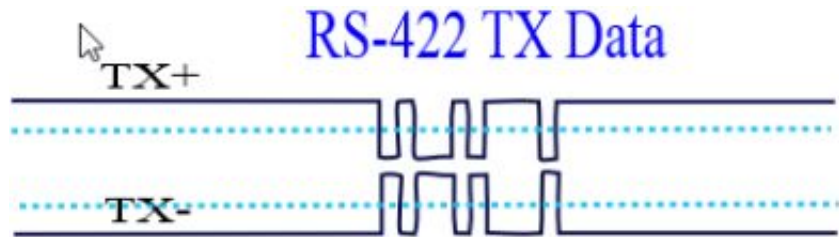
For the case where a device cannot process all the serial data at line speed, extra flow control signals can be used to pace the data into a device. This can be achieved with the *RTS* and *CTS* lines and are connected as follows:

Figure 4: Simple Straight Through Cable Route - 5 wire Mode

14.3. 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.

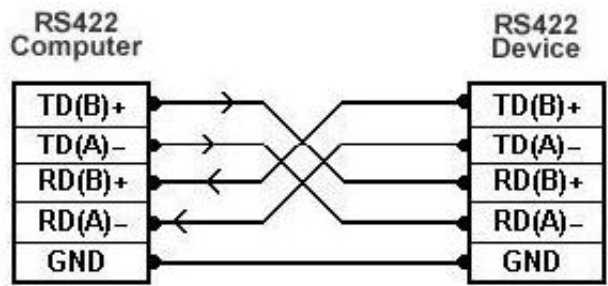
Figure 5: RS-422



Direct Connect Mode

This is the equivalent of the RS-232 3-wire Mode for RS-422, but allows for faster speeds, longer cables as it is more immune to noise.

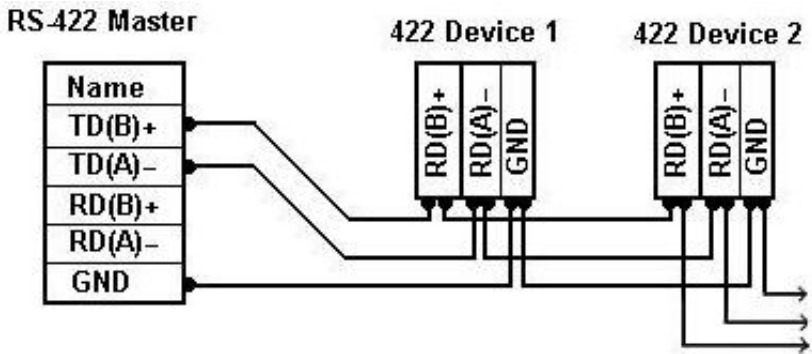
Figure 6: Direct Connect Mode



Multi Listener Mode

RS-422 also allows for up to 10 devices to be connected to the TX lines of the master. This allows for one-way communication (or only one device replying).

Figure 7: Multi Listener Mode



14.4. RS-485

The *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.

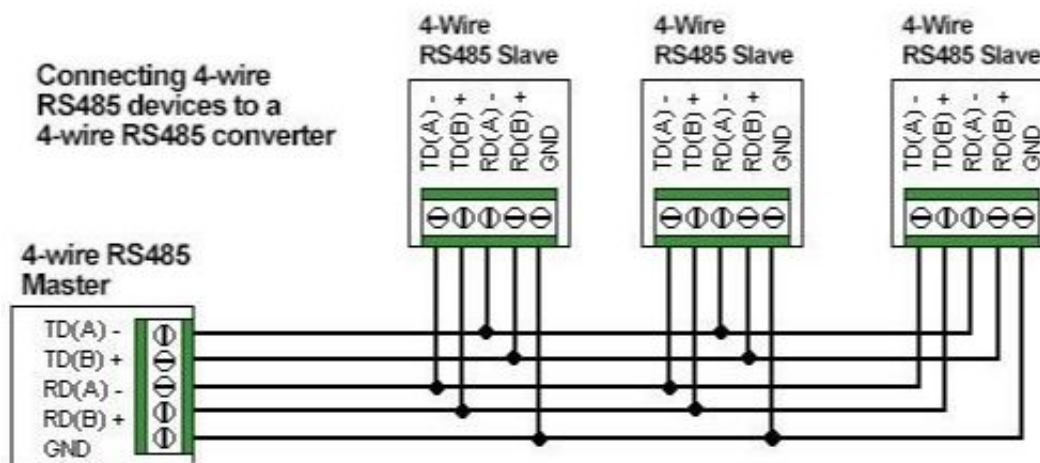
Figure 8: RS-485



4-Wire Full-duplex Mode

In 4-wire mode, the master, which can be either *RS-485* or *RS-422*, can transmit a message to all *RS-485* slaves and the addressed slave can reply to the master. Slaves can not communicate among themselves.

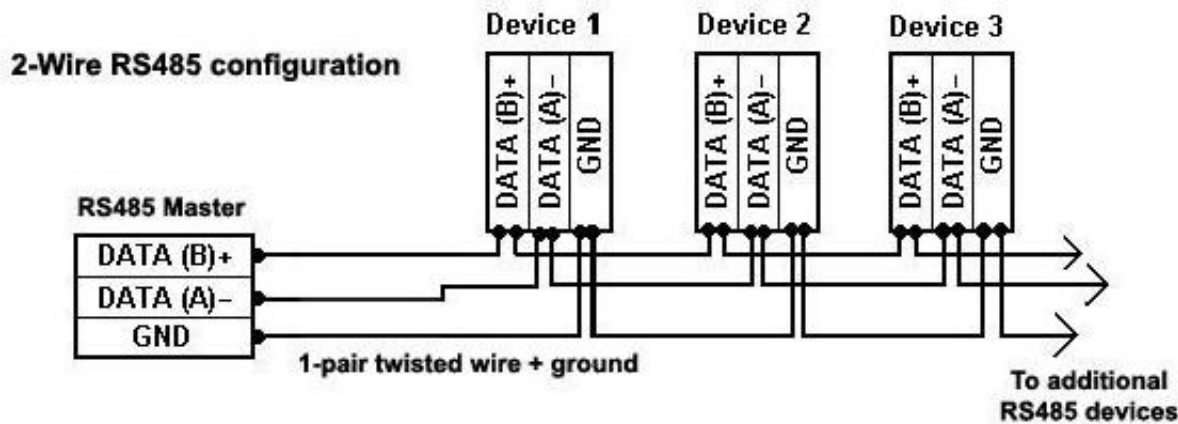
Figure 9: 4-wire Full-duplex Mode



2-wire Half-duplex Mode

In this mode all devices can communicate with each other, but only one device can communicate at a time. Higher level protocols and addressing schemes need to be used.

Figure 10: 2-wire Half-duplex Mode



14.5. Serial Port Configuration

Use the **Serial Port Configuration** dialog box to configure all characteristics of a serial port. To access **Serial Port Configuration** screens, go to **Serial Management > Serial Port Configuration**. By default, the tab **Serial Management** displays the **Serial Port Configuration** screen.

Serial Port Configuration

Figure 11: Serial Port Configuration

Serial Port Configuration

	Name	Alias	Description	Admin Status	Interface Type	Termination Resistor	Baud Rate	Data Bits	Stop Bits	Parity	Flow Control	Duplex	Turn Around Delay	Hold Time	Rx to Tx Delay
☐	Se0/9			Up	RS-232	Disabled	9600	8	2	Even	None	Half	0	0	500
☐	Se0/10			Up	RS-232	Disabled	9600	8	1	None	None	Full	0	0	0
☐	Se0/11			Up	RS-232	Disabled	9600	8	1	None	None	Full	0	0	0
☐	Se0/12			Up	RS-232	Disabled	9600	8	1	None	None	Full	0	0	0
☐	Se0/13			Up	RS-232	Disabled	9600	8	1	None	None	Full	0	0	0
☐	Se0/14			Up	RS-232	Disabled	9600	8	1	None	None	Full	0	0	0
☐	Se0/15			Up	RS-232	Disabled	9600	8	1	None	None	Full	0	0	0
☐	Se0/16			Up	RS-232	Disabled	9600	8	1	None	None	Full	0	0	0

Apply

Screen Objective	This screen allows the user to configure the Serial Port Configuration .
Navigation	Serial Management > Serial Port Configuration
Name	Select a serial port.
Alias	Describe the ifAlias for the interface of the serial port. This is a string with a maximum of 63 characters.
Description	Enter the description of the serial port. This is a string with a maximum of 27 characters.
Admin Status	• Up—select for the interface to be up. • Down—select for the interface to be shut down.
Interface Type	• RS-232—enter this option for <i>RS-232</i> interface. This is default. Use this option for full duplex, maximum distance of 15 meters at 9600 bps, contacts such as TxD, RxD, <i>RTS</i>, <i>CTS</i>, <i>DTR</i>, <i>DSR</i>, <i>DCD</i>, <i>GND</i>, point-to-point topology, and 1 connected device • RS-422—enter this option for <i>RS-422</i>. Use this option for full duplex, maximum distance of 1200 meters at 9600 bps, 4 wires with contacts such as TxA, TxB, RxA, RxB and a common <i>GND</i> wire, point-to-point topology, and 1 transmitting device (with 10 devices in receive mode). • RS-485-2—enter this option for <i>RS-485</i> (2 wires). Use this option for multipoint topology or maximum number of 32 connected devices (with the help of additional repeaters and signal amplifiers up to 256 devices). Other characteristics are half duplex, maximum distance of 1200 meters at 9600 bps and contacts such as DataA, DataB, and <i>GND</i>. • RS-485-4—this option for <i>RS-485</i> (4 wires). Use this option for multipoint topology or maximum number of 32 connected devices (with the help of additional repeaters and signal amplifiers up to 256 devices). Other characteristics are full duplex, maximum distance of 1200 meters at 9600 bps and contacts such as DataA, DataB, and <i>GND</i>.
Termination Resistor	Specify the status of the termination resistor. The options are: • Disabled—enter this option to disable the termination resistor. This is default. • Enabled—enter this option to enable the termination resistor. A special 120-ohm termination resistor can be used to prevent reflection of the signal from the end of the line for interface with 1200 meters distance between the receiver and the transmitter. For <i>RS-422</i>, the resistor is set between <i>RX +</i> and <i>RX-</i>contacts at the beginning and end of the line. NOTE: This field can be configured only for <i>RS-422</i> and <i>RS-485</i> interfaces.

Baud Rate	Select a number that represent the baud-rate setting. The available values are: • 115200 baudrate of 115200 bps • 1200 baudrate of 1200 bps • 14400 baudrate of 14400 bps • 19200 baudrate of 19200 bps • 230400 baudrate of 230400 bps • 2400 baudrate of 2400 bps • 38400 baudrate of 38400 bps • 4800 baudrate of 4800 bps • 57600 baudrate of 57600 bps • 9600 baudrate of 9600 bps - this is the default option
Data Bits	Select the number of bits for the port to operate with. The available values are: • 8—this is default. Binary data is typically transmitted as eight bits. • 7—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 0
Stop Bits	Select the number of stop bits to signal the end of a serial frame or packet. The available values are: • 1—this is default. Choose 1 stop bit if parity is used. • 2—choose 2 stop bits with no parity.
Parity	Select a number for parity. 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. The available options are: • None—this is default. Select this option for no error checking mechanism. • Odd—select this option for the number of 1's in the data plus parity to be an even number. • Even—select this option for the number of 1's in the data plus parity to be an odd number.

Flow Control	Select a method of flow control. 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. The available options are: • None—this is default. Select this option for no error checking mechanism. • Hardware—select this option for the hardware flow control. For RS-232, the hardware method uses the <i>RTS/CTS</i> outputs. If the transmitter is ready to send data, then it sets the signal on the <i>RTS</i> line. If the receiver is ready to receive data, it sets the signal on the <i>CTS</i> line. If one of the signals is not set, no data transfer will occur. • Software—select this option for the software flow control. 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.
Duplex	Select the number of enable half duplex or full duplex speed. The options are: • Full—this is default. Use this option when data can be received and transmitted simultaneously. • Half—choose this option for half duplex. Half duplex is to be used while the interface is either transmitting or receiving.
Turn Around Delay	Enter a number for the turn around delay. 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. This an integer in the range of 0 to 1000 ms with a default of 0 ms.
Hold Time	Enter a a value, in milliseconds, for the delay time after which <i>UART</i> start listening to Rx line. This an integer in the range of 0 to 15000 ms with a default of 0 ms. Hold time is the maximum amount of time that the serial packet can be held in the queue before being sent to the serial line.
Rx to Tx Delay	Enter a number for the Rx to Tx Delay. This is the delay between Receive mode and Transmit mode. This an integer in the range of 0 to 1000 ms.
Buttons	• Apply—modifies attributes and saves the changes.

14.6. Serial Profile Configuration

Use the **Serial Profile Configuration** dialog box to configure all parameters of a serial profile.

To access **Serial Port Configuration** screens, go to **Serial Management > Serial Profile Configuration**.

By default, the tab **Serial Management** displays the **Serial Port Configuration** screen.

Serial Profile Configuration

Figure 12: Serial Profile Configuration

Serial Profile Configuration

Profile Name

Connection Type

Raw Socket

Protocol

TCP

Direction

Out

Add

Profile Name	Status	Connection Type	Protocol	Direction / Role	Interfaces	Show	Delete
p1	inactive	Raw Socket	TCP	In	Se0/9	Show	Delete
p2	inactive	Preemptive Raw Socket	TCP	In	None	Show	Delete
p3	inactive	Modbus	TCP	Server	None	Show	Delete
m1	inactive	Modbus	TCP	Client	None	Show	Delete

The add form in this page is dynamic. When **Raw Socket** connection type is selected, protocol and direction fields are shown. If a protocol is switched to UDP, direction will be hidden.

Figure 13: Raw Socket with UDP

Serial Profile Configuration

Profile Name

Connection Type

Raw Socket

Protocol

UDP

Add

Figure 14: Preemptive Raw Socket

Serial Profile Configuration

Profile Name

Connection Type

Preemptive Raw Socket

Add

Finally, if **Modbus** connection type is selected, both protocol and direction fields will be hidden but a new field **Role** appears.

Figure 15: Role Modbus

Serial Profile Configuration

Profile Name

Connection Type

Modbus

Role

Server

Add

Screen Objective	This screen allows the user to configure the Serial Profile Configuration Status.
Navigation	Serial Management > Serial Profile Configuration
Profile Name	Enter the name of the profile.
Status	This field displays the status of the display.
Connection	This field displays / configures the connection type. The options are: • Raw Socket—select this option for raw mode. User can configure a simple raw mode for <i>TCP</i> or <i>UDP</i> communication. • Preemptive Raw Socket—select this option for preemptive mode. The device acts as a server in preemptive mode. In this mode, direction and protocol are implicitly set as IN and <i>TCP</i>. Any dynamic client can preempt the permanent client and start communicating with the device for specified period of time. • Modbus—select this option for Modbus.
Protocol	This field displays / configures the protocol type. The options are: • TCP—select for Transmission Control Protocol (<i>TCP</i>). • UDP—select for User Datagram Protocol (<i>UDP</i>).
Direction / Role	This field displays / configures the direction for a serial protocol. Select one of the following options: • Out—select this option if the device acts as a client in OUT direction. • In—select this option when the device acts as a server. • In-Out—select this option if the device acts as both server and client in IN-OUT direction. For UDP transport protocol, the default direction is IN-OUT
Interfaces	This field displays details about the serial interface.
Buttons	• Add—click to modify attributes and save the changes. • Show—click this button to display the configuration in a separate dialog box • Delete—click this button to delete the configured profile. • Apply—click this button to delete the configured profile.

Use the **Show** button display a configuration panel on the right side of page to edit the given profile. Each page will include a **Close** button for exiting the Serial Profile Configuration panel. The following options are available.

Figure 16: Profile p1 - Raw Socket In Configuration

Raw Socket In Configuration

Name	p1
Status	Inactive ▾
Interface	Se0/9 ▾
Packetizing	On ▾
Packet Size	1340
Packet Timer (ms)	500
Packet Character (Hex)	Off
Packet Buffering	Enabled ▾
Local Server IP	192.168.20.1
Local Server Port	15010
Keep Alive Timeout (s)	240
Maximum Connections	64
Apply Close	

Figure 17: Profile 3 - Raw Socket In-Out Configuration

Raw Socket In-Out Configuration

Name	profile3
Status	Inactive
Interface	None
Packetizing	On
Packet Size	1400
Packet Timer (ms)	10
Packet Character (Hex)	Off
Packet Buffering	Disabled
Keep Alive Timeout (s)	240

In Configuration

Local Server IP	0.0.0.0
Local Server Port	0
Maximum Connections	64

Out Configuration

Remote Server IP	0.0.0.0
Remote Server Port	0
Local Client Port	0
Reconnect Timeout (s)	120

Figure 18: Profile 1- Raw Socket Out Configuration

Raw Socket Out Configuration

Name	profile1
Status	Inactive ▼
Interface	None ▼
Packetizing	On ▼
Packet Size	1400
Packet Timer (ms)	10
Packet Character (Hex)	Off
Packet Buffering	Disabled ▼
Remote Server IP	0.0.0.0
Remote Server Port	1
Local Client Port	15010
Reconnect Timeout (s)	120
Keep Alive Timeout (s)	240
Apply Close	

Screen Objective	This screen allows the user to apply the Serial Profile Configuration .
Name	This field displays the profile name.
Status	This field configures the status of the profile. The options are: • Inactive—select for inactive profile. • Active—select for active profile.
Interface	This field configures the interface for the profile. The options are: • None • Se0/9 • Se0/10 • Se0/11 • Se0/12 • Se0/13 • Se0/14 • Se0/15 • Se0/16

Packetizing	This field configures the status of the packetizing feature. The options are: • On—select for packetizing enabled. • Off—select for packetizing disabled.
Packet Size	Enter a value for packet size. The range is from 16 to 1400. The default value is 1400.
Packet Timer (ms)	Enter a value for the delay between the packets sent from serial ports. The range is from 0 to 1000. The default value is 10 ms.
Packet Character (hex)	Enter a value for the delay between the packets sent from serial ports. The range is from 0 to 255. The default value is 10 ms. Or configure it as OFF to disable packet character feature. This is the default option.
Packet Buffering	This field configures the status of the packet buffering feature. The options are: • Enabled—select for enabled Packet Buffering. • Disabled—select for disabled Packet Buffering.
Local Server IP	Enter a local server IP address.
Local Server Port	Enter a value for the local port number. Port numbers range between 15010 to 15110. For Modbus, the software internally assigns 502 <i>TCP</i> port number if an user configures modbus as its port.
Keep Alive Timeout (s)	Enter a value for the time which specifies how long the device will wait for a response to keep alive packets sent before terminating the <i>TCP</i> connection. The range is from 60 to 600. The default value is 240 s.
Maximum Connections	Enter a value for the maximum number of allowed incoming <i>TCP</i> connections. The range is from 1 to 64. The default value is 64.
Buttons	• Add—click to modify attributes and save the changes. • Show—click this button to display the configuration in a separate dialog box • Delete—click this button to delete the configured profile. • Apply—click this button to apply the configured profile. • Close—click this button to exit the configured profile.

Figure 19: Profile 4 - Raw Socket UDP Configuration

Raw Socket UDP Configuration

Name	profile4
Status	Inactive ▼
Interface	None ▼
Packet Size	1400
Packet Timer (ms)	10
Packet Character (Hex)	Off
Local IP	0.0.0.0
Local Port	0
Maximum Connections	64
Remote Connections	Configure
ApplyClose	

Figure 20: Profile 4 - Raw Socket UDP Remote Connection Configuration

Raw Socket UDP Configuration

Name	profile4
Status	Inactive ▼
Interface	None ▼
Packet Size	1400
Packet Timer (ms)	10
Packet Character (Hex)	Off
Local IP	0.0.0.0
Local Port	0
Maximum Connections	64
Remote Connections	Hide
ApplyClose	

Serial UDP Remote Connection Configuration

Server IP

Server Port 1

Add

Server IP	Server Port	Delete
192.168.3.3	1	Delete

Some extra parameters shown in the **Raw Socket UDP Configuration** interface are as shown below.

Screen Objective	This screen allows the user to apply the Raw Socket UDP Configuration .
Server IP	Enter a local server IP address.
Server Port	Enter a value for the server port number.
Remote Connections	Enter a value for the maximum number of allowed incoming <i>TCP</i> connections. The range is from 1 to 64. The default value is 64.

Figure 21: Profile p2 - Preemptive Raw Socket Configuration

Preemptive Raw Socket Configuration

Name	p2
Status	Inactive ▼
Interface	None ▼
Packetizing	On ▼
Packet Size	1400
Packet Timer (ms)	Off
Packet Character (Hex)	0x64
Packet Buffering	Disabled ▼
Dynamic Packet Timer (ms)	100
Dynamic Packet Character (Hex)	0xff
Local Server IP	0.0.0.0
Local Server Port	15010
Keep Alive Timeout (s)	240
Dynamic Idle Timeout (s)	10
Permenant Remote Client IP	192.168.20.66
Apply Close	

Figure 22: Profile p3- Modbus Server Configuration

Modbus Server Configuration

Name	p3
Status	Inactive
Local IP	0.0.0.0
Local Port (502 or 15010-15110)	502
Keep Alive Timeout (s)	240
Maximum Connections	64
Transmit Exceptions	Enabled
Maximum Pending Messages	16
Interface Configuration	Configure
Apply Close	

Figure 23: Profile 6 - Modbus Server Interface Configuration

Modbus Server Configuration

Name	profile6
Status	Inactive
Local IP	0.0.0.0
Local Port (502 or 15010-15110)	502
Keep Alive Timeout (s)	240
Maximum Connections	64
Transmit Exceptions	Enabled
Maximum Pending Messages	16
Interface Configuration	Hide
Apply Close	

Modbus Server Interface Configuration

Interface	None
Response Timeout (ms)	2000
Slave ID's	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20
Apply	

Interface	Response Timeout (ms)	Slave ID's	Delete	Edit

Figure 24: Profile 7 - Modbus Client Configuration

Modbus Client Configuration

Name

Status

Interface

Remote IP

Remote Port

Local Port (502 or 15010-15110)

Keep Alive Timeout (s)

Reconnect Timeout (s)

m1

Inactive

None

0.0.0.0

502

502

240

120

Slave ID's

☐ 1

☐ 2

☐ 3

☐ 4

☐ 5

☐ 6

☐ 7

☐ 8

☐ 9

☐ 10

☐ 11

☐ 12

☐ 13

☐ 14

☐ 15

☐ 16

Select All

Deselect All

Response Timeout (ms)

DSCP

Forward Exception

300

0

Enabled

Apply

Close

Some extra parameters shown in the **Modbus Configuration** interface are as shown below.

Screen Objective	This screen allows the user to apply the Modbus Server / Client Configuration .
Transmit Exceptions	Select an option to enable / disable sending <i>TCP</i> exception back to the master if a response has not been received from RTU within the expected time. - Enabled - Disabled
Maximum Pending Messages	Enter a value for the maximum number of messages that Modbus server can handle from different clients. The range is from 0 to 16. The default value is 16.
Interface Configuration	If needed, select the button Configure . When this option is selected, the Modbus Server Interface Configuration dialog box appears which has the following parameters as shown below.

Interface	This field configures the interface for the profile. The options are: • None • Se0/9 • Se0/10 • Se0/11 • Se0/12 • Se0/13 • Se0/14 • Se0/15 • Se0/16
Response Timeout (ms)	Enter a value for the time to wait for a response from a serial port. The range is from 50 to 10000. The default is 2000 ms (as shown in the figure).
Slave ID's	Enter a value for the slave ID. The format is comma separated integer values with a maximum of 10 slave IDs per command. The range is from 1 to 247. For Modbus Client Configuration, there two extra buttons as follows: • Select All • Deselect All
DSCP	Enter a value decimal value for the Differentiated service code point (<i>DSCP</i>) which is set in the IP header for the outgoing packets. The range is from 0 to 63. The default is 0 (as shown in the figure).
Forward Exception	Select an option to enable / disable forwarding <i>TCP</i> exception back to the master if a response has not been received from RTU within the expected time. • Enabled—enter this option to enable forwarding <i>TCP</i> exception. Default is enabled which is numerically denoted as 1. • Disabled—enter this option to disable forwarding <i>TCP</i> exception. The numerical notation for disabled is 0.

14.7. Serial Port Statistics

This screen displays the **Serial Port Statistics** parameters for all serial interfaces.

Figure 25: Serial Port Statistics

Serial Port Statistics

Port	Rx					Tx		
	Char Count	Frame Count	Char Discard	Framing Errors	Parity Errors	Char Count	Frame Count	Char Discarded
Se0/9	0	0	0	0	0	0	0	0
Se0/10	0	0	0	0	0	0	0	0
Se0/11	0	0	0	0	0	0	0	0
Se0/12	0	0	0	0	0	0	0	0
Se0/13	0	0	0	0	0	0	0	0
Se0/14	0	0	0	0	0	0	0	0
Se0/15	0	0	0	0	0	0	0	0
Se0/16	0	0	0	0	0	0	0	0

Property	Description
Screen Objective	This screen displays the all serial interface counters for a particular interface.
Navigation	Statistics > Serial > Serial Port Statistics

15. Filters

The ability to filter packets in a modular and scalable way is important for both network security and network management. Access Control Lists (ACL)s provide the capability to filter packets at a fine granularity. Layer 2 ACLs on EVCs (Ethernet Virtual Connection) is a security feature that allows packet filtering based on MAC addresses.

To access **Filters** screens, go to **Layer 2 Management > Filters**.

The **Filters** link parameters are configured through the screens displayed by the following tabs:

[L2 Unicast Filter Configuration](#)

[L2 Multicast Filter Configuration](#)

[L2 Multicast Filter Configuration](#)

15.1. L2 Unicast Filter Configuration

By default, the tab **Unicast Filters** displays the **L2 Unicast Filter Configuration** screen.

Figure 1: L2 Unicast Filter Configuration

L2 Unicast Filter Configuration

FDB ID ▼

MAC Address *

Allowed Ports *

Status ▼

Add Reset

Select	FDB ID	MAC Address	Allowed Ports	Status

Apply
Delete

Screen Objective	This screen allows the user to configure the filter for controlling the Unicast packets that the switch needs to process.
Navigation	Layer 2 Management > Filters > Unicast Filters
Fields	FDB ID—select the specific identifier of Forwarding Database identifier (FDBID) to make forwarding decisions. NOTE: FDB ID is mapped to VLAN ID to share filtering information among them, this FDB ID can be created using Layer 2 Management > VLAN > Static VLANs

Fields (cont)	NOTE: If <i>VLANs</i> are mapped to the FID, this will cause the mapped <i>VLANs</i> to operate in Shared <i>VLAN</i> Learning (SVL) mode. <i>VLANs</i> mapped to a unique FID will operate in Independent <i>VLAN</i> Learning Mode (IVL). A SET operation on this table is allowed only when dot1qFutureVLANLearningMode is hybrid. By default, all <i>VLANs</i> will be mapped to the FID equal to their <i>VLAN</i> ID, when dot1qFutureVLANHybridTypeDefault is IVL. NOTE: If the value of dot1qFutureVLANHybridTypeDefault is SVL, all <i>VLANs</i> will be mapped to FDB ID 1 (as shown in the figure above). • MAC Address—enter the destination Unicast <i>MAC</i> address of the received packet. • Allowed Ports—enter the list of ports to which the received packet (with the above set <i>MAC</i> address) should be forwarded. • Status—select the status types for configuring Unicast filter. The list contains: – Other—specifies that Unicast filter is used currently, but the conditions under which it will remain in use differ from the following values. – Permanent—specifies that entry is allowed to reside even after restart of the switch. – DeleteOnReset—specifies that entry is deleted on restart of the switch. – DeleteOnTimeout—specifies that entry is deleted on expiry of the aging timer.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry

15.2. L2 Multicast Filter Configuration

Figure 2: L2 Multicast Filter Configuration

L2 Multicast Filter Configuration

VLAN ID

vlan1 ▾

MAC Address

*

Allowed Ports

*

Forbidden Ports

Status

Permanent ▾

Add

Reset

Select	VLAN ID	MAC Address	Allowed Ports	Forbidden Ports	Status
☒	1	01:00:5e:00:00:01	Gi0/9	Gi0/16	Permanent ▾

Apply

Delete

Screen Objective	This screen allows the user to configure the filter for controlling the multicast packets that the switch needs to process. A multicast access profile is configured to filter incoming reports that can be commonly utilized by all multicast protocols.
Navigation	Layer 2 Management > Filters > Multicast Filters
Fields	VLAN ID—select the <i>VLAN</i> ID from the list of <i>VLAN</i>s already created in the system. NOTE: <i>VLAN</i> ID can be created using Layer 2 Management > <i>VLAN</i> > Static <i>VLAN</i>s MAC Address—enter the destination Multicast <i>MAC</i> address of the received packet. Allowed Ports—enter the list of ports to which the received packet (with the above set <i>MAC</i> address) should be forwarded. Forbidden Ports—enter the list of ports to which the received packet (with the above set <i>MAC</i> address and if received from the configured port) must not be forwarded. Status—select the status types for configuring Multicast filter. The list contains. - Other—specifies that Unicast filter is used currently, but the conditions under which it will remain in use differ from the following values. - Permanent—specifies that entry is allowed to reside even after restart of the switch. - DeleteOnReset—specifies that entry is deleted on restart of the switch. - DeleteOnTimeout—specifies that entry is deleted expiry of the aging time

Buttons	• Add—adds and saves new configuration. • Reset—resets to default value and discards all user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry

15.3. Forward Ports Configuration

Figure 3: Forward Ports Configuration

Forward Ports Configuration

VLAN ID

Forward All Static

Forward All Forbidden

Forward Unregistered Static

Forward Unregistered Forbidden

Select	VLAN ID	ForwardAll Ports	ForwardAll Static Ports	ForwardAll Forbidden Ports	ForwardUnRegistered Ports	ForwardUnRegistered Static Ports	ForwardUnRegistered Forbidden Ports
☒	1				Gi0/1,Gi0/2,Gi0/3,G	Gi0/1,Gi0/2,Gi0/3,G	

Screen Objective	This screen allows the user to configure the ports for Multicast Forwarding.
Navigation	Layer 2 Management > Filters > Multicast Forwarding
Fields	• VLAN ID—enter the <i>VLAN</i> ID that represents the specific <i>VLAN</i>. This value ranges from 1 to 4094. • Forward All Static—enter the static ports allowing Multicast Forwarding. • Forward All Forbidden—enter the forbidden ports denying Multicast Forwarding. • Forward Unregistered Static—enter the unregistered static ports Multicast Forwarding. • Forward Unregistered Forbidden—enter the unregistered forbidden ports denying Multicast Forwarding. • Forward All Ports—displays the static ports as well as forward and learnt ports. • Forward All Static Ports—displays the static ports allowing Multicast Forwarding. • Forward All Forbidden Ports—displays the forbidden ports denying Multicast Forwarding.

Fields (cont)	• Forward Unregistered Ports—displays all forward unregistered forbidden ports denying Multicast Forwarding. • Forward Unregistered Static Ports—displays the unregistered static ports denying Multicast Forwarding. • Forward Unregistered Forbidden Ports—displays the unregistered forbidden ports denying Multicast Forwarding.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value and discards all user inputs. • Apply—modifies attributes and saves the changes.

16. Mirroring

This section describes how to configure the Mirroring feature.

The **Mirroring** feature is introduced in switches because of a fundamental difference that switches have with hubs. When a hub receives a packet on one port, the hub sends out a copy of that packet to all ports except to the one from where the hub received the packet. After a switch boots, it starts to build up a Layer 2 forwarding table on the basis of the source *MAC* address of the different packets that the switch receives. After this forwarding table is built, the switch forwards traffic that is destined for a *MAC* address directly to corresponding ports.

The switch can support up to 7 port mirroring sessions.

NOTE: The RSPAN feature is not supported at this time.

To access **Mirroring** screens, go to **Layer 2 Management > Mirroring**.

16.1. ISS Mirroring Control Settings

Figure 1: ISS Mirroring Control Settings

Mirroring Control Settings

Session Index

*

Mirror Type

PortBased

▼

*

Source Entity

*

Destination Entity

*

Mode

both

▼

Add

Select	Session ID	Mirror Type	Source Entity	Destination Entity	Mode	Status

Apply

Delete

Screen Objective	This screen allows the user to configure the Mirroring Control Settings.
Navigation	Layer 2 Management > Mirroring

Fields	• Select—click to select the session ID for which the configuration has to be modified or the session needs to be deleted. • Session Index—enter the index of the mirroring session. This value is from 1 to 20. The maximum number of sessions per switch is 7. • Mirror Type—the available option is port-based—receives / transmits mirroring packets depending on Mirroring mode (ingress/egress/both) on “source” port(s) to “destination” port(s) to 20. • Source Entity—enter the source entity which participates in a mirroring session. This is a combination of interface type and interface ID. The interface ID is a combination of slot number and port number (slot number/port number). For example, gi0/1, fa0/1, po1.
Fields	• Destination Entity—enter the destination port entity from which the packets will be transmitted. This is a combination of interface type and interface ID. The interface ID is a combination of slot number and port number (slot number/port number). For example, gi0/1,fa0/1. • Mode—select the mode of mirroring. The default option is Both. The list contains: – ingress—mirrors only traffic that is ingressing to the source ports – egress—mirrors only traffic that is egressing from the source ports – both—mirrors both traffic that is ingressing to the source ports and egressing from the source ports • Status—displays the status of the Mirror Control Extension table entries. The list contains: – Up—indicates the status of Mirror Control Extension table entries as enabled. – Down—indicates the status of Mirror Control Extension table entries as disabled. – Under creation—indicates that the Mirror Control Extension table entries are under creation.
Buttons	• Add—adds and saves new configuration

17. Split-Horizon

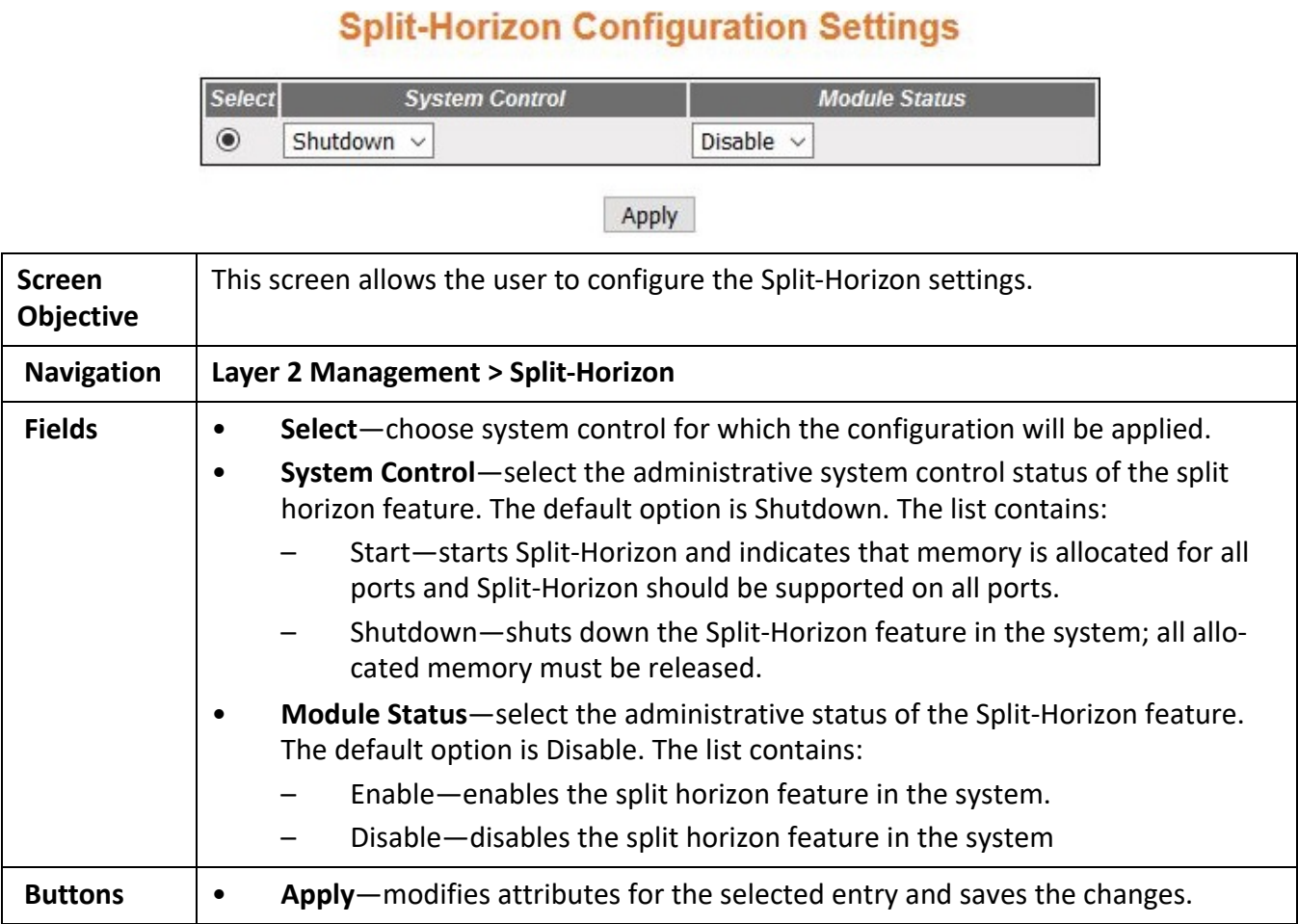
Split-Horizon is a feature used in routing and L2 VPN for avoiding loops. When a router in a network with only one data path receives a data packet, it does not send routing information back along the path on which the packet traveled (i.e., to an adjacent router); it only sends the information forward so that there is no possibility of the packet being routed back along the path it originally traveled. The Split-Horizon allows creating two types of port roles:

- Uplink Ports
- User Ports / Downlink ports

To access **Split-Horizon** screens, go to **Layer 2 Management > Split-Horizon**.

17.1. Split-Horizon Configuration Settings

Figure 1: Split-Horizon Configuration Settings



18. UFD

UFD (Uplink Failure Detection) allows a device to detect a link failure on uplink interfaces and to propagate the failure to the downlink interfaces so that servers connected to those downlink interfaces can switch over to secondary interfaces.

The *UFD* feature allows the administrator to create groups that contain a set of uplink interfaces and Raptor to monitor uplink interfaces to spot link failures. and a set of downlink interfaces to disable.

UFD supports network adapter teaming and provides network redundancy. In network adapter teaming, all network interface cards on a server are configured in a primary or secondary relationship and share the same IP address. When the primary link goes down, the server transparently shifts the connection to the secondary link. The primary and secondary links are connected to two switches each supporting uplink failure detection *UFD* feature.

When *UFD* is enabled, the switch monitors uplink interfaces for link failures. When the switch detects a link failure, the switch disables the downlink interfaces— one of which is connected to the server. When the server detects disabled downlink interfaces, it switches over to the secondary link connected to another switch to ensure that there is another path for the traffic flow.

To access **UFD** screen, click **Layer 2 Management > UFD Global Configuration**.

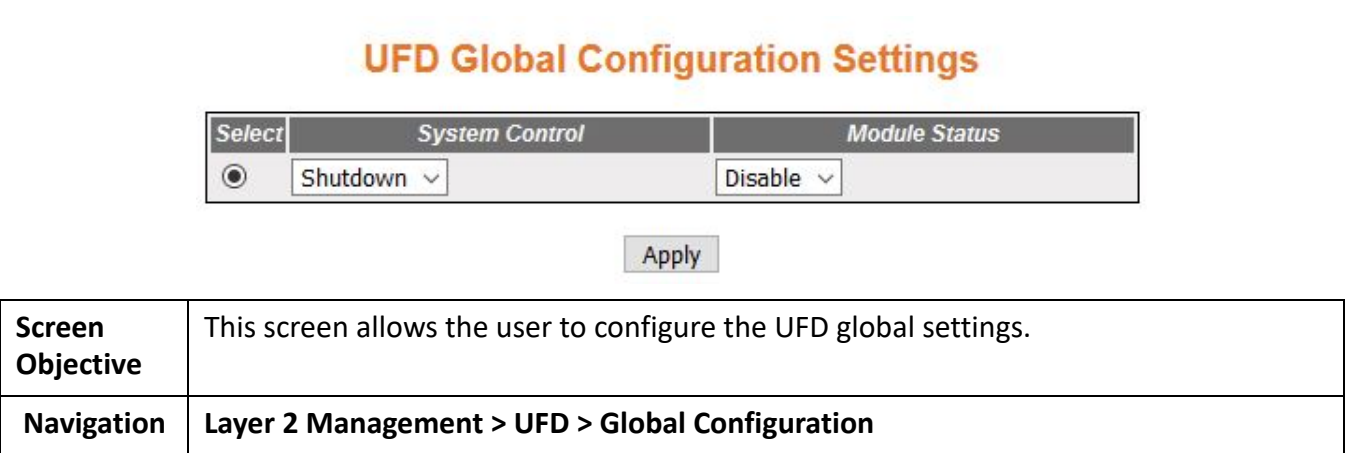
[UFD Global Configuration Settings](#)

[UFD Group Configuration](#)

By default, the tab **UFD** displays the **UFD Global Configuration Settings** screen.

18.1. UFD Global Configuration Settings

Figure 1: UFD Global Configuration Setting



Fields	• System Control—select the administrative system control status of the <i>UFD</i> module. The default option is Shutdown. The list contains: – Start—starts the <i>UFD</i> feature in the system, only when any one uplink port is in admin and operationally in “UP” state in the group. – Shutdown—shuts down the <i>UFD</i> feature in the system, only when all uplink ports within the group is in admin and operationally “DOWN”, or no uplink ports are assigned in the group. • Module Status—select the administrative module status of the <i>UFD</i> module. The default option is Disable. The list contains: – Enable—enables the <i>UFD</i> feature in the system. – Disable—disables the <i>UFD</i> feature in the system.
Buttons	• Apply—modifies attributes and saves the changes.

18.2. UFD Group Configuration

Figure 2: UFD Group Configuration

UFD group Configuration

Group Id *

Group Name

Port List

Designated UplinkPort

Select	Group Id	Group Name	Port List	Designated Uplink Port	UFD Group Status
☒	2	group	Gi0/1,Gi0/6		DOWN

Screen Objective	This screen allows the user to configure the <i>UFD</i> group configuration settings.
Navigation	Layer 2 Management > UFD > Group Configuration
Fields	• Select—click to select the group id for which the configuration need to be applied or deleted. • Group ID—enter the group identifier that uniquely identifies the group. Each group has uplink interfaces to monitor and downlink interfaces to disable. The <i>UFD</i> group ID value zero indicates that the port is not present in any group. By setting the <i>UFD</i> Group ID value to zero, the port will be removed from the <i>UFD</i> group to which it belongs to. This value ranges from 0 to 65535.

Fields	• Group Name—enter the name of the <i>UFD</i> group. This Group Name is a string of maximum size 32. NOTE: The Group Name should be only characters—no numerical symbols allowed. • Port List—enter the port list for <i>UFD</i> group name. – For interface type other than internal-lan and port-channel, this value is a combination of slot number and port number separated by a slash. – For interface types internal-lan and port-channel, only i-lan or port-channel ID is provided. <i>Use comma as a separator without a space while configuring list of interfaces. For example: 0/1, 0/3 or 1, 3</i> • Designated Uplink Port—enter the port that is termed as designated uplink when the port is connected to the network and it has more preference to a particular set of uplink ports. Broadcast/unknown multicast use this designated port to reach uplink. – For interface type other than internal-lan and port-channel, this value is a combination of slot number and port number separated by a slash. – For interface types such as internal-lan and port-channel, only i-lan or port-channel ID is provided. <i>Use comma as a separator without a space while configuring list of interfaces. For example: 0/1, 0/3 or 1, 3</i> • UFD Group Status—displays the <i>UFD</i> group status. The default value is DOWN. The list contains: – UP—specifies the status of the group as 'UP', only when any one uplink port is in admin and operationally 'UP' state in the group. – DOWN—specifies the status of the group as 'DOWN', only when all uplink ports within the group is in admin and operationally 'DOWN' or none uplink ports assigned in the group.
Buttons	• Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

DHCP Map

19. DHCP

This section describes the interfaces for the DHCP Server, Client and Relay.

19.1. DHCP Server

Describes how to configure the Dynamic Host Configuration Protocol Server on the switch.

DHCP (Dynamic Host Configuration Protocol) is used for assigning IP addresses to workstations in a wide variety of devices, such as *ISDN* routers, firewalls, etc. Besides obtaining IP address, other configuration parameters for a workstation can also be configured in a *DHCP* server. *DHCP* clients can retrieve these parameters along with the IP address.

DHCP is based on the 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 clients obtain the address for a time period termed as a “lease” period. *DHCP* clients renew the address by sending a request for the IP address before the lease expires

DHCP uses *UDP* as its transport protocol and a *UDP* port for communication. *DHCP* relay agents connect servers present on one LAN with the clients present on another.

DHCP server is responsible for dynamically assigning unique IP address and other configuration parameters, such as gateway, to the interfaces of a *DHCP* client. The IP address is leased to the interface only for a particular time period as stated in the *DHCP* lease. The interface should renew the *DHCP* lease once it expires. The *DHCP* server contains a pool of IP addresses from which an address is assigned to the interface.

To access **DHCP** screens, go to **Layer 3 Management > DHCP Server**.

The **DHCP Server** is configured through the screens displayed by the following tabs:

[DHCP Basic Settings](#)

[DHCP Pool Settings](#)

[DHCP Pool Settings](#)

[DHCP Server IP Exclude Settings](#)

[DHCP Host IP Settings](#)

[DHCP Host Options Settings](#)

[DHCP Bootfile Configuration](#)

DHCP Basic Settings

By default, the tab **Basic Settings** displays the **DHCP Basic Settings** screen.

Figure 1: DHCP Basic Settings

DHCP Basic Settings

DHCP Server	Disabled ▾
Blocked IP Address Re-Use Timer (secs)	5 *
ICMP Echo	Disabled ▾
DHCP Next Server	0.0.0.0
Apply	

Note : To enable *DHCP Server*, *DHCP Relay Status* should be disabled.

Screen Objective	This screen allows the user to configure the basic <i>DHCP</i> settings.
NOTE: To enable <i>DHCP Server</i> , <i>DHCP Relay Status</i> should be disabled.	
Navigation	Layer 3 Management > DHCP Server > Basic Settings
Fields	DHCP Server—select the <i>DHCP</i> server status in the router. The default option is Disabled. The list contains: - Enabled—enables the <i>DHCP</i> server in the router and starts serving the server with the IP addresses. It opens the UDP socket and starts listening for <i>DHCP</i> discover messages from clients. - Disabled—disables the <i>DHCP</i> server in the router. NOTE: The <i>DHCP</i> server can be set as Enabled, only if the <i>DHCP Relay</i> is set as Disabled using Layer 3 Management > DHCP Relay > Basic Settings > DHCP Relay Basic Settings screen. Blocked IP Address Re-Use Timer (secs)—enter the reuse timeout value used by <i>DHCP</i> in seconds. It denotes the amount of time the <i>DHCP</i> server entity waits for a DHCP REQUEST from a client, before reusing the offer (i.e. the blocked IP address). An value zero disables this timer. This value ranges from 1 to 120 seconds. The default value is 5 seconds. ICMP Echo—select the status of <i>ICMP</i> (Internet Control Message Protocol) Echo feature for the <i>DHCP</i> server. This object controls the server to probe for the IP address before allocating the IP address to a client through the <i>ICMP</i> echo message. The default option is Disabled. The list contains:

Fields (cont)	• ICMP Echo—the list contains (cont.): – Enabled—enables the <i>ICMP</i> Echo feature. Before allocating an IP Address to client, the server broadcasts <i>ICMP</i> Echo Request (Ping Packet) to check whether any other machine/host is using this IP. If there is no response received, the server allocates the IP to the client. – Disabled—disables the <i>ICMP</i> Echo feature. The <i>ICMP</i> Echo Request packet mechanism is not used. The IP is directly allocated to the client. • DHCP Next Server—select the IP address of the boot server (<i>TFTP</i> server) from which the initial boot file is to be loaded in a <i>DHCP</i> client. This boot server acts as a secondary server. The default address is 0.0.0.0 (No boot server is defined). The <i>DHCP</i> server is used as a boot server.
Buttons	• Apply—modifies attributes and saves the changes.

DHCP Pool Settings

Figure 2: DHCP Pool Settings

DHCP Pool Settings

Pool ID		*
Pool Name		*
Subnet Pool		*
Network Mask		*
Start IP Address		*
End IP Address		*
Lease Time (Secs)		
Utilization Threshold		
Add Reset		

Select	Pool ID	Pool Name	Subnet Pool	Network Mask	Start IP Address	End IP Address	Lease Time (secs)	Threshold	Status
Apply Delete									

Screen Objective	This screen allows the user to configure a <i>DHCP</i> address pool. A <i>DHCP</i> address pool is used by the servers to allocate IP addresses to clients.
Navigation	Layer 3 Management > DHCP Server > Pool Settings

Fields	• Select—click to choose a Pool ID for which the configuration needs to be modified or deleted. • Pool ID—enter the Pool ID. This is a unique index for any subnet pool. This value ranges from 1 to 2147483647. • Pool Name—enter the pool name to identify the subnet pool. This is a string of maximum size 64. • Subnet Pool—enter the subnet of the IP address in the pool. • Network Mask—enter the Network Mask. It denotes the client's subnet mask of the IP address in the pool. • Start IP Address—enter the first IP address in the address pool that is used for dynamic allocation by the <i>DHCP</i> server. This specifies the lower limit for IP address in an address pool. NOTE: Start IP Address should have same network of the subnet pools. • End IP Address—enter the last IP address in the address pool that is used for dynamic allocation by the <i>DHCP</i> server. This specifies the upper limit for IP address in an address pool. NOTE: Start IP Address should have same network of the subnet pools. • Lease Time (Secs)—enter the time interval for which the IP address is valid. This specifies the amount of time that the client can use the IP address assigned by the server and is specific to each IP address pool. Every IP address allocated from a pool will be returned to the pool if the client does not renew it. This value ranges from 60 to 2147483647 seconds. The default value is 3600. • Utilization threshold / Threshold—enter the <i>DHCP</i> pool utilization threshold value in percentage. This specifies the upper limit for the address pool utilization, after which a notification will be sent to <i>SNMP</i> Manager. This value ranges from 0 to 100 in percentage. The default value is 75. • Status—select the status of the entry. It denotes the status of address pool configuration and allocation of IP address. Options are. – UP—configures the address pool successfully for allocating IP address. – Down—does not configure address pool for allocating IP address
Buttons	• Create—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

DHCP Pool Option Settings

Figure 3: DHCP Pool Option Settings

DHCP Pool Option Settings

Pool Name

Option

Option Code

Option Value

Option Value 2

Add Reset

Select	Pool Name	Option Code	Option Name	Option Value
Apply Delete				

Screen Objective	This screen allows the user to configure a <i>DHCP</i> address pool. A <i>DHCP</i> address pool is used by the servers to allocate IP addresses to clients.
Navigation	Layer 3 Management > DHCP Server > Pool Options
Fields	Select—click to choose a Pool Name for the configuration to be modified/deleted. Pool Name—select a Pool Name from the list of Address Pools created in the system for which <i>DHCP</i> Pool Options a configuration needs to be applied. NOTE: This field lists the pool names created in <i>DHCP</i> Pool settings screen Option / Option Name—select the <i>DHCP</i> pool option to be set to the selected pool name. The default option is NetMask (IP Format). NOTE: Refer Appendix A for the items in the list and their description Option Code—displays the corresponding DHCP Option Code for the <i>DHCP</i> option selected in the field Option. The Option Code represents a specific <i>DHCP</i> option used in a DHCP OFFER message in response to a DHCP DISCOVER message. The default is 1 - the default Netmask (IP Format). NOTE: Refer Appendix A for the items in the list and their description. <i>This field is configurable if the option is selected as "Enter Option Code Manually"</i> Option Value—enter the value to be set for the <i>DHCP</i> option selected in the field Option. This value can be an ASCII string, hexadecimal string or unicast IP address based on the <i>DHCP</i> pool option. Option Value 2—enter the value to be set for the <i>DHCP</i> option selected in the field Option. This value can be an ASCII string, hexadecimal string or unicast IP address based on the <i>DHCP</i> pool option. NOTE: This field is enabled only when the Option/Option Name is set as Network Time Protocol server (IP Format), <i>SIP</i> Server IP Format, and <i>SIP</i> Server Domain name.

Buttons	• ADD—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

DHCP Server IP Exclude Settings

Figure 4: DHCP Server IP Exclude Settings

DHCP Server IP Exclude Settings

The screenshot shows the 'DHCP Server IP Exclude Settings' interface. It consists of two main parts. The top part is a configuration area with three text input fields labeled 'Pool ID', 'Start IP Address', and 'End IP Address', each followed by an asterisk (*). Below these fields are two buttons: 'Add' and 'Reset'. The bottom part is a table with four columns: 'Select', 'PoolID', 'Start IP Address', and 'End IP Address'. Below the table are two buttons: 'Apply' and 'Delete'.

Screen Objective	This screen allows the user to configure a <i>DHCP</i> address pool. A <i>DHCP</i> address pool is used by the servers to allocate IP addresses to clients.
Navigation	Layer 3 Management > DHCP Server > Exclude List
Fields	• Select—click to choose a Pool ID for the configuration to be reapplied. • Pool ID—click to select Pool ID for which the configuration needs to be re-applied. NOTE: Pool ID should be created using the <i>DHCP</i> Pool Settings screen prior to configuring the exclude list. • Start IP address—enter the start IP address for the Exclude List. This address denotes the first IP address of a range of IP addresses which needs to be excluded from the created subnet pool. NOTE: This IP address should be: – lower than the end IP address of the Exclude List, and – In the same network of the subnet pool start IP address. • End IP address—enter the end IP address for the Exclude List. This address denotes the first IP address of a range of IP addresses which needs to be excluded from the created subnet pool. NOTE: This IP address should be: – higher than the end IP address of the Exclude List, and – In the same network of the subnet pool start IP address.

Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

DHCP Host IP Settings

Figure 5: DHCP Host IP Settings

DHCP Host IP Settings

Host MAC Address *
 Pool Name v*
 Host IP *

Select	Host MAC Address	Pool Name	Host IP
☒	HOST_MAC_KEY	POOL_INDEX_	HOST_IP_KEY
Apply Reset IP Delete			

Screen Objective	This screen allows the user to configure the Host IP Settings.
Navigation	Layer 3 Management > DHCP Server > Host Settings
Fields	• Select—click to choose a Pool ID for the configuration to be reapplied. • Host MAC Address—enter the unicast MAC address for configuring the DHCP host. • Pool Name—select a Pool Name from the list of Address Pools created in the system for which DHCP host IP related configuration needs to be applied. NOTE: This field lists the pool names created in <i>DHCP</i> Pool settings (Layer 3 Management > DHCP Server > Pool Settings) screen. • Host IP—enter the IP address for configuring of the DHCP host.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

DHCP Host Options Settings

Figure 6: DHCP Host Options Settings

DHCP Host Option Settings

Host MAC Address

Pool Name

▼

Option

NetMask (IP Format) ▼

Option Code

1

Option Value

Option Value 2

Add Reset

Select	Host MAC Address	Pool Name	Option Code	Option Name	Option Value
Apply Delete					

Screen Objective	This screen allows the user to configure the Host IP Options.
Navigation	Layer 3 Management > DHCP Server > Host Options
Fields	Select—click to select Host MAC address for which the configuration is re-applied. Host MAC Address—enter Unicast MAC address for configuring the <i>DHCP</i> host. Pool Name—select a Pool Name from the list for which <i>DHCP</i> host IP related configuration needs to be applied. NOTE: Refer to Appendix A for the items in the list and their descriptions. Option Code—displays the corresponding <i>DHCP</i> option code for the <i>DHCP</i> option selected in the field option. The option code represents that represents a specific <i>DHCP</i> option used in a DHCP OFFER message in response to a DHCP DISCOVER message. The default is 1 (the code for the default option—Netmask (IP Format)). NOTE: Refer to Appendix A for details about option code and its corresponding <i>DHCP</i> option.This field is configurable if the option is selected as “Enter Option Code Manually”. Option Value—enter the value to be set for the <i>DHCP</i> option selected in the field option. This value can be an ASCII string, hexadecimal string, or unicast IP address based on the DHCP pool option. Option Value 2—enter the value to be set for the specified <i>DHCP</i> option. This value can be an ASCII string, hexadecimal string, or unicast IP address based on the <i>DHCP</i> pool option. NOTE: This field is enabled only when the Option/Option Name is set as Network Time Protocol server (IP Format), SIP Server IP Format and SIP Server Domain name.

Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

DHCP Bootfile Configuration

Figure 7: DHCP Bootfile Configuration

DHCP BOOTFILE CONFIGURATION

Screen Objective	This screen allows the user to configure the name of the initial boot file to be loaded in a <i>DHCP</i> client.
Navigation	Layer 3 Management > DHCP Server > Bootfile Configuration
Fields	• Enter the bootfile name—enter the name of the initial boot file to be loaded in a <i>DHCP</i> client. This value is a string of maximum size 64. The boot file contains the boot image that is used as the operating system for the <i>DHCP</i> client. NOTE: Only characters and numbers are accepted in the bootfile name string.
Buttons	• Apply—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user input.

19.2. DHCP Relay

This section describes how to configure the Dynamic Host Configuration Protocol Relay on the switch.

DHCP Relay (Dynamic Host Configuration Protocol 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.

DHCP Relay agent is used to forward *DHCP* packets between client and server when they are not in the same subnets. The relay receives packets from the client and inserts certain information such as network from which the packet is removed and then forwards it to the server. The server identifies the client's network from this information and allocates IP accordingly, then sends the reply to the relay. The relay strips the information inserted and broadcasts the packets into the client's network.

To access **DHCP Relay** screens, go to **Layer 3 Management > DHCP Relay**.

The **DHCP Relay** related parameters are configured through the screens displayed by the following tabs:

[DHCP Relay Configuration](#)

DHCP Relay Interface Configuration

DHCP Relay Configuration

By default, the tab **Basic Settings** displays the **DHCP Relay Configuration** screen.

Figure 8: DHCP Relay Configuration

DHCP Relay Configuration

Service DHCP-Relay

Enabled

IP DHCP Relay Information Option

Enabled

Apply

Note : To enable DHCP Relay, DHCP Server Status should be disabled.

DHCP Server Address

Add

Select

Server Address

Delete

Screen Objective	This screen allows the user to configure the basic <i>DHCP</i> Relay information.
NOTE: To enable <i>DHCP</i> Relay, <i>DHCP</i> Server Status should be disabled.	
Navigation	Layer 3 Management > DHCP Server > Basic Settings

Fields	• Select—select the interface for which configuration need to be applied or deleted. • Service DHCP-Relay—select the Service <i>DHCP</i> relay status in the switch. The default option is Disabled. The list contains: – Enabled—enables the <i>DHCP</i> relay service i.e. Relay Agent becomes active in the switch. <i>DHCP</i> relay agent relays <i>DHCP</i> messages between <i>DHCP</i> client and <i>DHCP</i> server located in different subnets. – Disabled—disables the <i>DHCP</i> relay service in the switch NOTE: The service <i>DHCP</i> relay can be set as Enabled, only if the <i>DHCP</i> Server is set as Disabled. • IP DHCP Relay Information Option—select the Service <i>DHCP</i> relay status in the switch. The default option is Disabled. The list contains: – Enabled—enables the controlling status of the processing related to the Relay Agent Information options for inserting the necessary information while relaying a packet from a client to a server and examining/stripping of the inserted information when relaying a packet from a server to a client. – Disabled—disables the controlling status of the processing related to the Relay Agent Information options • Server Address—displays the IP address of the <i>DHCP</i> Server to which the Relay Agent needs to forward the packets from the client. A maximum of 5 servers can be configured. If no servers are configured, the <i>DHCP</i> packets will be broadcast to entire network, except the network from which packet was received.
Buttons	• Apply—modifies attributes and saves the changes. • Add—adds and saves new configuration. • Delete—deletes the selected entry.

DHCP Relay Interface Configuration

Figure 9: DHCP Relay Interface Configuration

DHCP Relay Interface Configuration

Interface: vlan1 ▼*

Circuit ID:

Remote ID:

Add Reset

Select	Interface	Circuit ID	Remote ID

Screen Objective	This screen allows the user to configure a <i>DHCP</i> address pool. A <i>DHCP</i> address pool is used by the servers to allocate IP addresses to clients.
Navigation	Layer 3 Management > DHCP Server > Interface Settings

Fields	• Select—select the interface for which configuration need to be applied or deleted. • Interface—select the <i>VLAN</i> Interface which is already created in the system. NOTE: <i>VLAN</i> interface can be created using Layer 2 Management > VLAN > Static VLANs screen. • Circuit ID—enter the Circuit ID value for an interface. The circuit ID uniquely identifies a circuit over which the incoming <i>DHCP</i> packet is received. In <i>DHCP</i> relay, it is used to identify the correct circuit over which the <i>DHCP</i> responses should be relayed. The configured circuit ID is used in the <i>DHCP</i> relay agent information option to inform the <i>DHCP</i> server about the interface from which a <i>DHCP</i> packet is received. The minimum value depends upon the number of interfaces that can be created. For example, if a total of 160 interfaces are allowed to be created in the switch, the circuit ID value range starts from 161 only. The interfaces include all physical interfaces, port channels, and logical L3 interfaces. This value ranges from 1 to 2147483647. NOTE: String of length zero will reset the configuration. • Remote ID—enter the Remote ID value for an interface. The configured remote ID is used to inform the <i>DHCP</i> client about the remote circuit to which the <i>DHCP</i> packets should be forwarded from the interface. The remote ID is globally unique and an octet string of maximum size of 32. NOTE: The remote ID should not be same as that of the default value. NOTE: String of length zero will reset the configuration.
Buttons	• Create—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

19.3. DHCP Client

This section describes how to configure the Dynamic Host Configuration Protocol Client on the switch.

DHCP Client (Dynamic Host Configuration Protocol Client) client uses *DHCP* to temporarily receive a unique IP address for it from the *DHCP* server. It also receives other network configuration information, such as default gateway, from the *DHCP* server.

To access **DHCP Client** screens, go to **Layer 3 Management > DHCP Client**.

The **DHCP Client** related parameters are configured through the screens displayed by the following tabs:

[DHCP Option Type Settings](#)

[DHCP Client Identifier Setting](#)

Enabling DHCP Client

By default, the tab DHCP Option Type displays the **DHCP Option Types Settings** screen.

Figure 10: DHCP Client Global Configuration

DHCP Client Global Configuration

Screen Objective	This screen allows the user to enable the <i>DHCP</i> Client functionality.
Navigation	Layer 3 Management > DHCP Client > Global Configuration
Fields	Global Status—select either enabled or disabled.
Buttons	Apply—modifies attributes and saves the changes.

DHCP Option Type Settings

Figure 11: DHCP Option Type Settings

DHCP Relay Interface Configuration

Select	Interface	Circuit ID	Remote ID

Screen Objective	This screen allows the user to configure basic <i>DHCP</i> Relay information.
NOTE: To enable <i>DHCP</i> Relay, <i>DHCP</i> Server Status should be disabled.	

Navigation	Layer 3 Management > DHCP Server > DHCP Option Type
Fields	• Select—click to select an interface for which <i>DHCP</i> option type configuration needs to be modified or deleted. • Interface Name—select an interface for which <i>DHCP</i> option type settings to be configured from the list of <i>VLAN</i> interfaces already created in the system.

Fields	• Option Type/ DHCP Option Type—select the <i>DHCP</i> Client Option Type for the specified interface created in the system. The list contains: – <i>TFTP</i> Server Name (IP Format/String)—sends the <i>TFTP</i> requests to get the <i>TFTP</i> server's domain name – Bootfile Name (String)—sends the <i>DHCP</i> requests to get the boot File Name. – Vendor Specific (String)—sends the <i>DHCP</i> requests to get the Vendor Specific details. – <i>NTP</i> Servers (IP Format)—sends the <i>DHCP</i> requests to get the <i>NTP</i> server IP. – <i>DNS</i> Servers (IP Format)—sends the <i>DHCP</i> requests to get the <i>DNS</i> server IP. – <i>SIP</i> Servers (IP Format/String)—sends the <i>DHCP</i> requests to get the <i>SIP</i> server information. – Option 240—sends the <i>DHCP</i> requests to get the Option 240 information. • Option Code/DHCP Option Code—displays the Option code for the specified interface created in the system. When option code is displayed as: – 66—indicates <i>TFTP</i> Server Name (IP Format/String) is set. This allows to identify a <i>TFTP</i> server when the same field in the <i>DHCP</i> header is used for <i>DHCP</i> options – 67—indicates Bootfile Name (String) is set. This allows identifying a bootfile when the file field in the <i>DHCP</i> header is used for <i>DHCP</i> options. – 0—indicates no option type is set for the interface – 60—indicates Vendor Specific (String) is set. This allows identifying a vendor specific when the file field in the <i>DHCP</i> header is used for <i>DHCP</i> options. – 42—indicates <i>NTP</i> Servers (IP Format) is set. This allows identifying <i>NTP</i> Servers when the file field in the <i>DHCP</i> header is used for <i>DHCP</i> options. – 6—indicates <i>DNS</i> Servers (IP Format) is set. This allows identifying a <i>DNS</i> Servers when the file field in the <i>DHCP</i> header is used for <i>DHCP</i> options. – 120—indicates <i>SIP</i> Servers (IP Format/String) is set. This allows identifying <i>SIP</i> Servers when the file field in the <i>DHCP</i> header is used for <i>DHCP</i> options. – 240—indicates Option 240 is set. This allows identifying Option 240 when the file field in the <i>DHCP</i> header is used for <i>DHCP</i> options. – 0—indicates no option type is set for the interface. • Option Value/DHCP Option Value—enter an value to identify the octets of data, of length specified by length for that entry. This value will be taken from <i>DHCP</i> ACK message which is sent from server to client. NOTE: This field is enabled only when <i>DHCP</i> Option Type is set as Vendor Specific (String).
Buttons	• Create—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

DHCP Client Identifier Setting

Figure 12: DHCP Client Identifier Setting

Client Identifier Setting

Select	Interface Name	Dhcp Client Identifier

Screen Objective	This screen allows the user to configure <i>DHCP</i> client identifiers for the interfaces created in the system. The client identifier is advertised in the <i>DHCP</i> control packets.
Navigation	Layer 3 Management > DHCP Server > DHCP Client ID
Fields	• Select—select the interface for which configuration need to be applied or deleted. • Interface Name—select an interface for which <i>DHCP</i> option type settings need to be configured from the list of VLAN interfaces already created in the system. • Client Identifier—enter the unique identifier of <i>DHCP</i> client for the specified interface created in the system. Client ID is used in all <i>DHCP</i> client messages. This identifier will be used in <i>DHCP</i> server to maintain client information. This identifier can be mac address or any string NOTE: String of length zero will reset the configuration. • Remote ID—enter the Remote ID value for an interface. The configured remote ID is used to inform the <i>DHCP</i> client about the remote circuit to which the <i>DHCP</i> packets should be forwarded from the interface. The remote ID is globally unique and an octet string of maximum size of 32. NOTE: Set Get IP Address Mode as <i>DHCP</i> using the link Layer 3 Management > IP > IPv4 Address Configuration to access Get IP Address Mode screen NOTE: VLAN 1 should not be used as it is used to connect web session. If in case VLAN 1 is used, connectivity to the web will be lost.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input.

Routing Map

20. Routing

This section contains the routing protocols supported in the Web User Interface.

20.1. RIP

This section describes the Routing Information Protocol (*RIP*) on the switch.

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 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.

To access **RIP** screens, go to **Layer 3 Management > RIP**.

The **RIP** link allows the user to configure the *RIP* through the following tabs:

[RIP VRF Creation](#)

[RIP Basic Settings](#)

[RIP Interface](#)

[RIP Neighbour List](#)

[RIP Security Settings](#)

[RIP Interface Specific Address Summarization](#)

RIP VRF Creation

By default, the tab **Basic Settings** displays the **DHCP Relay Configuration** screen.

Figure 1: RIP VRF Creation**RIP VRF Creation**

VRF Name	
VRF Status	
Add	Delete

VRF Name	VRF Status
default	Disabled

Screen Objective	This screen allows the user to enable or disable <i>RIP</i> for default <i>VRF</i> (Virtual Routing and Forwarding) instance.
Navigation	Layer 3 Management > RIP > RIP VRF Creation
Fields	• VRF Name—default is available for a <i>VRF</i> context name for which <i>RIP</i> has to be enabled or disabled. <i>VRF</i> allows multiple instances of a routing table to co-exist within the same router at the same time. • VRF Status—select the <i>VRF</i> status in the router. The default option is Disabled. The list contains: – Disabled—disables <i>RIP</i> on the <i>VRF</i> instance. – Enabled—enables <i>RIP</i> on the <i>VRF</i> instance to allow multiple instances of a routing table
Buttons	• Add—adds and saves new configuration. • Delete—deletes the selected entry.

RIP Basic Settings**Figure 2:** RIP Basic Settings**RIP Basic Settings**

Select	Context Id	Context Name	Security	Output Delay	Trusted Neighbour Feature	Auto-Summary Status	Retransmission Timeout Interval	Maximum Retransmissions	Distance
☒	0	default	Maximum	Disabled	Disabled	Enabled	5	36	121

Screen Objective	This screen allows the user to configure the basic settings of <i>RIP</i> .
Navigation	Layer 3 Management > RIP > Basic Settings

Fields	• Select—click to select the Context ID for which the <i>RIP</i> configuration is modified. • Context ID—default. • Context Name—displays the Context name for the <i>VRF</i> instance. This value represents unique name of the <i>VRF</i> instance and is a string of maximum size of 32. • Security—select the security level of <i>RIP</i> to accept / ignore <i>RIPv1</i> packets when authentication is in use. The default option is Maximum. The list contains: – Minimum—sets the security status for the <i>RIP</i> domain context as minimum. When minimum security is set, the <i>RIP</i> packets will be accepted even when authentication is in use. – Maximum—sets the security status for the <i>RIP</i> domain context as maximum. When maximum security is set, <i>RIP</i> packets will be ignored when authentication is in use.

Fields (cont)	• OutputDelay—select Output Delay status for the <i>RIP</i> Domain Context. The default option is Disabled. The list contains: – Enabled—sets Output Delay status as Enabled and enables interpacket delay for RIP updates, where the delay between packets in a multiple-packet RIP update is in milliseconds. This interpacket delay feature helps in preventing the routing table from losing information due to flow of <i>RIP</i> update from high speed router to low speed router. – Disabled—sets Output delay status in the <i>RIP</i> Domain context as Disabled; thereby, disabling interpacket delay for <i>RIP</i> packets. • Trusted Neighbour Feature—select Trusted Neighbour Feature for the RIP domain context. The default option is Enabled. The list contains: – Enabled—sets the Trusted Neighbour Feature status as Enabled. When Enabled, a list of routers' IP addresses can be configured. <i>RIP</i> Packets from those routers will be processed by <i>RIP</i>, and packets from other routers will be dropped. – Disabled—sets the Trusted Neighbour Feature status as Disabled. When Disabled, <i>RIP</i> Packets from all routers will be processed. • Auto-Summary Status—select the Auto Summary status for the <i>RIP</i> domain context. The default option is Enabled. The list contains: – Enabled—sets the Auto Summary Status for the <i>RIP</i> domain context as Enabled. When Enabled, summary routes are sent in regular updates for both <i>RIP</i> version 1 and version 2. The summary is sent only if at least one subnet route, which is different from the interface over which the update is sent, is learned over an interface. – Disabled—sets the Auto Summary Status for the <i>RIP</i> domain context as Disabled. When Disabled, either individual subnet route is sent, or subnet routes are sent based on the specific aggregation configured over the interface. • Retransmission Timeout Interval—enter 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 number of retries is reached. The value ranges from 5 to 10. The default value is 5. • Maximum Retransmissions—enter the maximum number of retransmissions of the update request and update response packets. If no response is received. the routes via the next hop router are marked unreachable. This value ranges from 10 to 40 seconds. The default value is 36. • Distance—enter the distance value for the specified context id. This value ranges from 1 to 255. The default value is 121.
Buttons	• Apply—modifies attributes and saves the changes.

RIP Interface

Figure 3: RIP Interface

RIP Interface

Context Id *
 Interface *

Select	Context ID	IP Address	Status	Split Horizon	Default Route Installation	Send Version
☒	0	192.168.10.1	Enabled ▾	Poisson Reverse ▾	No ▾	RIP1 Compatible ▾

Receive Version	Route Age Timer	Update Timer	Garbage Timer	Rip Default Originate
RIP1 or RIP2 ▾	180	30	120	0

Screen Objective	This screen allows the user to configure <i>RIP</i> on the specified interface.
Navigation	Layer 3 Management > RIP > Interface Configuration
Fields	Select—click to select the Context ID for which the configuration needs to be modified or deleted. Context ID—default. Interface—select the interface ID for which the <i>RIP</i> parameters need to be configured. NOTE: The <i>VLAN</i> interface can be created in Layer 2 Management->VLAN screen IP Address—displays the IP Address of the <i>RIP</i> interface. This is a read-only field. Status—select the administrative status of the <i>RIP2</i> in the router. The default option is Enabled. The list contains: - Enabled—activates <i>RIP2</i> process throughout the system. - Disabled—disables <i>RIP2</i> process in the system. - Passive—runs <i>RIP2</i> process as a passive one. Split Horizon—select the operational status of split horizon in the system. The default option is Poison Reverse. The list contains: - Split Horizon—enables the Split Horizon updates for the <i>RIP</i> which prevents the routing loops in distance routing protocol. This is done by prohibiting the router from advertising a route back onto the interface. The Split Horizon updates are applied in the response packets sent.

Fields (cont)	• Split Horizon—the list contains (cont): – Poisson Reverse—enables the poison updates for the <i>RIP</i> which sends route with the metric value 16 on an interface from which route is learnt. – Disabled—disables Split Horizon updates for the <i>RIP</i> which sends route on all interfaces with the metric same as that in the <i>RIP</i> Routing Table. • Default Route Installation—select the default route installation status in the <i>RIP</i> Interface. The default option is No. The list contains: – Yes—enables default route installation which installs the default route received in updates to the <i>RIP</i> database. – No—disables default route installation which blocks the installation of default route received in updates to the <i>RIP</i> database. • Send Version—select the version of <i>RIP</i> packets that will be sent by the router. The default option is <i>RIP1</i> Compatible. The list contains: – Do not send—stops the IP <i>RIP</i> transmitting advertisements to be sent on a VLAN interface / router port – <i>RIP</i> Version1 sends only <i>RIP</i> updates compliant with RFC 1058. – <i>RIP1</i> Compatible—sends both Multicasting <i>RIP</i> updates and <i>RIP</i> updates compliant with RFC 1058 on the interface. – <i>RIP</i> Version2—sends only Multicasting <i>RIP</i> updates on the interface • Receive Version—select the version of <i>RIP</i> updates to be received. The default option is <i>RIP1</i> or <i>RIP2</i>. The list contains: – <i>RIP1</i>—receives only <i>RIP</i> updates compliant with RFC 1058 on the interface. – <i>RIP2</i>—receives only multicasting <i>RIP</i> updates on the interface. – <i>RIP1</i> or <i>RIP2</i>—receives both multicasting <i>RIP</i> updates and <i>RIP</i> updates compliant with RFC 1058 on the interface. – Do not receive—sets that no IP <i>RIP</i> transmitting advertisements are received on a VLAN interface / router port. • Route Age Timer—enter the time (in sec) after which the route entry goes in garbage collect (marked as invalid). The value is from 30 to 500 sec—default 180. • Update Timer—enter the time interval (in seconds) at which the <i>RIP</i> updates should be sent. This is the fundamental timing parameter of the routing protocol. The value ranges from 10 to 3600 seconds. The default value is 30. • Garbage Timer—enter the time (in seconds) after which the route entry marked as invalid is deleted. The advertisement of this entry is set to INFINITY while sending to others. The value ranges from 120 to 180 seconds with a default of 120. • Rip Default Originate—enter the metric to be used for default route propagated over the VLAN interface / router port in a <i>RIP</i> update message and generates a default route into <i>RIP</i>. This value ranges from 0 to 15. The default option is 0 which implies that origination of default route over the interface is disabled.
Buttons	• Apply—modifies attributes and saves the changes.

RIP Neighbour List

Figure 4: RIP Neighbour List

RIP Neighbour List

Context Id

default ▾*

IP Address

Add

Reset

Select

Context Id

IP Address

Delete

Screen Objective	This screen allows the user to add a trusted neighbor router with which routing information can be exchanged and from which <i>RIP</i> packets can be accepted. This permits the point-to-point (non broadcast) exchange of routing information. When used in combination with the passive-interface <i>VLAN</i> , routing information can be exchanged between a subset of routers and access servers. On a LAN, multiple neighbor IP addresses can be used to specify additional neighbors or peers.
Navigation	Layer 3 Management > RIP > Neighbors List
Fields	Select—click to select the Context ID for which the configuration needs to be modified or deleted. Context ID—default. IP Address—enter the IP Address of the neighbor router from which this router will accept RIP packets
Buttons	Add—adds and saves new configuration. Reset—resets to default value for respective fields and discards all user input. Delete—deletes the selected entry.

RIP Security Settings

Figure 5: RIP Security Settings

RIP Security Settings

Context Id
 Interface Address
 Authentication Type
 Authentication Key
 Authentication Key ID
 Start Generate Time
 Start Accept Time
 Stop Generate Time
 Stop Accept Time

Select	Context	IP Address	Authentication Type	Authentication Key	Authentication Key ID	Start Generate Time	Start Accept Time	Stop Generate Time	Stop Accept Time
☒	0	192.168.10.1	Simple Password		0				

RIP Security Settings

Context Id
 Interface Address
 Authentication Type
 Authentication Key
 Authentication Key ID
 Start Generate Time
 Start Accept Time
 Stop Generate Time
 Stop Accept Time

Select	Context	IP Address	Authentication Type	Authentication Key	Authentication Key ID	Start Generate Time	Start Accept Time	Stop Generate Time	Stop Accept Time
☒	0	192.168.10.1	MD5		1	2019-08-01,12:35:00	2019-08-01,12:35:00	2019-08-01,12:45:00	2019-08-01,12:45:00

Screen Objective	This screen allows the user to configure the type of authentication that is used on the interface.
Navigation	Layer 3 Management > RIP > Security Settings
Fields	Select—click to select the Context ID for which the configuration needs to be modified or deleted. Context ID—default. Interface Address—select the required interface from the list of interfaces for which crypto authentication parameters are to be configured. NOTE: The VLAN interface can be created in Layer 2 Management->VLAN screen

Fields (cont)	Authentication Type—select the type of authentication used on the interface. The default option is No Authentication. The list contains: - No Authentication—disables authentication when No Authentication is set. - Simple Password—sets the authentication type as simple text. - MD5—sets the authentication type as keyed <i>MD5</i> (Message Digest 5) authentication. - SHA -1—sets the authentication type as Secure Hash Algorithm 1 (<i>SHA1</i>) authentication. <i>SHA1</i> generates Authentication digest of length 20 bytes. - SHA-256—sets the authentication type as Secure Hash Algorithm 256 (<i>SHA 256</i>) authentication. <i>SHA 256</i> generates Authentication digest of length 32 bytes. - SHA-384—sets the authentication type as Secure Hash Algorithm 384 (<i>SHA384</i>) authentication. <i>SHA 384</i> generates Authentication digest of length 48 bytes. - SHA- 512—sets the authentication type as Secure Hash Algorithm 512 (<i>SHA512</i>) authentication. <i>SHA512</i> generates Authentication digest of length 64 bytes. Authentication Key—enter the key—value to be used as the authentication key. This value is a string with a size of 16 octets 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). NOTE: This field is greyed out if the Authentication type is selected as No Authentication. Authentication Key ID—enter the active authentication KeyID currently used in the particular interface for sending RIP updates. This value ranges from 0 to 255. NOTE: This field is greyed out if the Authentication type is selected as No Authentication or Simple Password. Start Generate Time—enter the time that the router will start using this key for packet generation. If the value is not set, then it will be taken as infinite and displayed as 2136–02–06, 06:28:15. For example, Tuesday May 26, 1992 at 1:30:15 PM should be configured as 1992–5-26, 13:30:15.0. . NOTE: This field is greyed out if the Authentication type is selected as No Authentication or Simple Password. Start Accept Time—enter the time that the router will start accepting packets that have been created with this key. If the value is not set, then it will be taken as infinite and displayed as 2136–02–06, 06:28:15. For example, Tuesday May 26, 1992 at 1:30:15 PM should be entered as, 1992–5-26, 13:30:15. NOTE: This field is greyed out if the Authentication type is selected as No Authentication or Simple Password.

Fields (cont)	• Stop Generate Time—enter the time that the router will stop using this key for packets generation. If the value is not set, then it will be taken as infinite and displayed as 2136–02–06, 06:28:15. For example, Tuesday May 26, 1992 at 1:30:15 PM should be configured as, 1992–5–26, 13:30:15.0. Stop Generate Time should be later than the Start Generate Time. NOTE: This field is greyed out if the Authentication type is selected as No Authentication or Simple Password. • Stop Accept Time—enter the time when the router will stop accepting packets that have been created with this key. If the value is not set, it will be taken as infinite and displayed as 2136–02–06, 06:28:15. For example, Tuesday May 26, 1992 at 1:30:15 PM should be configured as 1992–5–26, 13:30:15.0. Stop Accept Time should be later than the Start Accept Time. NOTE: This field is greyed out if the Authentication type is selected as No Authentication or Simple Password.
Buttons	• Create—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

RIP Interface Specific Address Summarization

Figure 6: RIP Interface Specific Address Summarization

RIP Interface Specific Address Summarization

Context Id *

Interface *

Aggregate Address *

Subnet Mask *

Select	Context Id	Interface	Aggregate Address	Subnet Mask
Delete				

Screen Objective	This screen allows the user to set route aggregation over a <i>VLAN</i> interface / router port for all subnet routes that fall under the specified IP address and mask.
Navigation	Layer 3 Management > RIP > Address Summary

Fields	• Select—click to select the Context ID for which summary address is to be deleted. • Context ID—default. • Interface—select the Interface ID from the list of <i>VLAN</i> interfaces created in the system to configure the summary address. • Aggregate Address—enter 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. • Subnet Mask—enter 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.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Delete—deletes the selected entry.

20.2. Route Map

Route Map may be used for policy based routing and route redistribution on the switch.

Route Map table contains route map name, sequence number, and access status (Permit/Deny). Route maps can be used in policy based routing and route redistribution.

Route Map provides a set of rules which should be satisfied for a route to be redistributed from one routing domain to another. When a route is to be redistributed from a routing domain to another, it is checked against a set of match conditions. If the match conditions are satisfied, access control of Permit/Deny is provided to the route. Route Map permits modifying of route information during redistribution and setting conditions using the match clause and sets actions using the set clause.

To access **Route Map** screens, go to **Layer 3 Management > Route Map**.

The Route Map related parameters are configured through the screens displayed by the following tabs:

[Route Map Creation](#)

[Route Map Match](#)

[Route Map Set](#)

[IP Prefix List](#)

Route Map Creation

By default, the tab **Route Map Creation** displays the **Route Map Creation** screen.

Figure 7: Route Map Creation

Route Map Creation

Route Map Name *
 Route Map Sequence Number *
 Route Map Access Permit ▾

Add
Reset

Select	Route Map Name	Sequence Number	Access
Apply Delete			

Screen Objective	This screen allows the user to create Route Map which can be used in policy based routing and route redistribution.
Navigation	Layer 3 Management > Route Map > Route Map Creation
Fields	• Route Map Name—enter the Route Map Name to identify the specified Route Map from the list of route maps. The value is a string of maximum size 20. • Route Map Sequence Number—enter the number that indicates position of a new route map in the list of route maps already configured with the same name. This value range is from 1 to 10. The default value is 1.
Fields	• Route Map Access—select the access type associated with the sequence number in a route map. Once an instance of this object is created, its value cannot be changed. The default option is Permit. Options are: – Permit—sets the access type associated with sequence number in a route map as Permit. This permits matching of route entry with entry rules. – Deny—sets the access type associated with sequence number in a route-map as Deny. This denies the route entry to match entry rules.
Buttons	• Create—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

Route Map Match

Figure 8: Route Map Match

Route Map Match

Route Map Name

Sequence Number

Destination Address Type

N/A

Match Destination Address

Destination Address Prefix

0

Source Address Type

N/A

Match Source Address

Source Address Prefix

0

Next Hop Type

N/A

Match Next Hop Address

Match Interface

loopback5

Match Metric

Match Tag

Match Metric Type

N/A

Match Route Type

N/A

Match AS Path Tag

Match Community

N/A

Match Local Preference

Match Origin

Add

Reset

Select	Route Map Name	Sequence Number	Destination Address Type	Match Destination Address	Destination Address Prefix	Source Address Type	Match Source Address	Source Address Prefix
☒	Route1	1	N/A		0	N/A		0
Delete								

Next Hop Type	Match Next Hop Address	Match Interface	Match Metric	Match Tag	Match Metric Type	Match Route Type	Match AS Path Tag	Match Community	Match Local Preference	Match Origin
N/A		vlan1	0	0	N/A	N/A	0	N/A	0	N/A

Screen Objective

This screen allows the user to match the Route Map from the list of route maps.

NOTE:

This screen can be configured only if Route Map is created using the Route Map Creation screen (Layer 3 Management > Route Map > Route Map Creation)

Navigation

Layer 3 Management > Route Map > Route Map Match

Fields	• Route Map Name—specify Route Map from the list of route maps. NOTE: The route map is created using the Route Map Creation screen. • Sequence Number—select a position of a new route map in the list of route maps already configured with the same name. The value is a string of maximum size 10. NOTE: The sequence number is created using Route Map Creation screen. • Destination Address Type—select the type of destination network IP address. Options are: – N/A—no destination network IP address selected – IPv4—sets the destination network IP address as IPv4 – IPV6—sets the destination network IP address as IPV6 • Match Destination Address—enter the destination network IP address that fits the permitted range of addresses. The destination IP address provides the range of addresses that will get to pass the route map, when logically ANDed with the mask. • Destination Address Prefix—enter the prefix length of network IP address of destination network. This value ranges from 0 to 128. • Source Address Type—select the type of source network IP address. Options are: – N/A—specifies not applicable i.e. no source network IP address is selected – IPv4—sets the source network IP address as IPv4 – IPV6—sets the source network IP address as IPV6 • Match Source Address—enter the source network IP address that matches the permitted range of addresses. • Source Address Prefix—enter the prefix length of network IP address of source network. This value ranges from 0 to 128. • Next Hop Type—select the type of network IP address for next hop. Options are: – N/A— no network IP address type is selected for next hop – IPv4—sets the network IP address type of next hop as IPv4 • Match Next Hop Address—specifies the next hop router address and matches the routes having the specified address. • Match Interface—identifies local interface through which the next hop can be reached, and which matches next hop interface of the route of the specified interface. • Match Metric—enter the metric, which is matching the metric specified in the route map. The metric value ranges from 1 to 167772152147483647.

Fields (cont)	• Match Tag—enter the tag value, which is matching the tag specified in the route map. The Match Tag ranges from 1 to 2147483647. • Match Metric Type—select the Metric Type, which is matching the metric type specified in the route map. Options are: – N/A—specifies not applicable i.e. no metric type is selected. – intra-area—matches <i>OSPF</i> routes with metric type as <i>OSPF</i> inter area route metric – Inter-area—matches the <i>OSPF</i> routes with metric type as <i>OSPF</i> intra area route metric. – external-type-1—matches the <i>OSPF</i> routes with metric type as external type 1 routes. If the option external type-1 is specified as the route-type, Cost from the Router to Autonomous Border System Router (<i>ASBR</i>) + Cost from <i>ASBR</i> to Destination are included when route calculation is done for a destination. – external-type-2—matches the <i>OSPF</i> routes with metric type as external type 2 routes. If the option external type-2 is specified as the route-type, only the Cost from the Router to <i>ASBR</i> is included when route calculation is done for a destination. • Match Route Type—select the Route Type, which is matching the Route Type specified in the route map as per RFC 2096. Options are: – N/A—specifies not applicable i.e. no match route-type is selected – Local—matches route-type to the entries in route-map as local routes. – Internal—matches the route-type with the entries in route-map as remote, where the routes are matched to the non-connected routes (static/ routing protocol installed routes). • Match AS Path Tag—enter the <i>AS</i> (Autonomous System) path tag of the route which is matching the existing <i>AS</i> path in <i>BGP</i>. This match applies only when redistributing routes into <i>BGP</i>. The <i>AS</i> path tag ranges from 1 to 214748367. • Match Community—select the <i>BGP</i> communities attribute to be matched to The route in the specified community. The preference is sent only to all routers in the local autonomous system This match applies only when redistributing routes into <i>BGP</i>. Options are: – N/A—specifies not applicable i.e. no match community is selected – Internet—sets the community as Internet community. This configures and matches the <i>BGP</i> community attribute in the route as Internet where it advertises this route to the Internet community. All routers in the network belong to it.

Fields (cont)	• Match Community—options are (cont): – local-as—sets the community as local AS community. This configures and matches the <i>BGP</i> community attribute in the route as local, where it sends the route to peers in other sub autonomous systems within the local confederation. Does not advertise this route to an external system. – No-advt—sets the community as no advertisement community. This configures and matches the <i>BGP</i> community attribute in the route to no-advt, where it does not advertise all routes carrying a community attribute to other BGP peers. – No-export—sets the community as no export community. This configures and matches the <i>BGP</i> community attribute to no-export, where all routes received carrying communities attribute containing this value MUST NOT be advertised outside a <i>BGP</i> confederation boundary. – comm-num—sets the community as community number. This sets the <i>BGP</i> community number. This value ranges from 1 to 0x7ffffff (214748367). – none—sets the community as no community. This configures the <i>BGP</i> community attribute as none which implies that no community is matched. • Match Local Preference—enter preference value for the autonomous system path. The preference is sent to all routers in the local autonomous system only. The Local Preference ranges from 1 to 214748367. • Match Origin—select the option to match BGP origin code. Options are: – N/A—specifies not applicable i.e. no match origin is selected. – IGP—specifies that the route is originated through Remote Interior Gateway Protocol. – EGP—specifies that the route is originated through Local Exterior Gateway Protocol. – Incomplete—specifies that the route is originated through unknown heritage or Remote autonomous system.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

Route Map Set

Figure 9: Route Map Set

Route Map Set

Route Map Name

Sequence Number

Next Hop Type

Set Next Hop Address

Set Interface

Set Metric

Set Tag

Set Route Type

Set AS Path Tag

Set Community

Set Local Preference

Set Origin

Set Weight

Set Auto Tag

Set Level

Set External Community Id

Set External Cost

Select	Route Map Name	Sequence Number	Next Hop Type	Set Next Hop Address	Set Interface	Set Metric	Set Tag	Set Route Type	Set AS Path Tag	Set Community
☒	Route1	1	IPv4	255.255.255.255	vlan1	1057	0	N/A	0	N/A

Set Local Preference	Set Origin	Set Weight	Set Enable Auto Tag	Set Level	Set ExtCommId	Set ExtCommCost
0	N/A	0	N/A	N/A	0	0

Screen Objective	This screen allows the user to set the Route Map Set information.
NOTE: This screen can be configured only if Route Map is created using the Route Map Creation screen (Layer 3 Management > Route Map > Route Map Creation)	
Navigation	Layer 3 Management > Route Map > Route Map Set
Fields	Select—select the route map name for which the configuration needs to be deleted. Route Map Name—select the specified route-map in the list of route-maps. NOTE: The route map is created using Route Map Creation screen. Sequence Number—select the position of a new route map in the list of route maps already configured with the same name. This value ranges from 1 to 10. NOTE: The sequence number is created using Route Map Creation screen. Next Hop Type—select the inet type of address for next hop. The option is IPv4. Set Next Hop Address—select the inet type of address for next hop. The option is IPv4. Set Interface—select the <i>VLAN</i> interface which is already created and through which the next hop can be reached; sets the interface for a route that satisfies the match conditions.

Fields (cont)	• Set Metric—enter the primary routing metric. The semantics of the metric are determined by the routing-protocol specified. This value ranges from 1 to 214748367 (0x7fffffff). • Set Tag—enter the tag value of the routing protocol. This value ranges from 1 to 214748367 (0x7fffffff). • Set Route Type—select the route type as per RFC 2096. The list contains: – N/A—specifies that no route type is selected. – local—sets the connected routes. – remote—sets the non-connected routes (static / routing protocol installed routes). • Set AS Path Tag—enter the tag of a route into an AS path. Applies only when redistributing routes into BGP. This value ranges from 1 to 214748367 (0x7fffffff). • Set Community—enter the tag of a route into an AS path. Applies only when redistributing routes into BGP. This value ranges from 1 to 214748367 (0x7fffffff). – N/A—specifies that no BGP communities attribute is set in the route – internet—sets the BGP community attribute in the route as Internet where it advertises this route to the Internet community. All routers in the network belong to it. – local-as—sets the BGP community attribute in the route as local-as, where it sends this route to peers in other sub autonomous systems within the local confederation; it does not advertise this route to an external system. – no-advt—sets the BGP community attribute in the route as No-advt, which does not advertise all routes carrying communities' attributes to other BGP peers. – no-export—sets the BGP community attribute in the route as No-export, where all routes carrying a community attribute containing this value MUST NOT be advertised outside a BGP confederation boundary. – none—sets the BGP community attribute in the route as none which implies that no community is set. • Set Local Preference—enter a preference value for the AS path in the route. The preference is sent to all routers in the local AS only. This value ranges from 1 to 214748367. • Set Origin—select the origin of the route in BGP. The list contains: – NA—specifies that no origin is selected. – igp—sets the origin of route in BGP is remote interior gateway protocol. – egp—sets the origin of route in BGP is local exterior gateway protocol. – incomplete—sets the origin of the route in BGP is incomplete. Incomplete indicates unknown heritage • Set Weight—enter the BGP weight for the routing table. This value ranges from 1 to 65535 (0xffff). This is set during the process of policy routing or route redistribution.

Field (cont)	• Set Auto Tag / Set Enable Auto Tag—select the status of computing of tag table when distributing routes from <i>BGP</i> into IGP. The default option is disable. The list contains: – N/A—indicates that no status is selected for computing of tag table when distributing routes from <i>BGP</i> into IGP. – 1—enables automatic computing of tag table when redistributing routes from <i>BGP</i> into IGP. – 2—disables automatic computing of tag table when redistributing routes from <i>BGP</i> into IGP. • Set Level—select the level for routes that are advertised into the specified area of the routing domain. This is set during the process of policy routing or route redistribution. The list contains: – N/A—indicates that no level of routes is selected. – level-1—imports routes that are advertised in a Level 1 area. – level-2—imports routes that are advertised in a Level 2 subdomain – level-1-2—imports routes that are advertised in a Level 1 and Level 2. – stub-area—imports routes that are advertised in an <i>OSPF NSSA</i> (Not-so-stubby Area). – Backbone—imports routes that are advertised into an <i>OSPF</i> backbone area. • Set External Community ID / Set ExtCommID—enter the community ID attribute, used in determining the <i>BGP</i> best route when extcommunity cost is same for the routes. Route with lowest cost is preferred. Note that this is a type of the opaque extended community. This value ranges from 1 to 255. • Set External Cost / Set ExtCommCost—enter the extended cost community value that is used to determine the <i>BGP</i> best route. This value ranges from 1 to 4294967295.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • DELETE—deletes the selected entry.

IP Prefix List

Figure 10: IP Prefix List

Ip Prefix List

Ip Prefix Name *

Sequence Number *

Address Type IPv4 ▾ *

Address Prefix *

Prefix Length *

Min Prefix Length 0

Max Prefix Length 0

Action Permit ▾ *

Select	Ip Prefix Name	Sequence Number	Address Prefix	Prefix Length	Min Prefix Length	Max Prefix Length	Action
☒	ip1	1	10.0.0.0	1	0	0	Permit
Delete							

***Note : IP Prefix filters with sequence number greater than 100
can be created only if the related Sizing parameters are increased***

Screen Objective	This screen allows the user to create Route Map which can be used in policy-based routing and route redistribution.
Navigation	Layer 3 Management > Route Map > IP Prefix List
Fields	• Select—select the IP Prefix Name for which the configuration needs to be deleted. • IP Prefix Name—enter the name of a prefix list entry. This value is a string of maximum size 32 characters. NOTE: IP Prefix filters with sequence number greater than 100 can be created only if the related sizing parameters are increased. • Sequence Number—enter the sequence number of an entry. If sequence number is not specified it will be generated automatically. This value ranges from 1 to 4294967295. • Address Type—select the type of IP address at which the prefix list can be created. IPv4—sets the type of IP address prefix as IP version 4. • Address Prefix—enter the IPv4 / IPv6 Address Prefix. • Prefix Length—enter the prefix length for IPv4 / IPv6 address. This value ranges from 1 to 32 for IPv4 address and 0 to 128 for IPv6 address. • Min Prefix Length—enter the minimum prefix length to be matched. This value ranges from 1 to 32 for IPv4 address. NOTE: Minimum prefix length must be greater than prefix length and less than or equal to max prefix length.

Fields	• Max Prefix Length—enter the maximum prefix length to be matched. This value ranges from 1 to 32 for IPv4 address and 0 to 128 for IPv6 address. NOTE: Maximum prefix length must be greater than prefix length and greater than or equal to min prefix length. • Action—select the access type associated with the sequence number in a route map. Once an instance of this object is created, its value cannot be changed. The default option is Permit. Options are: – Permit—sets the access type associated with sequence number in a route map as Permit. This permits matching of route entry with entry rules. – Deny—sets the access type associated with sequence number in a route-map as Deny. This denies the route entry to match entry rules.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Delete—deletes the selected entry.

20.3. OSPF

This section describes the configuration options for the Open Shortest Path First (*OSPF*) routing protocol.

OSPF (Open Shortest Path First) 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).

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.

To access **OSPF** screens, go to **Layer 3 Management > OSPF**.

[OSPF VRF Creation](#)

[Debug Trace Settings](#)

[OSPF Basic Settings](#)

[OSPF Area Configuration](#)

[OSPF Interface Configuration](#)

[OSPF Virtual Interface Configuration](#)

[OSPF Neighbor Configuration](#)

[OSPF RRD Route Configuration](#)

[OSPF Area Aggregation](#)

[OSPF AS External Area Aggregation](#)

[Graceful Restart Settings](#)

OSPF VRF Creation

By default, the tab **OSPF VRF Creation** displays **OSPF VRF Creation** screen.

Figure 11: OSPF VRF Creation

Ospf VRF Creation

VRF Name	default ▾
VRF Status	Enabled ▾
Add Delete	

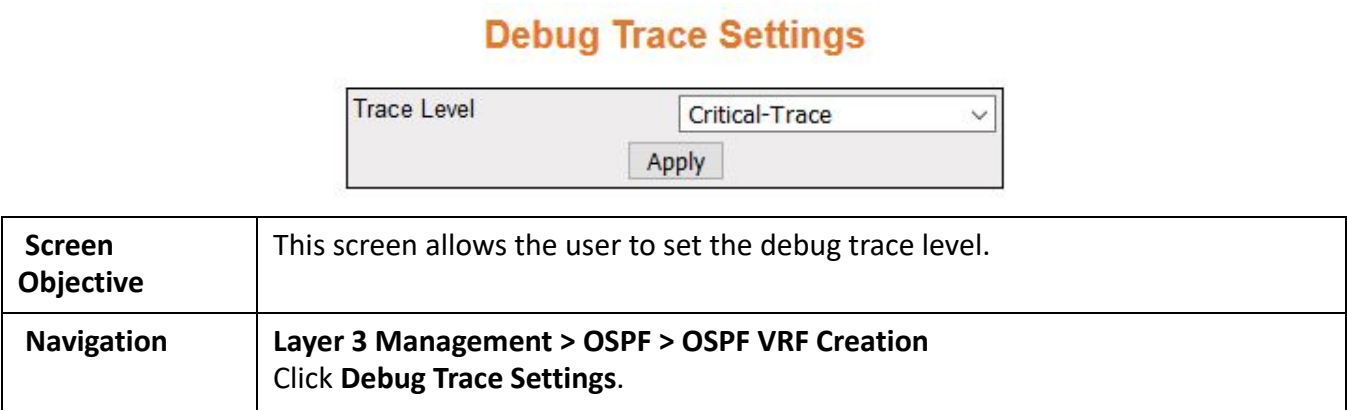
VRF Name	VRF Status
default	Enabled ▾

Note: Follow this link to enable [Global Debug Traces](#)

Screen Objective	This screen allows the user to enable or disable <i>OSPF</i> for the specified <i>VRF</i> instance.
Navigation	Layer 3 Management > OSPF > OSPF VRF Creation
Fields	VRF Name—default. VRF Status—select the admin status of <i>OSPF</i> virtual context. The default option is Disabled. The list contains: - Enabled—enables <i>OSPF</i> in the virtual context. - Disabled—disables <i>OSPF</i> in the virtual context.
Buttons	Add—adds and saves new configuration. NOTE: Status cannot be disabled using this option. Delete—delete the selected entry. NOTE: Entry can be deleted only when the <i>VRF</i> status is configured as disabled.

Debug Trace Settings

Figure 12: Debug Trace Settings



Fields	• Trace Level—select the level of trace required for <i>OSPF</i>. The list contains: – High-Level-Trace—generates debug statements for Packet High Level Dump trace. – Low-level-Trace—generates debug statements for Packet Low Level Dump trace. – Hex-Dump-Trace—generates debug statements for Packet Hex Dump trace. – Critical-Trace—generates debug statements for Critical trace. – Func-entry-Trace—generates debug statements for Function Entry trace. – Func-exit-Trace—generates debug statements for Function Exit trace. – Memory-Success-Trace—generates debug statements for Memory Allocation Success Trace. – Memory-Failure-Trace—generates debug statements for Memory Allocation Failure Trace. – Hello-pkt—generates debug statements for Hello packet Trace. – DDP—generates debug statements for DDP packet Trace. – LRQ—generates debug statements for Link State Request Packet Trace. – LSU—generates debug statements for Link State Update Packet Trace. – LS-ACK—generates debug statements for Link State Acknowledge Packet Trace. – ISM—generates debug statements for Interface State Machine Trace. – NSM—generates debug statements for Neighbor State Machine Trace. – RTC-TRACE—generates debug statements for Routing Table Calculation Trace. – RTM Module-Trace—generates debug statements for RTM Module Trace. – Interface-Trace—generates debug statements for Interface Trace. – NSSA Trace—generates debug statements for <i>NSSA</i> Trace. – Route-aggregation Trace—generates debug statements for Route Aggregation Trace. – Configuration-Trace—generates debug statements for Configuration Trace.
Fields (cont)	• Trace Level—the list contains (cont): – Adjacency—generates debug statements for Adjacency formation Trace. – LSDB—generates debug statements for Link State Database Trace (LSDB). – Protocol pkt processing—generates debug statements for Protocol Packet Processing Trace.

Buttons	Add—modifies attributes for the selected entry and saves the changes.

OSPF Basic Settings

Figure 13: OSPF Basic Settings

OSPF Basic Settings

Context Name

default ▾*

Router ID

Autonomous System Border Router

No ▾

RFC 1583 Compatibility

Yes ▾

NSSA ASBR-Default-Route Translator

Disabled ▾

ABR-type

Standard ▾

Distance

Default-Information

SPF Delay

1

SPF Hold Time

10

Trace Level

Critical-Trace ▾

GR Trace-Level

Restarting-router ▾

ADD

Select	Context Name	Router Id	Autonomous System	RFC 1583 Compatibility	NSSA ASBR-Default-Route	ABR-type
☒	default	5.5.5.1	No ▾	Yes ▾	Disabled ▾	Standard ▾

Distance	Default-Information	SPF Delay	SPF Hold Time	Trace-Level	GR-Trace
110	0	1	10	Critical-Trace ▾	▾

Apply Delete

Screen Objective	This screen allows the user to configure the basic settings of <i>OSPF</i> .
Navigation	Layer 3 Management > OSPF > Basic Settings

Fields	• Select—click to choose the Context Name for which configuration needs to be modified or deleted. • Context Name—default. • Router ID—enter a 32-bit integer that uniquely identifies the originating router in the AS. • Autonomous System Border Router/ Autonomous System—select the status of an <i>ASBR</i> (AS Border Router). The default option is Yes. The list contains: – Yes—configures the router as an <i>ASBR</i>. – No—configures the router within AS. • RFC 1583 Compatibility—select the compatibility status of RFC 1583 or RFC 2178. This controls the preference rules, when choosing among multiple AS external <i>LSAs</i> advertising the same destination. The default option is Yes. The list contains: – Yes—sets the preference rules to those specified by the RFC 1583. – No—sets the preference rules to those specified by the RFC 2178. • NSSA ASBR Default Route Translator/ NSSA ASBR Default Route—select the status of the P-Bit setting for the default Type-7 <i>LSA</i> (Link State Advertisement) generated by <i>NSSA</i> internal <i>ASBR</i>, which is not <i>ABR</i> (Area Border Router)). The default option is Disabled. The list contains: – Enabled—sets the P-Bit in the generated Type-7 default <i>LSA</i>. – Disabled—clears the P-Bit in the generated default <i>LSA</i>. • ABR Type—select the type of <i>ABRs</i> supported. The default option is Standard. The list contains: – Standard—chooses the <i>ABR</i> type as Standard. – CISCO— chooses the <i>ABR</i> type as CISCO. – IBM— chooses the <i>ABR</i> type as IBM. • Distance—enter the administrative distance (the metric to reach destination) of the routing protocol. This value ranges from 1 to 255. The default value is 0. The value 0 represents the directly connected route. NOTE: The administrative distance can be enabled for only one route map. The distance should be disassociated from the already associated route map if distance needs to be associated for another route map. • Default Information—enter the default information that is to be used for configuring the OSPF basic settings. This value ranges from 0 to 65535.

Fields (cont)	• SPF Delay—configures the interval by which SPF calculation is delayed after a topology change reception. This value ranges from 0 to 65535 seconds. The default value is 1. • SPF Hold Time—configures the minimum time between two consecutive SPF calculations. This value ranges from 0 to 65535 seconds. The default value is 10. • Trace Level—select the level of trace required for OSPF. The list contains: – Packet High Level Dump Trace—generates debug statements for Packet High Level Dump trace. – Packet Low Level Dump Trace—generates debug statements for Packet Low Level Dump trace. – Packet Hex Dump Trace—generates debug statements for Packet Hex Dump trace. – Critical Trace—generates debug statements for Critical trace. – Function Entry Trace—generates debug statements for Function Entry trace. – Function Exit Trace—generates debug statements for Function Exit trace. – Memory Allocation Success Trace—generates debug statements for Memory Allocation Success Trace. – Memory Allocation Failure Trace—generates debug statements for Memory Allocation Failure Trace. – Hello packet Trace—generates debug statements for Hello packet Trace. – DDP packet Trace—Generates debug statements for DDP packet Trace. – Link State Request Packet Trace—generates debug statements for Link State Request Packet Trace. – Link State Update Packet Trace—generates debug statements for Link State Update Packet Trace. – Link State Acknowledge Packet Trace—generates debug statements for Link State Acknowledge Packet Trace. – Interface State Machine Trace—generates debug statements for Interface State Machine Trace. – Neighbor State Machine Trace—generates debug statements for Neighbor State Machine Trace. – Routing Table Calculation Trace—generates debug statements for Routing Table Calculation Trace. – RTM Module Trace—generates debug statements for RTM Module Trace.

Fields (cont)	• Trace Level—the list contains (cont): – Interface Trace—generates debug statements for Interface Trace. – NSSA Trace—generates debug statements for NSSA Trace. – Route Aggregation Trace—generates debug statements for Route Aggregation Trace. – Configuration Trace—generates debug statements for Configuration Trace. – Adjacency formation Trace—generates debug statements for Adjacency formation Trace. – Link State Database Trace—Generates debug statements for Link State Database Trace. – Protocol Packet Processing Trace—generates debug statements for Protocol Packet Processing Trace. • GR Trace-Level—select the graceful restart trace level for <i>OSPF</i>. The list contains: – Restarting-router—generates debug statements for messages related to restarting router. – Helper—generates debug statements for messages related to router in helper Mode. – Redundancy—generates debug statements for redundancy messages.
Buttons	• ADD—adds and saves new configuration. • Apply—modifies attributes for the selected entry and saves the changes • Delete—delete the selected entry.

OSPF Area Configuration

Figure 14: OSPF Area Configuration

OSPF Area Configuration

Context Name: default *

Area ID: *

Type: Normal

Send Summary Routes: No

Metric: 10

Metric Type: ospfMetric

Type Of Service: 0

Translator Role: candidate

NSSA Translator Stability Interval: 40

ADD Reset

Select	Context Name	Area ID	Type	Send Summary Routes	Stub Metric	Stub Metric Type	TOS	Translator Role	Stability Interval	SPF Run Count
☒	default	0.0.0.0	Normal	No	10	ospfMetric	0	candidate	40	0

Apply Delete

Screen Objective	This screen allows the user to configure the parameters of the router's attached areas.
Navigation	Layer 3 Management > OSPF > Area

Fields	• Context Name—default. • Area ID—enter the IP Address that uniquely identifies an area that is associated with the <i>OSPF</i> address range for which authentication is to be enabled. • Type—select the required type for an area. The default option is Normal. The list contains: – Normal—allows all external <i>LSAs</i> (Type 5 <i>LSA</i>) to be flooded through the area. – Stub—does not allow the external <i>LSA</i> to be flooded into the area. – NSSA—allows only limited number of Type 5 external <i>LSA</i> to be translated into Type 7 <i>LSA</i> and flooded into the area. • Metric / Stub Metric—enter the metric value applied at the indicated type of service. This is applicable to stub and <i>NSSA</i> area. This value ranges from 0 to 16777215. The default value is 10. NOTE: This field is enabled only when Type is set as “<i>NSSA</i>” and Send Summary routers is set as “Yes”. • Metric Type/ Stub Metric Type—select the type of metric advertised as a default route. This is applicable to stub and <i>NSSA</i> area. The default option is <i>ospfMetric</i>. The list contains: – <i>ospfMetric</i>—sets the metric type as <i>ospfMetric</i>. – <i>comparableCost</i>—sets the metric type as comparable cost. – <i>nonComparable</i>—sets the metric type as noncomparable. NOTE: This field is enabled only when Type is set as “<i>NSSA</i>” and Send Summary routers is set as “Yes”. • Type of Service / TOS—enter the type of service associated with the metric. This is applicable to stub and <i>NSSA</i> area. The default value is 0. NOTE: This field is enabled only when Type is set as “<i>NSSA</i>” and Send Summary routers is set as “Yes”. • Translator Role—select an <i>NSSA</i> border router’s ability to perform <i>NSSA</i> translation of Type-7 <i>LSAs</i> to Type-5 <i>LSAs</i>. The default option is Candidate. The list contains: – Always—sets the translator role as always to perform <i>NSSA</i> translation of Type-7 <i>LSAs</i> to Type-5 <i>LSAs</i>. – Candidate—sets the translator role as candidate to perform <i>NSSA</i> translation of Type-7 <i>LSAs</i> to Type-5 <i>LSAs</i> • NSSA Translator Stability Interval/ Stability Interval—enter the number of seconds after which an elected translator determines that its services are no longer required. This value ranges from 0 to 2147483647. The default option is 40 seconds. • SPF Run Count—displays the shortest path first (SPF) run count. The Run Count depends upon the metric type value. This value ranges from 0 to 65535. This field is greyed out.

Buttons	• ADD—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes • Delete—delete the selected entry. NOTE: An auto generated entry cannot be deleted.

OSPF Interface Configuration

Figure 15: OSPF Interface Configuration

OSPF Interface Configuration

Context Name	*
Interface	loopback5 *
Area ID	0.0.0.0
Priority	1
Authentication Type	None
MD5 Key ID	
Authentication Key	
Metric	1
Passive	No
Demand Circuit	No
If Type	broadcast
Transit Delay	1
Retransmit Interval	5
Hello Interval	10
Dead Interval	40
ADD Reset	

Select	Context Name	IP Address	Area ID	Priority	Designated Router	Authentication Type
☐	default	5.5.5.1	0.0.0.0	1	0.0.0.0	None
☒	default	192.168.10.1	0.0.0.0	1	192.168.10.1	None

MD5 Key Id	Authentication Key	Metric	Passive	Demand Circuit	If Type	Transit Delay	Retransmit Delay	Hello Interval	Router Dead Interval
		1	No	No		1	5	10	40
		1	No	No	broadcast	1	5	10	40

Screen Objective	This screen allows the user to configure an <i>OSPF</i> for the specified interface.
Navigation	Layer 3 Management > OSPF > Interface
Fields	• Select—choose the context name for the <i>OSPF</i> Interface configuration. • Context Name—default. • Interface—select the interface index of the port which are already configured. NOTE: VLAN interface should be created in Layer 3 Management->IP->VLAN Interface Basic settings. • Area ID—enter the IP Address that uniquely identifies an area that is associated with the OSPF address range for which authentication is to be enabled. • Priority—enter the priority of the interface, which is used in the <i>DR</i> (Designated Router) election algorithm. 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. This value ranges from 0 to 255. The default value is 1. • Authentication Type—enter the type of authentication used on the interface. The default option is None. The list contains: – None—sets the authentication type as no password authentication. – Simple Password—sets the authentication type as Simple password type authentication. – MD5—sets the authentication type as Message Digest 5 based authentication. – SHA-1—sets the authentication type as Secure Hash Algorithm 1 (<i>SHA1</i>) authentication. <i>SHA1</i> generates Authentication digest of length 20 bytes. – SHA-224—sets the authentication type as Secure Hash Algorithm 224 (<i>SHA224</i>) authentication. <i>SHA224</i> generates Authentication digest of length 28 bytes. – SHA-256—sets the authentication type as Secure Hash Algorithm 256 (<i>SHA256</i>) authentication. <i>SHA256</i> generates Authentication digest of length 32 bytes. – SHA-384—sets the authentication type as Secure Hash Algorithm 384 (<i>SHA384</i>) authentication. <i>SHA384</i> generates Authentication digest of length 48 bytes. – SHA-512—sets the authentication type as Secure Hash Algorithm 512 (<i>SHA512</i>) authentication. <i>SHA512</i> generates Authentication digest of length 64 bytes.

Fields (cont)	• MD5 Key ID—enter the secret key used to create the message digest appended to the <i>OSPF</i> packet if the authentication type is MD5. This value ranges from 0 to 255. NOTE: This field is inactive when the authentication type is None and Simple Password • Authentication Key—enter the key required for authentication, if authentication is enabled on this interface. NOTE: This field is inactive when the authentication type is None. • Metric—enter the metric of using the type of service on the interface. This value ranges from 1 to 65535. The default value is 10. • Passive—select the interface as passive or normal. The default option is No. The list contains: – Yes—sets the interface as passive. – No—sets the interface as normal. • Demand Circuit—select the Demand <i>OSPF</i> procedures that should be performed on this interface. The default option is No. The list contains: – No—demand <i>OSPF</i> procedures do not perform on the selected interface – Yes—demand <i>OSPF</i> procedures perform on the selected interface. NOTE: On point-to-point interfaces, only one end of the demand circuit must be configured • If Type—select the OSPF interface type. The default option is broadcast. The list contains: – Broadcast—specifies that the network supports many (more than two) attached routers and has the capability to address a single physical message to all of the attached routers (broadcast) – nbma—specifies that the network supports many (more than two) routers but has no broadcast capability – point-to-point—sets the network topology to point-to-point type; this type displays a network of exactly two routers. – point-to-multipoint—sets the network type to point-to-multipoint and treats the non-broadcast network as a collection of point-to-point links. • Transit Delay—enter the number of seconds taken to transmit a link state update packet over the interface. This value ranges from 0 to 3600 seconds. The default option is 1 second. • Retransmit Interval—enter the number of seconds between link-state advertisement retransmissions, for adjacencies belonging to the interface. The retransmit-interval value is also used while retransmitting database description and link-state request packets. This value ranges from 0 to 3600 seconds. The default option is 5.

Fields (cont)	• Hello Interval—enter the length of time, in seconds, between the <i>OSPFv3</i> hello packets to a particular interface (i.e. the length of time, in seconds, between the Hello packets that the router sends to the interface). This value ranges from 1 to 65535 seconds. The default option is 10. • Dead Interval—enter the time period for which the router waits for hello packet from the neighbor before declaring this neighbor down. This value ranges from 0 to 2147483647 seconds. The default option is 40. • IP Address—displays the IP Address of the <i>OSPF</i> interface. This is a read-only field. • Designated Router—displays the IP Address of the Designated Router (<i>DR</i>). This is a read-only field.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes • Delete—delete the selected entry.

OSPF Virtual Interface Configuration

Figure 16: OSPF Virtual Interface Configuration

OSPF Virtual Interface Configuration

Context Name	default ▾ *
Transit Area ID	*
Neighbor Router ID	*
Authentication Type	None ▾
MD5 Key ID	
Authentication Key	
Hello Interval	10
Router Dead Interval	60
Transit Delay	1
Retransmit Interval	5
ADD Reset	

Select	Context Name	Transit Area ID	Neighbor Router ID	Authentication Type	MD5 Key Id	
☒	default	0.0.0.0	10.0.0.0	None ▾	MD5KeyId_KEY	Au

Authentication Key	Hello Interval	Router Dead Interval	Transit Delay	Retransmit Interval
Auth_KEY	10	60	1	5

Screen Objective	This screen allows the user to configure an <i>OSPF</i> virtual link and its parameters. NOTE: In <i>OSPF</i>, 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.
Navigation	Layer 3 Management > OSPF > Virtual Interface
Fields	• Select—click to choose the context name for which the <i>OSPF</i> Interface configuration needs to be done. • Context Name—default. • Transit Area ID—enter the 32-bit integer uniquely identifying an area, which is traversed by the virtual link NOTE: Area ID 0.0.0.0 is used for the <i>OSPF</i> backbone. • Neighbor Router ID—enter the router ID of the virtual neighbor. • Authentication Type—select the type of authentication used on the interface. The default option is None. The list contains: – None—sets the authentication type as no password authentication. – Simple Password—sets the authentication type as Simple password type authentication. – MD5—sets the authentication type as Message Digest 5 authentication. – SHA-1—sets the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes. – SHA-224—sets the authentication type as Secure Hash Algorithm 224 (SHA224) authentication. SHA224 generates Authentication digest of length 28 bytes. – SHA-256—sets the authentication type as Secure Hash Algorithm 256 (SHA256) authentication. SHA256 generates Authentication digest of length 32 bytes. – SHA-384—sets the authentication type as Secure Hash Algorithm 384 (SHA384) authentication. SHA384 generates Authentication digest of length 48 bytes. – SHA-512—sets the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. SHA512 generates Authentication digest of length 64 bytes. • MD5 Key ID—enter the secret key used to create the message digest appended to the OSPF packet if the authentication type is md5. This value ranges from 1 to 255. NOTE: This field is inactive when the authentication type is None and Simple Password. • Authentication Key—enter the key required for authentication, if authentication is enabled on this interface. NOTE: This field is inactive when the authentication type is None.

Fields (cont)	• Hello Interval—enter the length of time, in seconds, between the Hello packets send on the interface. This value ranges from 1 to 65535 seconds. The default option is 10. • Router Dead Interval—enter the time period for which the router waits for hello packet from the neighbor before declaring this neighbor down. This value ranges from 0 to 2147483647 seconds. The default option is 40. • Transit Delay—enter the number of seconds taken to transmit a link state update packet over the interface. This value ranges from 0 to 3600 seconds. The default option is 1 second. • Retransmit Interval—enter the number of seconds between link-state advertisement retransmissions, for adjacencies belonging to the interface. This value ranges from 0 to 3600 seconds. The default option is 5.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes • Delete—delete the selected entry.

OSPF Neighbor Configuration

Figure 17: OSPF Neighbor Configuration

OSPF Neighbor Configuration

The form contains three input fields: 'Context Name' with a dropdown menu showing 'default' and an asterisk, 'Neighbor IP Address' with a text box and an asterisk, and 'Priority' with a text box containing the value '1'. Below these fields are two buttons: 'ADD' and 'RESET'.

Note : Neighbor can be configured on NBMA or point-to-multipoint networks

Select	Context Name	Neighbor IP Address	Neighbor Priority

Apply Delete

Screen Objective	This screen allows the user to configure the neighbor router and its priority. NOTE: Neighbor configuration can be configured only on NBMA or Point-to-Multi-point networks. These networks can be configured using the Layer 3 Management > OSPF > Interface > OSPF Interface Configuration

Navigation	Layer 3 Management > OSPF > Neighbor
Fields	• Context Name—default • Neighbor IP Address—enter the Neighbour IP address. The priority of the neighbor is defined by the Neighbor router ID • Priority / Neighbor Priority—enter the priority of the neighbor in the designated router election algorithm. This value ranges from 0 to 255. The default value is 1. A value of 0 signifies that the neighbor is not eligible to become a designated router on this particular network.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes • Delete—delete the selected entry.

OSPF RRD Route Configuration

Figure 18: OSPF RRD Route Configuration

OSPF RRD Route Configuration

Context Name: default *

Destination Network: *

Network Mask: *

Route Metric: 10

Route Metric Type: asexttype2

Route Tag: 0

ADD Reset

Select	Context Name	Dest Network	Network Mask	Metric	Metric Type	Route Tag

Apply Delete

Screen Objective	This screen allows the user to configure the neighbor router and its priority. NOTE: Neighbor configuration can be configured only on NBMA or Point-to-Multipoint networks. These networks can be configured using the Layer 3 Management > OSPF > Interface > OSPF Interface Configuration
Navigation	Layer 3 Management > OSPF > Redistribution Route

Fields	• Context Name—default • Destination Network—enter the IP address of the destination route • Network Mask—enter the mask for the given destination route. • Route Metric / Metric—enter the metric value applied to the route before it is advertised into the OSPF domain. This value ranges from 1 to 16777215. The default value is 10. • Route Metric Type / Metric Type—select the metric type applied to the route before it is advertised into the OSPF domain. The default option is asexttype2. The list contains: – asexttype1—sets the route metric type as AS-External type 1 before it is advertised. – asexttype2—sets the route metric type as AS-External type 2 before it is advertised. • Route Tag—sets the tag type which describes whether tags will be automatically generated or will be manually configured. This value ranges from 0 to 4294967295. The default value is 0.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes for the selected entry and saves the changes • Delete—delete the selected entry.

OSPF Area Aggregation

Figure 19: OSPF Area Aggregation

OSPF Area Aggregation

Context Name *
Area ID *
Lsdb Type *
Network *
Mask *
Advertise *
External Tag

Select	Context Name	Area ID	Lsdb Type	Network	Mask	Advertise	External Tag
☒	default	0.0.0.0	summaryLink	10.0.0.0	255.0.0.0	advertiseMatching	0

Screen Objective	This screen allows the user to configure the External Tag for configured Type-7 address ranges.
Navigation	Layer 3 Management > OSPF > Aggregation

Fields	• Context Name—default • Area ID—enter the 32-bit integer uniquely identifying the area in which the address aggregate is to be found • Lsdb Type—select the Lsdb type of the address aggregate. The default option is summaryLink. The list contains: – summaryLink—sets the <i>LSA</i> type as summary <i>LSA</i> – nssaExternalLink—sets the <i>LSA</i> type as <i>NSSA</i> external Link • Network—enter the IP address of the network that enables the OSPF routing for interfaces defined and removing 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. • Mask—enter the Subnet Mask that pertains to the Net or Subnet for the given destination IPv4 address. • Advertise—select whether the subnets are advertised outside the area or not. The default option is advertiseMatching. The list contains:: – advertiseMatching—allows the subnets subsumed by ranges to trigger the advertisement of the indicated aggregate – doNotAdvertiseMatching—does not advertise subnets outside the area • External Tag—enter the External Tag of the external route. This tag is used to communicate information between AS boundary routers. The default value is 0.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes for the selected entry and saves the changes • Delete—delete the selected entry.

OSPF AS External Area Aggregation

Figure 20: OSPF AS External Area Aggregation

OSPF As External Aggregation Configuration

Context Name *
Network *
Mask *
Area ID *
Aggregation Effect
Translation

ADD
Reset

Select	Context Name	Network	Network Mask	Area ID	Advertise	Translation
☒	default	10.0.0.0	255.0.0.0	0.0.0.0	advertise	enabled

Apply
Delete

Screen Objective	This screen allows the user to configure the Type-5 / Type-7 address ranges specifying whether for the configured range, Type-5 / Type-7 <i>LSA</i> will be aggregated or not.
Navigation	Layer 3 Management > OSPF > AS Ext Aggregation
Fields	• Context Name—default • Network—enter the IP address of the network that enables the <i>OSPF</i> routing for interfaces defined and removing 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. • Mask—enter the Subnet Mask for the given destination IPv4 address • Area ID—enter 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. • Aggregation Effect /Advertise—select whether Type-5/Type-7 will be aggregated or not. The default option is advertise. The list contains: – advertise—generates aggregated Type-5 if the associated Area ID is 0.0.0.0; generates aggregated Type-7 in the corresponding <i>NSSA</i> area if Area ID is other than 0.0.0.0 – doNotAdvertise—generates aggregated Type-7 in all attached <i>NSSA</i> areas if the associated Area ID is 0.0.0.0. Does not generate aggregated Type-7 in the corresponding <i>NSSA</i> area if the Area ID is other than 0.0.0.0 – allowAll—generates aggregated Type-5 for the specified range and generates aggregated Type-7 in all attached <i>NSSA</i> areas only if the associated Area ID is 0.0.0.0. This allowAll option is not valid for Area ID other than 0.0.0.0. – denyAll—does not generate Type-5 or Type-7 for the specified range. This option is not valid for Area ID other than 0.0.0.0
Fields (cont)	• Translation—select the P Bit setting in the generated Type-7 <i>LSA</i>. The default option is enabled. The list contains: – enabled—sets P Bit in the generated Type-7 <i>LSA</i>. – disabled—clears the P Bit in the generated Type-7 <i>LSA</i>.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes for the selected entry and saves the changes • Delete—delete the selected entry.

Graceful Restart Settings

Figure 21: Graceful Restart Settings

Graceful Restart Settings

Context Name

default ▾*

Opaque Option

Enable ▾

Restart Support

None ▾

Restart Grace LSA Ack

Enable ▾

Grace LSA Retransmit Count

2

Restart Interval

120

Restart Reason

Unknown ▾

Helper Support:

UnKnown

☒

S/W Restart

☒

S/W Reload UpGrade

☒

Switch to Redundant

☒

Helper Strict LSA Checking

True ▾

Helper Grace Time Limit

0

Apply

Screen Objective	This screen allows the user to configure Graceful Restart for <i>OSPF</i> . The Graceful Restart feature allows forwarding of data packets to continue along known routes, while the routing protocol information is being restored following a processor switchover.
Navigation	Layer 3 Management > OSPF > Graceful Restart Settings

Fields	• Context Name—default • Opaque Option—select the opaque-capable option. The default option is Disable. The list contains: – Enable—enables the opaque-capable option. – Disable—disables the opaque-capable option. • Restart Support—select the router support for the <i>OSPF</i> Graceful Restart feature. The default option is None. The list contains: – None—does not restart support of the <i>OSPF</i> Graceful Restart feature. – Planned Only—restarts support of the <i>OSPF</i> Graceful Restart feature only in planned state. – Planned and Unplanned—restarts of the <i>OSPF</i> graceful restart feature both in planned and unplanned state. NOTE: This option is enabled only when opaque option is enabled. • Restart Grace LSA Ack—select whether the Grace <i>LSAs</i> sent by the router are expected to be acknowledged by the peers if the Grace Ack Required state is enabled. The default option is Enable. The list contains: – Enable—Grace <i>LSAs</i> sent by the router are acknowledged by the peers. – Disable—Grace <i>LSAs</i> sent by the router are not acknowledged. NOTE: This option is enabled only when opaque option is enabled. • Grace LSA Retransmit Count—enter the number of retransmissions for unacknowledged Grace <i>LSAs</i>. This value ranges from 0 to 180. The default value is 2. NOTE: This option is enabled only when opaque option is enabled. • Restart Interval—enter the <i>OSPF</i> Graceful Restart timeout interval. This value specifies the Graceful Restart interval, in seconds, during which the restarting router has to reacquire <i>OSPF</i> neighbors that are fully operational prior to the Graceful Restart. This value ranges from 1 to 1800. The default is 120. NOTE: This option is enabled only when opaque option is enabled. • Restart Reason—select the router Restart Reason code of the <i>OSPF</i> graceful restart feature. The default option is Unknown. The list contains: – UnKnown—restarts the system due to unplanned events (such as restarting after a crash). – S/W Restart—restarts the system due to software restart. – S/W Reload UpGrade—restarts system due to reloading / upgrading of software. – Switch to Redundant—restarts system due to switch over to a redundant support processor. NOTE: This option is enabled only when opaque option is enabled.

Fields (cont)	• Helper Support—select an opaque-capable option. The default option is Disable. The list contains: – UnKnown—sets the Helper Support for restarting of system due to unplanned events (such as restarting after a crash). – S/W Restart—sets the Helper Support for restarting of system due to restart of software. – S/W Reload UpGrade—sets the Helper Support for restarting of system due to reload or upgrade of software. – Switch to Redundant—sets the Helper Support for restarting of system due to switch over to a redundant support processor. • Helper Strict LSA Checking—select whether strict <i>LSA</i> checking is enabled for Graceful Restart. The default option is False. The list contains: – True—strict LSA checking is enabled for the Graceful Restart. – False—strict LSA checking is disabled for the Graceful Restart. NOTE: This option is enabled only when opaque option is enabled. • Helper Grace Time Limit—enter the <i>OSPF</i> Graceful Restart interval limit, in seconds, in the helper side. During this period, the router advertises that the restarting router is active and is in FULL state. This value ranges from 0 to 1800 seconds. The default option is 0. NOTE: This option is enabled only when the Opaque Option is enabled.
Buttons	• Apply—modifies attributes for the selected entry and saves the changes

20.4. Route Redistribution

RRD (Route Redistribution) allows different routing protocols to exchange routing information.

RRD (Route Redistribution) allows different routing protocols to exchange routing information. Using a routing protocol to advertise routes that are learnt by other means, such as another routing protocol, static routes, or directly connected routes, is called redistribution. While running a single routing protocol throughout an entire IP internetwork is desirable, multi-protocol routing is widespread for a number of reasons (e.g. company mergers, multiple departments managed by multiple network administrators, and multi-vendor environments). If a single routing protocol cannot be used, RRD is the only solution. Running different routing protocols is often part of a network design.

Every routing protocol on a network is separated into an Autonomous System (AS). All routers in the same autonomous system (running the same routing protocol) have complete knowledge of the entire AS. A router that connects two (or more) autonomous systems is known as a Border Router (*BR*). A *BR* advertises routing information from one AS to the other ASs. It is not possible to redistribute routing information for different routing protocols. Different routing protocols have different and often incompatible algorithms and metrics.

To access **Route Redistribution** screens, go to **Layer 3 Management > Redistribution**.

The Route Redistribution-related parameters are configured through the screens displayed by the following tabs:

[Redistribution RIP Configuration](#)

[Redistribution RIP Configuration](#)

[Redistribution OSPF Configuration](#)

Redistribution BGP Configuration

Figure 22: Redistribution BGP Configuration

Redistribution BGP Configuration

BGP Status

Disabled

Import Routes

Direct

RouteMap Name

Metric Value

0

Match Type

VRF Name

default

ADD

Select	BGP Status	Imported Route Type	RouteMap Name	Metric Value	Match Type	Context Name
☒	Enable	Direct	newroute	1		default

Delete

Note : To enable BGP Functionality, **BGP** module should be enabled.

Screen Objective	This screen allows the user to configure redistribution of the routes that are learnt through other routing protocols to <i>BGP</i> .
NOTE: To enable BGP functionality, enable BGP by going to Layer 3 Management > BGP > BGP Creation	
Navigation	Layer 3 Management > Redistribution > BGP

Fields	• Select—click to select the <i>BGP</i> routes for which <i>RRD</i> status needs to be deleted. • BGP Status—select the route redistribution status for <i>BGP</i>. The default option is Disabled. The list contains: – Enabled—imports the specified routes into BGP and distributes the BGP learnt routes to IGP (Interior Gateway Protocol) (RIP and OSPF). Redistributes route information for both internal and external BGP.. – Disabled—removes the specified routes from BGP and does not distribute or import routes from IGP (RIP and OSPF). • Import Routes—select Import Routes and control the redistribution of routes. The default option is Direct Route. The list contains: – Direct—enables import of directly connected routes into <i>BGP</i>. – Static—enables import of static routes into <i>BGP</i>. – RIP—enables import of RIP routes into <i>BGP</i>. – OSPF—enables import of OSPF routes into <i>BGP</i>. – ALL—enables import of all routes into <i>BGP</i>. • Route Map Name—enter the Routemap Name that identifies the specified route-map in the list of route-maps. This value is a string of maximum size 20. • Metric Value—enter the Metric Value that needs to be applied to the route before it is advertised into the BGP. This value is the domain Metric used for generating the default route. If the metric value is not specified, the default metric value considered as 1. The value used is specific to the protocol. This value ranges from 1 and 2147483647. • Match Type—select the metric type applied to the route before it is advertised into the OSPF domain. The options are: – External—redistributes OSPF external routes – Internal—redistributes OSPF internal routes – NSSA-External—redistributes OSPF NSSA external routes NOTE: This field is enabled only when the Import Routes are set as OSPF Routes.
Buttons	• ADD—adds and saves new configuration. • Delete—deletes the selected entry.

Redistribution RIP Configuration

Figure 23: Redistribution RIP Configuration

Redistribution RIP Configuration

RIP Status

Disabled ▾

Default Metric

3

Import Routes

Direct ▾

Route Tag Type

Manual ▾

Route Tag

0

RouteMap Name

ADD

Select	RIP Status	Default Metric	Imported Route Type	RouteTag Type	RouteTag	RouteMap Name
☒	Enable ▾	3	Direct ▾	Manual ▾	0	aa

Delete

Screen Objective	This screen allows the user to configure redistribution of the routes that are learnt through other routing protocols to <i>RIP</i> .
NOTE: To enable <i>RRD RIP</i> status, create <i>VRF</i> instance by using Layer 3 Management > RIP > RIP VRF Creation	
Navigation	Layer 3 Management > Redistribution > RIP

Fields	• Select—click to select the <i>RIP</i> routes for which <i>RRD</i> status needs to be deleted. • RIP Status—select the route redistribution status for <i>RIP</i>. The default option is Disabled. The list contains: – Enabled—sets the route redistribution status as enabled. When enabled, it advertises the routes learned by other protocols and redistributes route information for both internal and external <i>RIP</i>. – Disabled—sets the route redistribution status as disabled and stops redistribution of routes but sends updates to the RTM. • Default Metric—enter the default metric for the imported routes. This value ranges from 0 to 16. The default value is 3. • Import Routes—select Import Routes to be imported to <i>RIP</i>. The default option is Direct. The list contains: – Direct routes—enables import of directly connected routes into <i>RIP</i>. – Static—enables import of static routes into <i>RIP</i>. – BGP—enables import of <i>BGP</i> routes into <i>RIP</i>. – OSPF routes—enables import of <i>OSPF</i> routes into <i>RIP</i>. • Route Tag Type—elect whether the tag is manually configured or automatically generated. The default option is Manual. The list contains: – Manual—generates the tags manually. – Automatic—generates the tag automatically. • Route Tag—enter the Route Tag if the Route Tag type is selected as Manual. This value ranges from 0 to 65535. The default value is 0. • Route Map Name—enter the name that identifies the specified route map in the list of route-maps. This value is a string of maximum size 20.
Buttons	• ADD—adds and saves new configuration. • Delete—deletes the selected entry.

Redistribution OSPF Configuration

Figure 24: Redistribution OSPF Configuration

Redistribution OSPF Configuration

OSPF Status

Disabled ▾

Import Routes

Direct ▾

RouteMap Name

Metric Value

0

Metric Type

Type 2 External ▾

ADD

Select	OSPF Status	Imported Route Type	RouteMap Name	Metric Value	Metric Type
☒	Enable ▾	Direct ▾	bb	1	Type 2 External ▾

Delete

Note : *OSPF* module should be enabled to enable route redistribution functionality in *OSPF*.

Screen Objective	This screen allows the user to configure the redistribution of the routes that are learnt through other routing protocols to <i>OSPF</i> .
NOTE: To enable <i>RRD OSPF</i> status, <i>OSPF</i> must be enabled using Layer 3 Management > OSPF > OSPF VRF Creation	
Navigation	Layer 3 Management > Route Map > Route Map Match

Fields	• Select—click to select the <i>RIP</i> routes for which RRD status needs to be deleted. • OSPF Status—select the <i>OSPF</i> Status. The default option is Disabled. The list contains: – Enabled—sets the <i>OSPF</i> status as enabled. When enabled the advertises the routes learnt by other protocols. – Disabled—stops the redistribution of the routes but updates the Common Routing Table using the queue interface • Import Routes / Imported Route Type—select the source protocols from which routes are imported to <i>OSPF</i>. The default option is Direct routes. The list contains: – Direct routes—enables import of directly connected routes into <i>OSPF</i>. – Static routes—enables import of static routes into <i>OSPF</i>. – <i>RIP</i> routes—enables import of <i>RIP</i> routes into <i>OSPF</i>. – <i>BGP</i>—enables import of <i>BGP</i> routes into <i>OSPF</i>. – ALL—enables import of all routes into <i>OSPF</i>. • Route Map Name—enter the name that identifies the specified route-map in the list of route-maps. This value is a string of maximum size 20. • Metric Value—sets the Metric Type applied to the route before it is advertised into the <i>OSPF</i> Domain External link type associated with the default route advertised into the <i>OSPF</i> routing domain. • Metric Type—select the Metric type applied to the route before it is advertised into the <i>OSPF</i> domain. The default option is Type 2 External. The list contains: – Type 1 External—sets metric type as Type 1. – Type 2 External—sets metric type as Type 2.
Buttons	• ADD—adds and saves new configuration. • Delete—deletes the selected entry.

20.5. 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*.

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.

To access **VRRP** screens, go to **Layer 3 Management > VRRP**.

The *VRRP*-related parameters are configured through the screens displayed by the following tabs:

[VRRP Global Settings](#)

[IF Track Settings](#)

[IP Track Settings](#)

[VRRP Virtual Router Settings](#)

[Associated IP Table](#)

VRRP Global Settings

By default, the tab **Basic Settings** displays the **VRRP Basic Settings** screen.

Figure 25: VRRP Global Settings

VRRP Global Settings

VRRP Version

Version2

▼

VRRP Status

Enabled

▼

Auth Deprecate Status

Disabled

▼

Notification Control

Disabled

▼

Add

VRRP Version	VRRP Status	Auth Deprecate	Notification Control
v3	enabled	disabled	enabled

Note : *Auth Deprecate Configuration is valid when VRRP version enabled is v2.*

Screen Objective	This screen allows the user to set the global status of VRRP in the router.
Navigation	Layer 3 Management > VRRP > VRRP Global Settings

Fields	• VRRP Version—select the <i>VRRP</i> Version. The default is Version 2. Options are: – Version 2—sets the version for <i>VRRP</i> as version 2. – Version 2 and 3—sets the version for <i>VRRP</i> as version 2 and 3. – Version 3—sets the version for <i>VRRP</i> as version 3 NOTE: <i>VRRP</i> Version cannot be downgraded i.e. when <i>VRRP</i> version is set as V3, the <i>VRRP</i> version in the router cannot be configured to V2 or V2and3. • VRRP Status—select the <i>VRRP</i> Status. The default option is Disabled. The list contains: – Enabled—enables <i>VRRP</i> in the router. – Disabled—disables <i>VRRP</i> in the router. • Auth Deprecate Status—select an option to enable or disable authentication status. The default option is Enabled. The list contains: – Enabled—sets the authentication to Type 0 alone. – Disabled—sets the authentication to any one of the values Type 0–2 and the authentication feature is compatible with RFC 2338. NOTE: Auth Deprecate Configuration is valid with V2 <i>VRRP</i> version enabled. • Notification Control—select the <i>SNMP</i> trap generation status for the specified <i>VRRP</i> Router. The default option is Disabled. The list contains: – Enabled—enables the <i>VRRP</i> router to generate <i>SNMP</i> traps. – Disabled—disables the <i>VRRP</i> router from generating <i>SNMP</i> traps.
Buttons	• Add—adds and saves new configuration.

IF Track Settings

Figure 26: IF Track Settings

IF Track Settings

Group Number
No. of Link
Interface

Select	Group No	No of Links	Interface
☐	30	-	vlan1

Screen Objective

This screen allows the user to configure track settings for a *VRRP* router.

Navigation	Layer 3 Management > VRRP > IF Track Settings																
Fields	Select—click to select the group number for which the configuration need to be deleted. Group number/ Group No—enter the Group Number to have its track settings configured for the specified interface. The default value is 0. This value ranges from 1 to 4294967295. No. of Link/No. of Links—enter the number of links to be tracked. The default value is 0. This value range is from 1 to 255. NOTE: Tracked Links count should be lesser than or equal to the tracked interfaces created. Interface—select the interface from the list of VLAN interfaces already created and map the virtual router. NOTE: VLAN interface can be created using Layer 3 Management > IP >VLAN Interface screen, and IP can be assigned using Layer 3 Management > IP >IPV4 Address Configuration screen. VLAN Interface Basic Settings VLAN Interface Switch Admin State IPv4 Enabled State Proxy ARP MTU Create Reset <table><thead><tr><th>Select</th><th>VLAN Interface</th><th>Switch</th><th>Admin State</th><th>IPv4 Enabled State</th><th>Oper State</th><th>Proxy ARP</th><th>MTU</th></tr></thead><tbody><tr><td>☐</td><td>1</td><td>default</td><td>Up</td><td>Up</td><td>Up</td><td></td><td>1500</td></tr></tbody></table>	Select	VLAN Interface	Switch	Admin State	IPv4 Enabled State	Oper State	Proxy ARP	MTU	☐	1	default	Up	Up	Up		1500
Select	VLAN Interface	Switch	Admin State	IPv4 Enabled State	Oper State	Proxy ARP	MTU										
☐	1	default	Up	Up	Up		1500										
Buttons	ADD—adds and saves new configuration. Delete—deletes the selected entry.																

IP Track Settings

Figure 27: IP Track Settings

IP Track Settings

Query Delay	5
Pings Per Query	5
Query Success	4
Ping Frequency	2
Success	5
Failure	2
Save	

Group Number	
IP Address	0.0.0.0
Add	

Select	Group No	IP Address
Delete		

Screen Objective	This screen allows the user to configure IP track settings for a <i>VRRP</i> router.
Navigation	Layer 3 Management > VRRP > IP Track Settings
Fields	• Query Delay—enter the delay between consecutive tracking queries; default is 5. • Pings Per Query—number of pings per tracking query. The default value is 5. • Query Success—enter the number of successful pings per tracking query for it to be a success. The default value is 4. • Ping Frequency—frequency of pings in a query (pings/second); default is 2. • Success—enter the number of consecutive successful tracking queries for raising the priority; the default is 5. • Failure—enter the number of failed tracking queries for lowering the priority; the default is 2. • Group number/ Group No—enter the Group Number to have its IP track settings configured for the specified interface. The default value is 0. This value ranges from 1 to 4294967295. • IP Address—enter the IP Address.
Buttons	• ADD—adds and saves new configuration. • Delete—deletes the selected entry.

VRRP Virtual Router Settings

Figure 28: VRRP Virtual Router Settings

VRRP Virtual Router Settings

Virtual Router ID

Interface

Address-Type

Primary IP Address

Priority

Authentication Type

Authentication Key

Advt Timer unit

Advertisement Interval

Pre-emption

Accept-mode

Track Group Number

Decrement Priority

Select	Virtual Router ID	Interface	Address Type	Primary IP	Priority	Authentication Type	Authentication Key	Advertisement Interval (msecs)	Pre-emption
☐	1	vlan1	ipv4	12.0.0.1	100	no Auth	-	100	Enable

Note : Auth Type and Auth key Configuration is valid when VRRP version enabled is v2.

Accept Mode	Group No	Decrement Priority	Virtual MAC	Master Ip Addr	Oper State	Admin Status
☐	1	1	00:00:5e:00:01:0	0.0.0.0	Backup	Down

Screen Objective	This screen allows the user to configure the <i>VRRP</i> virtual router parameters.
Navigation	Layer 3 Management > VRRP > VRRP Virtual Router Settings
Fields	Select—click to select the virtual router for which the configurations need to be modified or deleted. Virtual Router ID—enter the virtual ID associated with each virtual router. This value ranges from 1 to 255.

Fields (cont)	• Interface—select the interface from the list of available <i>VLAN</i> interfaces to configure the virtual router. NOTE: <i>VLAN</i> interfaces can be created by using Layer 3 Management > IP > <i>VLAN</i> Interface screen, and IP can be assigned using Layer 3 Management > IP > <i>IPv4</i> Address Configuration screen. • Address Type—select the Address Type for configuring the virtual router. The default option is <i>IPv4</i>, which sets the address type as <i>IPv4</i> for configuring the virtual router. • Primary IP Address—enter the Primary IP Address for the virtual router. This is the IP address listed as the source in <i>VRRP</i> advertisement last received by this virtual router. NOTE: The Primary IP should be the same as the Interface IP when address type is set as <i>IPv4</i>. NOTE: Primary IP address can be configured when <i>VRRP</i> Version in the router is set as Version 2 and 3 or Version 3 in the <i>VRRP</i> Global Settings screen (Layer 3 Management > <i>VRRP</i> > <i>VRRP</i> Global Settings) • Priority—enter the priority to be used for the virtual router master election process. This value ranges from 1 to 254. The default value is 100. • Authentication Type—select the authentication type for the <i>VRRP</i> Protocol exchanges. The default option is no Authentication. Options are: – no Authentication/no Auth—configures the authentication type as No Authentication. This implies that the <i>VRRP</i> protocol exchanges are not authenticated. – Simple Text Password/Simple Txt—configures the authentication type as No Authentication. This implies that the <i>VRRP</i> protocol exchanges are authenticated by a clear text password. NOTE: Simple Text Password can be configured only when <i>VRRP</i> AuthDeprecate flag is disabled. NOTE: Authentication Type configuration is valid when <i>VRRP</i> version enabled is v2. • Authentication Key—enter the authentication key for the virtual router. This field is an octet string of maximum size 16. NOTE: This configuration is effective only if the Authentication type is Simple Text Password. NOTE: Authentication key configuration is valid when <i>VRRP</i> version enabled is v2 • Advertisement Timer unit—select the timer unit in which advertisement packets are sent. The list contains: – sec—sets the advertisement timer unit as seconds. – msec—sets the advertisement timer unit as milliseconds.

Fields (cont)	• Advertisement Interval—enter the time interval (in seconds) for sending the advertisement packets. Only the master router sends the <i>VRRP</i> Advertisements. This value ranges from 1 to 255 seconds. The default value is 1 second. NOTE: For version 2, the advertisement interval can be both in seconds and milliseconds, i.e. for seconds the value range is from 1 to 255 seconds, and for milliseconds the value range is from 100 to 255000 millisecond. NOTE: For version 3, the advertisement interval should be in milliseconds, and should start from 1 millisecond. • Preemption—select the option to enable or disable pre-emption of state change from either Backup to Master or vice versa based on election process. This controls whether a higher priority virtual router will pre-empt a lower priority master. The default option is Enable. Options are: – Enable—enables Accept-mode for the specified interface. – Disable—disables pre-emption of state change from either Backup to Master or vice versa based on the election process. • Accept-mode—select the option to enable or disable accept mode for the specified interface. The default option is Disable. The list contains: – Enable—enables Accept-mode for the specified interface. – Disable—disables Accept-mode for the specified interface. • Track Group Number / Group No—enter the group number to configure track settings for the specified interface. The default value is 0. • Decrement Priority—enter the value to configure the decrement priority for the specified interface. The default value is 0. This value range is from 0 to 254. • Virtual MAC—displays the virtual MAC address for the specified interface. • Master IP Address—displays the master IP address for the specified interface. • Operational State—displays the current state of the virtual router. This is a read-only field. The list contains: – Initialize—specifies that the virtual router is waiting for a start-up event. – Backup—specifies that the virtual router is monitoring the availability of the master router. – Master—specifies that the virtual router is forwarding packets for IP addresses that are associated with the router. • Admin Status—adds and saves new configuration. – Up—changes the state of the virtual router from Initialize to Backup or Master based on the priority value. – Down—changes the state of the virtual router from Master or Backup to Initialize. NOTE: Admin Status is Down when <i>VRRP</i> module status is disabled.

Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes for the selected entry and saves the changes. • Delete—deletes the selected entry. NOTE: When the entry is deleted, the entry in the Associated IP Table screen is also deleted.

Associated IP Table

Figure 29: Associated IP Table

Associated Ip Table

Virtual Router ID *

Interface *

Address-Type *

Secondary IP Address × *

Select	Virtual Router ID	Interface	Address Type	Assoc IP
Delete				

Screen Objective	This screen displays the IP addresses which are associated with the virtual router.
Navigation	Layer 3 Management > VRRP > Associated IP
Fields	• Select—click to select the virtual router for which the configuration need to be deleted. • Virtual Router ID—displays the virtual ID associated with each virtual router. This value ranges from 1 to 255. • Interface—displays the interface from the list of available VLAN interfaces to configure the virtual router. NOTE: Interface value can be created by using Layer 3 Management > IP >VLAN Interface screen, and IP can be assigned using Layer 3 Management > IP >IPv4 Addr Conf screen. • Address type— displays the Address type for configuring the virtual router. The list contains: – IPv4—sets the address type as IPv4 for configuring the virtual router. – IPv6—sets the address type as IPv6 for configuring the virtual router.

Fields	Secondary IP Address—enter the Secondary IP Address for the virtual router. NOTE: A Primary IP Address must be set up first Otherwise the following error message is appear. Associated IP—displays the IP address which is associated with the virtual router. NOTE: This field populates the Secondary IP Address which is configured for the interface using the VRRP virtual router settings screen. (Layer 3 Management > VRRP > VRRP Virtual Router Settings).
Buttons	ADD—adds and saves new configuration. NOTE: When the entry is added in this table, the added entry is automatically added in the VRRP Virtual Router Setting screen Delete—deleted the selected entry. NOTE: When the entry is deleted, the entry in the VRRP Virtual Router Setting screen is also deleted.

20.6. 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.

BGP (Border Gateway Protocol) is an Inter AS (Autonomous Systems) Routing Protocol that manages the distribution of Network Layer Reachability Information (*NLRI*) across AS.

To access **BGP** screens, go to **Layer 3 Management > BGP**.

BGP Creation

Figure 30: BGP Creation

BGP Creation

AS Number

BGP Context default ▾

BGP State Enabled ▾

AS Number	BGP State
1	Enabled

Screen Objective	This screen allows the user to configure the basic settings of <i>BGP</i> .
Navigation	Layer 3 Management > BGP > BGP Context
Fields	AS Number—enter the local AS number (<i>ASN</i>). The default value is 1. NOTE: This field can be configured only if the state of the <i>BGP</i> system is set as Disabled in the Basic Settings screen. NOTE: When four-byte <i>ASN</i> is enabled, this value ranges from 1 to 4294967295. NOTE: When four-byte <i>ASN</i> is disabled, this value ranges from 1 to 65535. NOTE: Four-byte <i>ASN</i> can be enabled/disabled using Layer 3 Management > BGP > BGP Basic Settings screen. BGP Context—default. BGP State—select the status of the <i>BGP</i> system: - Enabled—enables the <i>BGP</i> system. - Disabled—disables the <i>BGP</i> system.
Buttons	Add—adds and saves new configuration.

BGP Basic Settings

Figure 31: BGP Basic Settings

BGP Basic Settings

Select	Context Id	Status	Router Identifier	Synchronisation	Default Local Preference	Advertisement of Non-BGP Routes	Trace Level	Debug Level
☒	0	Enabled ▾	192.168.	Disabled ▾	100	ExternalAndInternal ▾	0	0

Overlap Router Policy	Always Compare MED	Default route redistribution	Default IPv4 unicast	Client to client reflection	AS Confed identifier	AS Confed Best-path compare MED	Bgp Trap	Internal BGP Routes Redistribution	4 Byte ASN Support Status	VPNv4 Capability	Label Allocation policy
Both ▾	Disabled ▾	Disable ▾	Enable ▾	Client support ▾	0	clear ▾	Enabled ▾	Disable ▾	Enable ▾	▾	▾

Screen Objective	This screen allows the user to configure the basic parameters of <i>BGP</i> in the system.
Note	To enable <i>BGP</i>, Route Redistribution must be enabled. Use Layer 3 Management > RRD. The <i>BGP</i> system can be enabled and the basic <i>BGP</i> parameters for a context can be configured, only if the local AS Number is configured for the context using the Layer 3 Management > BGP > BGP Context > BGP Creation screen.
Navigation	Layer 3 Management > BGP > BGP Basic Settings

Fields	• Select—select the context id for which the configurations need to be reapplied. • Context Id—0. • Status—select the status of <i>BGP</i> in the system. The default option is Disabled. The list contains. – Enabled—enables the <i>BGP</i> system. – Disabled—disables the <i>BGP</i> system. • Router Identifier—enter the <i>BGP</i> identifier of the local system. This router-id is advertised to other peers and identifies the <i>BGP</i> speaker uniquely. 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. NOTE: This field can be configured explicitly only if the <i>BGP</i> speaker is administratively active. The explicitly configured value will be preserved even after the restart of the <i>BGP</i>. NOTE: Peering sessions will be reset if the <i>BGP</i> identifier is changed. NOTE: This field can be set only if the local AS number is configured. NOTE: To restore the default value for <i>BGP</i> identifier, this field must be configured as 0.0.0.0. • Synchronization—select the synchronization status within an AS. The default option is Disabled. The list contains: – Enabled—enables the synchronization between <i>BGP</i> and <i>IGP</i>. This allows routers and access servers within an autonomous system to have the route before <i>BGP</i> makes it available to other autonomous systems. – Disabled—disables the synchronization between <i>BGP</i> and <i>IGP</i>. • Default Local Preference—enter 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 AS. This value ranges from 0 to 2147483647 with a default of 100. • Advertisement of Non-BGP routes—elect the peer type to which non-<i>BGP</i> routes must be sent. The default option is External and internal. The list contains: – External—sends non-<i>BGP</i> routes only to external peers. – External and internal—sends non-<i>BGP</i> routes to both external and internal peers.

Fields (cont)	• Trace Level—enables the traces in <i>BGP</i> module. This value ranges from 0 to 16. This value represents the tracing levels as follows: – 0—All Failures – 1—All Resource Allocation Failures – 2—Init and Shutdown Trace – 3—Management Trace – 4—Control Path Trace – 5—Data Path Trace – 6—Peer Connection Trace – 7—Update Message Trace – 8—<i>FDB</i> Update Trace – 9—Keep-Alive Trace – 10—All Transmission Trace – 11—All Reception Trace – 12—Dampening Trace – 13—Events Trace – 14—High level Packet Dump – 15—Low level packet Dump – 16—Hex Dump • Debug Level—enables the debug dynamically in <i>BGP</i> module. This value ranges from 0 to 4294967295. This is a four-byte integer value specified for enabling the level of debugging. Each bit in the four-byte integer variable represents a level of debug. • Overlap Router Policy—select to set the overlap policy which configures the <i>BGP</i> speaker's policy for handling the overlapping routes. When an overlapping route is received, depending upon the configured policy, either the less-specific routes or more-specific routes or both routes are installed in the <i>RIB</i> tree. The default option is both. This list contains: – More-Specific—installs more specific routes in the <i>RIB</i> tree. – Less Specific—installs more specific routes in the <i>RIB</i> tree. – Both—installs both more specific and less specific routes in the <i>RIB</i> tree. NOTE: This field can be set only if Local <i>ASN</i> is configured and Global Admin Status is down

Fields (cont)	• Always Compare MED—select the status of comparison of Multi Exit Discriminator (<i>MED</i>) for routes received from different autonomous systems. <i>MED</i> is one of the parameters considered for selecting the best path among many alternative paths. The path with a lower <i>MED</i> is preferred over a path with a higher <i>MED</i>. The default option is disable. The list contains: – Enabled—enables the comparison of <i>MED</i> for routes received from different autonomous system. This implies that <i>MED</i> is compared irrespective of the autonomous system from which the routes are received. – Disabled—disables the comparison of <i>MED</i> for routes received from different autonomous system. This implies that <i>MED</i> is compared only between routes received from the same autonomous system. • Default route redistribution—select the redistribution and advertisement status of the default route (0.0.0.0/0). The default option is Disable. The list contains: – Enable—enables redistribution and advertisement of default route to BGP peers. The default route advertisement is possible only if the default route is present in the IP <i>FDB</i> or is received from any peers. – Disable—disables redistribution and advertisement of the default route. • Default IPv4 unicast—select the status of default routing to IPv4-unicast. The default option is Enable. The list contains: – Enable—enables the negotiation of MP IPv4 Unicast Address Family Capability for that peer if a neighbor is created. – Disable—disables default routing to IPv4 unicast which implies that if a neighbor is created, IPv4 unicast capability will not be negotiated unless IPv4 unicast capability is explicitly configured for that neighbor. NOTE: This affects the negotiation of the MP IPv4 Unicast Address Family Capability for newly created peers but will not affect the MP IPV4 Unicast negotiation status of the already existing peers. • Client to client reflection—select the desired support of the Route Reflector in the cluster. By default, the Client to client reflection value is set as client support. 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 list contains: – None—sets Route Reflector support in the cluster as none. This is a read only field when set as none. – Client support—sets Route Reflector support in the cluster as client support. Non-client Support—sets Route Reflector support in the cluster as Non-client support • AS Confed Best-path compare MED—enter the Local Confederation Identification number of the AS confederation. This value ranges from 0 to 4264697295. The default value is 0. NOTE: When confed id is set to a non-zero value, this value must be reset to zero before reconfiguring confed id.

Fields (cont)	• Capability support—select the status of the Capability Advertisement Support. – True—enables Capability Advertisement Support – False—disables Capability Advertisement Support NOTE: This field can be set only if Global Admin Status is down and Local AS is configured. • Bgp Trap—select the trap status to be set for <i>BGP</i>. This status is used to control the sending of <i>BGP</i> notification messages to SNMP manager. The <i>BGP</i> notification messages are sent when any error is detected in input <i>BGP</i> messages received from peer or in the <i>BGP</i> state event machine. These notification messages are used to close an active session and to provide information about the closure of the session. The default option is Enabled. The list contains: – Enabled—enables the trap notification for the <i>BGP</i> system. – Disabled—disables the trap notification for the <i>BGP</i> system. • Internal BGP Routes Redistribution—elect the status of the <i>IBGP</i> routes redistribution to other <i>IGP</i> protocols. The default option is Disabled. The list contains: – Enabled—enables <i>IBGP</i> routes to be redistributed to other <i>IGP</i> protocols. – Disabled—disables <i>IBGP</i> routes to be redistributed to other <i>IGP</i> protocols. NOTE: This field can be set only if Global Admin Status is down and Local AS is configured. • 4 Byte ASN Support Status—select the 4 Byte ASN Support status in the <i>BGP</i> system. The default option is Enabled. The list contains: – Enable—enables 4-byte ASN support in <i>BGP</i>. If this is enabled, the Remote As value ranges between 1 and 4294967295. – Disable—disables 4-byte ASN support in <i>BGP</i>. If this is disabled, the Remote As value ranges between 1 and 65535. NOTE: This field can be set only if Global Admin Status is down and Local AS is configured. • VPN4 Capability—select the standard <i>VPNv4</i> address prefixes carrying capability. The default value is Disable. The list contains: – Enable—enables configuration of the session that carries standard <i>vpn4</i> address prefixes. <i>BGP4 VPN</i> allows the Service Providers to use their IP backbone to provide <i>VPN</i> services to their customers. <i>BGP</i> distributes <i>VPN</i> routing information across the provider’s backbone, and <i>MPLS</i> is used to forward <i>VPN</i> traffic from one <i>VPN</i> site to another. – Disable—disables configuration of the session that carries standard <i>VPNv4</i> address prefixes.

Fields (cont)	• Label Allocation policy—select the label allocation policy which is used for allocating the <i>VPN</i> label to be used for advertising the <i>VPN</i> routes. The default value is per-vrf. The list contains – per-vrf—sets label allocation policy as per vrf to advertise all routes learnt in the router with the same label. – per-route—sets label allocation policy as per route to advertise all routes learnt in the router with the unique label.
Buttons	• Add—adds and saves new configuration.

BGP Settings

Figure 32: BGP Settings

BGP Settings

Select	Cluster ID	BGP Next Hop Processing Interval	Default Metric	Admin Status	Capability support	eBgp Multipath count	iBgp Multipath count	eiBgp Multipath count	Table version	Context Id
☒	192.168.102.1	60	0	Enable	True	1	1	1	2	0

Screen Objective	This screen allows the user to configure the <i>BGP</i> Settings.
Note	This screen can be configured only when the BGP status is enabled using Layer 3 Management > BGP > Basic Settings > BGP Basic Settings screen.
Navigation	Layer 3 Management > BGP > BGP Settings

Fields	• Select—select the Cluster ID for which the configurations need to be modified. • Cluster ID—enter the Cluster ID of the Router Reflector of the <i>BGP</i> cluster which has more than one route reflector. By default, when the <i>BGP</i> speaker acts as Route Reflector, the <i>BGP</i> Identifier is used as the cluster ID. 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. • BGP Next Hop Processing Interval—enter the interval at which next hops are monitored for reachability. This value ranges from 1 to 120. The default value is 60. • Default Metric—enter the default metric value for the <i>IGP</i> routes and static route. If configured to 0, the metric received from the <i>IGP</i> route will be used. If configured to other value, the <i>MED</i> value of the redistributed routes takes this value. This value has no effect on direct routes. This value ranges from 1 to 2147483647. The default value is 0. • Admin Status—select the admin status of <i>BGP</i>. The default option is Disable. The list contains: – Enabled—enables the <i>BGP</i> system. – Disabled—disables the <i>BGP</i> system. • Capability Support—select the Capability Advertisement Support status. The default option is True. The list contains: – True—enables Capability Advertisement Support. – Disabled—disables the <i>BGP</i> system. • EBGP Multipath Count—enter the maximum number of external <i>BGP</i> (<i>EBGP</i>) multipath routes to be added per destination network in the routing table. This value ranges from 1 to 64. • IBGP Multipath Count—enter the maximum number of <i>IBGP</i> multipath routes to be added per destination network in the routing table. This value ranges from 1 to 64. • EIBGP Multipath Count—enter the maximum number of external plus internal <i>BGP</i> (<i>EIBGP</i>) multipath routes (with same AS PATH) to be added per destination network in Routing table. This value ranges from 1 to 64. • Table version—displays the table version which is the total number of valid routes learnt in the system. This is an integer value which is incremented by 1 when a valid route is learnt. • Context Id—0.
Buttons	• Add—adds and saves new configuration.

Neighbor Configuration

Figure 33: Neighbor Configuration

Neighbor Configuration

Peer Address	0.0.0.0 *
Remote AS	*
Configured BGP Maximum Prefix Limit	100
Configured Connect Retry Count	5
Automatic Start	Disable ▾
Automatic Stop	Disable ▾
Damp Peer Oscillations	Disable ▾
Delay OPEN	Disable ▾
EBGP MultiHop	Disable ▾
Next Hop	automatic ▾
Source Address	0.0.0.0
Gateway Address	0.0.0.0
Default originate	Disable ▾
Community Send status	send ▾
Extended Community Send status	send ▾
Route Reflector Client	nonClient ▾
Peer Connection passive	Disable ▾
EBGP Hop Limit	1
TCP Send Buffer Size	65536
TCP Receive Buffer Size	65536
Authentication	None ▾
Password	
TCP-AO MKT	
Peer Status	start ▾
BFD Monitoring	disable ▾
VRF Name	default ▾ *

ADDReset

Screen Objective

This screen allows the user to configure the *BGP* Neighbors.

Note	This screen can be configured only if the Route Re-distribution (<i>RRD</i>) status is enabled with valid <i>ASN</i> and router ID from the Layer 3 Management > RRD .
Navigation	Layer 3 Management > BGP > Neighbors
Fields	Select—select the neighbor for which the configurations need to be modified. Peer Address—enter the remote IP address of the <i>BGP</i> peer. NOTE: For a peer address with external <i>AS</i>, route reflector client cannot be set as Client. Remote AS—enter the remote <i>ASN</i> of the peer. This value ranges from 1 to 4294967295. NOTE: The admin status of the peer can be made up only if this field is configured for a valid <i>ASN</i>. NOTE: When four-byte <i>ASN</i> is enabled, this value ranges from 1 to 4294967295. NOTE: When four-byte <i>ASN</i> is disabled, this value ranges from 1 to 65535. NOTE: Four-byte <i>ASN</i> can be enabled/disabled using Layer3 Management > BGP > Basic Setting>BGP Basic settings screen. Configured BGP Maximum Prefix Limit—enter the prefix limit value to set upper bound on the number of address prefixes to be accepted by <i>BGP</i> speaker from a neighbor. The system will not process the prefixes exceeding the upper limit. This value ranges from 1 to 2147483647. The default value is 100. NOTE: The default value is calculated based on the following formula: Maximum number of routes in the routing table / Maximum number of peers supported by BGP. Configured Connect Retry Count—enter the retry count to specify the maximum number of times a <i>BGP</i> peer should try for issuing a TCP-Connect with its neighboring peers. This value ranges from 1 to 50. The default value is 5. Automatic Start—select the automatic start status for the <i>BGP</i> session with the associated peer. The automatic start will not occur, if the Idle-Hold timer value of the peer exceeds its maximum threshold value. The default option is Disable. The list contains: - Disable—disables automatic initiation of the <i>BGP</i> session with the peer for starting the peer status. - Enable—enables automatic starting of peer session from the idle state after peer idle hold time once the <i>BGP</i> peer session is brought down either by the following: - Automatic stop feature - Reception of invalid <i>BGP</i> message

Fields (cont)	• Automatic Stop—select the automatic stop status for the <i>BGP</i> connection with the associated peer. The default option is Disable. The list contains: – Disable—disables automatic stopping of <i>BGP</i> connection with the associated peer, as the connect retry count will be set as 0. – Enable—enables automatic stopping of <i>BGP</i> connection with the associated peer after the <i>BGP</i> peer attains configured maximum number of TCP connect retry count value. The allocated resources are released, and the peer remains in idle state. The peer session initiation is once again started based on the automatic start status, peer idle hold timer and damp peer oscillation status. • Damp Peer Oscillations—select the damp peer oscillation status that controls the usage of additional logic to dampen peer oscillations in states other than established. The default option is Disable. The list contains: – Disable—disables utilization of any logic to dampen the oscillations of <i>BGP</i> peers by <i>BGP</i> connection (disables peer connection damping). – Enable—utilization additional logic to dampen the oscillations of <i>BGP</i> peers by <i>BGP</i> connection during a series of automatic start and stop operations in the IDLE state. For each successive damp oscillations, the current idle hold timer value will be increased twice its previous value. This happens through internal logic. • Delay OPEN—select the delay open status that controls the option to apply delay in sending of open messages. The open message is the initial message sent by the <i>BGP</i> peers after establishing a <i>TCP</i> connection to open a <i>BGP</i> session between them. The default option is Disable. The list contains: – Disable—disables the delay option for sending open messages, which implies that open messages are sent to the remote <i>BGP</i> peer without any delay. – Enable—delay in sending open messages to the remote <i>BGP</i> peer for a configured open delay time period. This delay allows the remote peer to send the first open message.

Fields (cont)	• EBGP MultiHop—select the <i>EBGP</i> MultiHop option which enables/disables the BGP4 speaker to establish connections to external peers residing on network that are not directly connected. The default option is Disable. The list contains: – Disable—disables <i>BGP</i> to establish connection with external peers residing on networks that are not directly connected. If <i>EBGP</i> MultiHop is disabled and external <i>BGP</i> peers are indirectly connected, then <i>BGP</i> peer session will not be established. – Enable—enables <i>BGP</i> to establish connection with external peers residing on networks that are not directly connected. If external <i>BGP</i> peer are not connected directly, then <i>EBGP</i> MultiHop is enabled to initiate the connection with that external peer. NOTE: This field is applicable only for the directly connected <i>EBGP</i> peers and not applicable for the internal peers. • Next Hop—whether the next hop attribute sent in the update message to the peer has to be generated automatically or self. This is useful in non-meshed networks where <i>BGP</i> neighbors may not have direct access to all other neighbors on the same IP subnet. The default option is automatic. The list contains: – automatic—generates the next hop based on the IP address of the destination and the present next hop in the route information. – self—sets the sender local address as the next hop attribute. • Source Address—enter the address to be used as the source address for the <i>TCP</i> session initiated with the peer. NOTE: The configured peer address is set as the source address, if no value is configured for the source address • Gateway Address—enter the gateway router’s address to be used as NextHop in the routes advertised to the peer. • Default originate—select the status of the advertisement of the default route to the peer or neighbor for use as a default route. The default option is Disable. The list contains: – Disable—disables the advertisement of the default route. – Enable—enables the advertisement of the default route. NOTE: This field overrides the global default route configuration and always sends a default route to the peer with self next-hop. This advertisement occurs irrespective of the presence of default route in <i>FDB</i>.

Fields (cont)	• Community Send status—select the status of the send community attribute to a <i>BGP</i> neighbor. The default option is send. The list contains: – none—sets Community Send status as none. – send—sends community attribute to a <i>BGP</i> neighbor and enables advertisement of community attributes (standard/extended) to peer – dontSend—disables advertisement of standard community attributes to peer the advertisement of the default route. • Extended Community Send status—select the status of extended community send attribute of the <i>BGP</i> peer. The <i>BGP</i> extended community is used to label <i>BGP</i> routing information for controlling the distribution of the information. The default option is send. The list contains: – none—sets extended Community Send status as none. – send—sends extended community attribute to a <i>BGP</i> neighbor and enables advertisement of community attributes (standard/extended) to peer – dontSend—disables advertisement of standard community attributes to peer the advertisement of the default route. • Route Reflector Client—the Route Reflector Client status of the peer. This status is used to define client and non-client peers for implementing route reflection. The default option is nonClient. The list contains: – nonClient—Configures the peer as non-client peer, which denotes that the peer is outside the cluster – Client—Configures the peer as client peer, which denotes that the peer is within the cluster. <i>The route reflection mechanism operates as follows:</i> – A cluster system acting as route reflector sends a route to all client peers within the cluster, if the route is received from a nonclient peer. – The cluster system acting as route reflector sends a route to all nonclient peers and all client peers except the originator, if the route is received from a client peer. • Peer Connection passive—select the <i>BGP</i> peer connection status to control the initiation of session from remote peer or speaker. The default option is Enable. The list contains: – Enable—sets the peer connection as passive. <i>BGP</i> speaker waits for the remote peer to initiate the session with the peer. – Disable—sets the peer connection as active. <i>BGP</i> speaker initiates the session with the peer.

Fields (cont)	• TCP Send Buffer Size—enter the <i>TCP</i> send window buffer size. This value ranges from 4096 to 65536. The default value is 65536. • TCP Receive Buffer Size—enter the <i>TCP</i> Receive window buffer size. This value ranges from 4096 to 65536. The default value is 65536. • EBGP Hop Limit—enter the maximum hop limit value that is used during connection with external peers. This value does not have any effect on connection with internal peers. This value ranges from 1 to 255. The default value is 1. NOTE: BGP speaker accepts or attempts connection to external peers residing on network that are not directly connected but separated by the configured hop limit value. • Authentication—select the desired authentication mode for the BGP connection. The default option is None. The list contains: – None—indicates no authentication is set. – MD5—sets authentication type as Message Digest 5 (MD5) where authentication is set on a <i>TCP</i> connection between two BGP peers where each segment sent on the <i>TCP</i> connection between the peers is verified. – TCP-AO—indicates <i>TCP-AO</i> configurations for the specified BGP Peer. • Password—enter the <i>TCP</i> MD5 Authentication Password that has to be sent with all <i>TCP</i> packets originated from the peer. This value is a string of maximum size 80. NOTE: This field is enabled only when Authentication type is set as MD5 • TCP-AO MKT—enter the <i>TCP-AO MKT</i> key-id which needs to be associated with this peer. This value's range is from 0 to 255. NOTE: This field is enabled only when Authentication type is set as <i>TCP AO</i>. NOTE: This value should be the <i>MKT</i> id created using the Layer3 Management > BGP > TCP-AO Authentication > TCP-AO MKT Configuration screen

Fields (cont)	• Peer Status—select the desired state of the <i>BGP</i> peer connection. This is used to manually start or stop a <i>BGP</i> peer connection. The default option is start. The list contains: – stop—generates <i>BGP</i> stop event to manually stop the <i>BGP</i> session with the peer. The <i>BGP</i> stop event is automatically generated: • once the automatic stop feature is enabled and • the peer idle hold time exceeds its maximum threshold value. – start—generates <i>BGP</i> start event to manually initiate the <i>BGP</i> session with the peer. The <i>BGP</i> start event is generated only after configured peer idle hold time. The manual start is required for the peers damped using damp peer oscillation feature. The <i>BGP</i> start event is automatically generated after peer idle hold time to start <i>BGP</i> session in idle state when • Automatic start feature is enabled, and • <i>BGP</i> session is brought down either by automatic stop feature or through reception of invalid <i>BGP</i> message. NOTE: The peer status is internally set as auto-start when automatic start feature is enabled. • BFD Monitoring—select the <i>BFD</i> monitoring status for the <i>BGP</i> peer. The default value is set as disable. The list contains: – Disable—specifies that <i>BFD</i> monitoring is disabled. The <i>BGP</i> deregisters with <i>BFD</i> if it is already registered. – Enable—specifies that <i>BFD</i> monitoring is enabled. When enabled, <i>BGP</i> will register with <i>BFD</i> for IP path monitoring when the session state becomes Established. • VRF Name—default.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes. • Delete—deletes the selected entry.

BGP MED Configuration

Figure 34: BGP Creation

BGP MED Configuration

MED ID

*

Remote AS

0

*

Address Family

ipv4

Sub-Address Family

unicast

IP Address Prefix

*

IP Address Prefix Length

*

Intermediate AS

Direction

In

*

Value

0

*

Preference

False

VRF Name

default

*

ADD

Reset

Select	MED ID	Remote AS	AFI	SAFI	IP Address Prefix	Prefix Length	Intermediate AS	Direction	Value	Preference	Status	Context Name
Apply												

Note : Admin status should be down to configure the row

Screen Objective	This screen allows the user to configure the Multi-Exit Discriminators (<i>MED</i>) values that are to be assigned to routes learnt from <i>BGP</i> peers.
Navigation	Layer 3 Management > BGP > Multi-Exit Discriminators

Fields	• Select—select the <i>MED</i> entry for which the configurations need to be modified. • MED ID—enter the <i>MED</i> Index value which is the index value of the BGP <i>MED</i> Table. This value ranges from 1 to 100. • Remote AS—enter the remote <i>ASN</i> with which BGP <i>MED</i> is to be associated. This value ranges from 0 to 4294967295. The default value is 0. NOTE: When four-byte-<i>ASN</i> is enabled, this value ranges from 0 to 4294967295. NOTE: When four-byte-<i>ASN</i> is disabled, this value ranges from 0 to 65535. NOTE: Four-byte <i>ASN</i> can be enabled/disabled using Layer3 Management > BGP > Basic Setting> BGP Basic settings screen • Address Family / AFI—select the type of IP address prefix in the <i>NLRI</i> field in the update. The list contain: – <i>ipv4</i>—sets the type of IP address prefix as IP version 4. – <i>ipv6</i>—sets the type of IP address prefix as IP version 6. NOTE: This field should be configured before configuring the IP Address Prefix. • Sub-Address Family / SAFI—select the sub-sequent address family of IP address prefix in the <i>NLRI</i> field in the update. The default option is unicast. The list contains: – <i>unicast</i>—sets the sub-sequent address family of IP address prefix as unicast. – <i>labelledIpv4</i>—sets the sub-sequent address family of IP address prefix as labeled IP version 4. – <i>vpn4</i>—sets the sub-sequent address family of IP address prefix as <i>VPN</i> version 4. NOTE: This field should be configured before configuring the IP Address Prefix. • IP Address Prefix—enter the IP address prefix in the <i>NLRI</i> field on which local-preference policy needs to be applied. • IP Address Prefix Length—enter the length (in bits) of the IP address prefix in the <i>NLRI</i> field. This value ranges from 0 to 32 bits. The default value is 0.

Fields (cont).	• Intermediate AS—enter a list of intermediate AS numbers through which the route update is expected to travel. This is a comma separated list of AS numbers that are to be checked against the AS_PATH attribute of the updates. This value is a string of maximum size 100. • Direction—select the direction of application of the <i>MED</i> Policy. The default option is In. The list contains: – In—indicates the updates on the received routes – Out—indicates the updates that needs to be advertised to peers on the route • Value—enter the <i>MED</i> value assigned to the <i>MED</i> attribute for the route present in <i>NLRI</i>. This value ranges from 0 to 2147483647. The default value is 0. • Preference—select the preference status which denotes whether the value present in this entry takes precedence when the attribute is already present in the update message that has been received. The default option is False. The list contains: – True—indicates that the value present in this entry takes precedence when the attribute is already present in the update message that has been received – False—indicates that the value present in this entry does not take precedence • Status—select the preference status which denotes whether the value present in this entry takes precedence when the attribute is already present in the update message that has been received. The default option is False. The list contains: – Up—sets <i>MED</i> Status as UP. – Down—sets <i>MED</i> Status as Down. • VRF Name / Context Name—default.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes.

BGP Local Preference Configuration

Figure 35: BGP Local Preference Configuration

BGP Local Preference Configuration

Local Preference ID

*

Remote AS

*

Address Family

ipv4

▼

Sub-Address Family

unicast

▼

IP Address Prefix

*

IP Address Prefix Length

*

Intermediate AS

Direction

In

▼

*

Value

*

Preference

False

▼

VRF Name

default

▼

*

ADD

Reset

Select	ID	Remote AS	AFI	SAFI	IP Prefix	Prefix Length	Intermediate AS	Direction	Value	Preference	Status	Context Name
Apply												

Note : Admin status should be down to configure the row

Screen Objective	This screen allows the user to configure the Local Preference values for the routes.
Navigation	Layer 3 Management > BGP > Local Preferences

Fields	• Select—select the Local Preference Identifier entry for which the configurations need to be modified (this is a radio button in the first column of the table). • Local preference ID—enter the Local Preference ID for the route. This value ranges from 1 to 100. • Remote AS—enter the Remote <i>ASN</i> that identifies the <i>BGP</i> router to other routers and tags the routing information passed along. This value ranges from 0 to 4294967295. The default value is 0. NOTE: When four-byte-<i>ASN</i> is enabled, this value ranges from 0 to 429496729. NOTE: When four-byte-<i>ASN</i> is disabled, this value ranges from 0 to 65535. NOTE: Four Byte <i>ASN</i> can be enabled/disabled using Layer3 Management > BGP > Basic Setting > BGP Basic settings screen. • Address Family / AFI—select the type of IP address prefix in the <i>NLRI</i> field in the update. The list contains: – ipv4—sets the type of IP address prefix as IP version 4. – ipv6—sets the type of IP address prefix as IP version 6. NOTE: This field should be configured before configuring the IP Address Prefix. • Sub-Address Family / SAFI—select the sub-sequent address family of IP address prefix in the <i>NLRI</i> field in the update. The default option is unicast. The list contains: – unknown—sets the sub-sequent address family of IP address prefix as unknown which implies that any sub-sequent address family can be used for IP address prefix. – unicast—sets the sub-sequent address family of IP address prefix as unicast. – labelledIpv4—sets the sub-sequent address family of IP address prefix as labeled IP version 4. – vpn4—sets the sub-sequent address family of IP address prefix as <i>VPN</i> version 4. NOTE: This field should be configured before configuring the IP Address Prefix. • IP Address—enter the IP address prefix in the <i>NLRI</i> field. The default value is 0.0.0.0. • IP Address Prefix Length / Prefix Length—enter length (in bits) of the IP address prefix in the <i>NLRI</i> field. This value ranges from 0 to 32 bits for <i>ipv4</i> address and 0 to 128 for <i>ipv6</i> address type. By default, IP Address Prefix Length is set as 0 bits.

Fields (cont)	• Intermediate AS—enter a list of intermediate Autonomous system numbers through which the route update is expected to travel. This is a comma separated list of ASNs that are to be checked against the AS_PATH attribute of the updates. This value is a string of maximum size 10. • Direction—select the direction of application of the Local Preference Policy with which the entry is to be associated. The default option is In. The list contains: – In—indicates the updates on the received routes. – Out—indicates the updates that needs to be advertised to peers on the route • Value—enter the value assigned to the LP (Local Preference) Attribute for the route present in <i>NLRI</i>. This value ranges from 0 to 2147483647. The default value is 100. • Preference—select the preference status which denotes whether the value present in this entry takes precedence when the attribute is already present in the update message that has been received. The default option is false. The list contains: – True—indicates that the value present in this entry takes precedence when the attribute is already present in the update message that has been received. – False—indicates that the value present in this entry does not take precedence • Status—select the status of the Local Preference routes learnt by BGP peers. The default option is Down. The list contains: – Up—sets Local Preference Status as UP. – Down—sets Local Preference Status as Down. • VRF Name / Context Name—default.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes.

BGP Filter Configuration

Figure 36: BGP Filter Configuration

BGP Filter Configuration

Filter ID

*

Remote AS

Address Family

ipv4

▼

Sub-Address Family

unicast

▼

IP Address

0.0.0.0

IP Address Prefix Length

0

Intermediate AS

Direction

In

▼

Action

Deny

▼

VRF Name

default

▼

*

ADD

Reset

Select	Filter ID	Remote AS	AFI	SAFI	IP Address	Prefix Length	Intermediate AS	Direction	Action	Status	Context Name
Apply											

Note : Admin status should be down to configure the row

Screen Objective	This screen allows the user to configure an entry in Update Filter Table which contains rules to filter out updates based on the AS from which they are received, NLRI, and AS through which it had passed.
Navigation	Layer 3 Management > BGP > Filters

Fields	• Select—select the Filter Identifier entry for which the configurations need to be modified (this is a radio button in the first column of the table). • Filter ID—enter the filter index. This value ranges from 1 to 100. • Remote AS—enter the remote <i>ASN</i> that identifies the BGP router to other routers and tags the routing information passed along. This value ranges from 0 to 4294967295. The default value is 0. NOTE: When four-byte-<i>ASN</i> is enabled, this value ranges from 0 to 429496729. NOTE: When four-byte-<i>ASN</i> is disabled, this value ranges from 0 to 65535. NOTE: Four byte <i>ASN</i> can be enabled/disabled using Layer3 Management > BGP > Basic Setting>BGP Basic settings screen. • Address Family / AFI—select the type of IP address prefix in the <i>NLRI</i> field in the update. The list contain: – ipv4—sets the type of IP address prefix as IP version 4. – ipv6—sets the type of IP address prefix as IP version 6. NOTE: This field should be configured before configuring the IP Address Prefix. • Sub-Address Family / SAFI—select the sub-sequent address family of IP address prefix in the <i>NLRI</i> field in the update. The default option is unicast. The list contains: – unknown—sets the sub-sequent address family of IP address prefix as unknown which implies that any sub-sequent address family can be used for IP address prefix. – unicast—sets the sub-sequent address family of IP address prefix as unicast. – labelledIpv4—sets the sub-sequent address family of IP address prefix as labeled IP version 4. – vpnv4—sets the sub-sequent address family of IP address prefix as <i>VPN</i> version 4. NOTE: This field should be configured before configuring the IP Address Prefix. • IP Address—enter the IP address prefix in the <i>NLRI</i> field. The default value is 0.0.0.0. • IP Address Prefix Length / Prefix Length—enter length (in bits) of the IP address prefix in the <i>NLRI</i> field. This value ranges from 0 to 32 bits for ipv4 address and 0 to 128 for ipv6 address type. By default, IP Address Prefix Length is set as 0 bits.

Fields (cont)	• Intermediate AS—enter a list of intermediate AS numbers through which the route update is expected to travel. This is a comma separated list of AS numbers that are to be checked against the AS_PATH attribute of the updates. This value is a string of maximum size 10. • Direction—select the direction of application of filters with which the entry is to be associated. The default option is In. The list contains: – In—indicates the updates on the received routes – Out—indicates the updates that needs to be advertised to peers on the route • Action—select the status that controls addition or deletion of the non bgp routes. The default option is Deny. The list contains: – Allow—allows addition of non-BGP routes. – Deny—denies addition of non-BGP routes. • Status—select the status of the routes learnt by BGP peers. The default option is Down. The list contains: – Up—sets BGP Filter Status as UP – Down—sets BGP filter Status as Down. • VRF Name / Context Name—default.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes.

BGP Route Aggregation Configuration

Figure 37: BGP Route Aggregation Configuration

BGP Route Aggregation Configuration

ID

*

Address Family

ipv4

Sub-Address Family

unicast

IP Address Prefix

*

IP Address Prefix Length

*

Route Advertise

Summary Only

As-Set

Disable

Suppress-Map

Advertise-Map

Attribute-Map

VRF Name

default

*

ADD

Reset

Select	ID	AFI	SAFI	IP Address Prefix	Prefix Length	Route Advertise	As-Set	Suppress-Map	Advertise-Map	Attribute-Map	Context Name
Delete											

Screen Objective	This screen allows the user to configure the aggregation of the routing information. This creates an aggregate entry in a <i>BGP</i> or multiprotocol BGP routing table if any more-specific <i>BGP</i> or multiprotocol <i>BGP</i> routes are available that fall in the specified range. The entries in the table specify 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; otherwise, it will not be set.
Navigation	Layer 3 Management > BGP > Route Aggregation

440

Fields	• Select—select the neighbor for which the configurations need to be reapplied. • ID—enter the index to <i>BGP</i> Route Aggregation table. This value ranges from 1 to 100. • Address Family / AFI—select the type of IP address prefix in the <i>NLRI</i> field in the update. The list contain: – ipv4—sets the type of IP address prefix as IP version 4. – ipv6—sets the type of IP address prefix as IP version 6. NOTE: This field should be configured before configuring the IP Address Prefix. • Sub-Address Family / SAFI—select the sub-sequent address family of IP address prefix in the <i>NLRI</i> field in the update. The default option is unicast. The list contains: – unknown—sets the sub-sequent address family of IP address prefix as unknown which implies that any sub-sequent address family can be used for IP address prefix. – unicast—sets the sub-sequent address family of IP address prefix as unicast. – labelledIpv4—sets the sub-sequent address family of IP address prefix as labeled IP version 4. – vpn4—sets the sub-sequent address family of IP address prefix as <i>VPN</i> version 4. NOTE: This field should be configured before configuring the IP Address Prefix. • IP Address—enter the IP address prefix in the <i>NLRI</i> field. • IP Address Prefix Length / Prefix Length—enter the length (in bits) of the IP address prefix in the <i>NLRI</i> field. This value ranges from 0 to 32 for ipv4 address and 0 to 128 bits for ipv6 address. • Route Advertise—select the route updates that should be sent to the peers. The default option is Summary-only. The list contains: – Summary Only—indicates that only the summarized route has to be advertised to peers. – All—indicates that both the summary and the more-specific routes based on which the summary entry was generated, have to be advertised to the peers.

Fields (cont)	• As-Set—select the generation status of autonomous system set path information. The default option is Disable. The list contains – Enable—enables the generation of AS set path information. – Disable—disables the generation of AS set path information. • Suppress-Map—enter the name for suppress route-map. The route map contains the rules for suppressing the routes while aggregation. When suppress-map configuration is used along with summary-only option, summary-only configuration does not 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 of maximum size 20. • Advertise-Map—enter the name for advertise route-map. The route map contains the rules for advertising the routes during aggregation. 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 of maximum size 20. • VRF Name / Context Name—default.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes.

BGP Timer Configuration

Figure 38: BGP Timer Configuration

BGP Timer configuration

Select	Address Type	Ip Address	KeepAlive	Hold time	Route Advertisement interval	Min As Origination interval	Connect retry interval	IdleHold interval	DelayOpen interval	Context Name

Apply

Screen Objective	This screen allows the user to configure the timer related parameters for the peer.
Note	The <i>BGP</i> peer timer entry is created ONLY for the peer entries created in the Neighbor Configuration screen. Generate peer entries before creating <i>BGP</i> Timer configuration.

Navigation	Layer 3 Management > BGP > Timer
Fields	• Address Type—displays the address type of the remote peer. This is a read-only field. The type can be: – ipv4—denotes the remote peer IP address type as IP version 4. – ipv6—denotes the remote peer IP address type as IP version 6. • Ip Address—displays the IP address of the <i>BGP</i> peer; a read-only field. • Keep Alive—enter the maximum time interval between successive keepalive messages exchanged between two peers. This value ranges from 0 to 21845 seconds. The optimal value is 30 seconds. NOTE: Periodical KEEPALIVE messages will be sent to the peer after the BGP connection is established. • Hold time—enter the timer interval that a BGP will wait, before it decides that a connection to the peer is to be turned down. The system declares a peer as dead, after ensuring that a keepalive message is not received within this time period from the peer. This value ranges from 3 to 65535 seconds or 0. The optimal value is 90. • Route Advertisement interval—enter the minimum interval between router advertisements (in seconds). This value ranges from 1 to 65535 seconds. The optimal value is 30 seconds. This is a read-only field. • Min As Origination interval—enter minimum time between advertisements of changes within the speaker's AS (in seconds). This value ranges from 1 to 65535 seconds. The default value is 15. • Connect retry interval—enter the time (in seconds) for waiting before the router attempts to reconnect with the <i>BGP</i> neighbor after failing to connect. This value ranges from 1 to 65535 seconds. The default value is 120. • Idle Hold interval—enter the time interval during which the <i>BGP</i> peer is held in idle state prior to the next automatic restart. This value ranges from 1 to 65535 seconds. The default value is 60. For each successive damp oscillations, the current IdleHold time value will be increased twice its previous value. This will happen through internal logic. <i>The IdleHold Interval can be configured if either:</i> – Automatic start feature is enabled, or – Damp peer oscillation feature is enabled NOTE: If both damp peer oscillation and automatic start features are disabled, the existing value is always set instead of the newly configured value.

Fields (cont)	• Delay Open interval—enter the amount of time the <i>BGP</i> peer should postpone sending open message to the remote peer. This delay allows the remote peer to send the first open message. This value ranges from 0 to 65535 seconds. The default value is 0 seconds. NOTE: This time can be configured only if the Delay Open status is set as enabled. Otherwise, the existing value is always set instead of the newly configured value. • Context Name—default.
Buttons	• Apply—modifies attributes for the selected entry and saves the changes.

BGP GR Settings

Figure 39: BGP GR Settings

BGP GR Settings

GR Admin Status	Enabled ▾
Restart Time	90
Selection Deferral timer Value	60
Stale Timer Interval	150
Restart support	Planned ▾
Restart Reason	Software restart ▾
Apply Reset	

Note : WHEN BGP GR ADMIN STATUS is enabled None Option cannot be set for Restart Support.

Screen Objective	This screen allows the user to configure the Graceful Restart (<i>GR</i>) settings of the <i>BGP</i>. <i>GR</i> capability in a router which allows forwarding of data packets to continue along known routes, while the routing protocol information is being restored following a processor switchover. When <i>GR</i> is enabled, peer networking devices are informed, through protocol extensions prior to the event, of the stateful switch over-capable routers ability to perform <i>GR</i>. When a switch over occurs, the peer will continue to forward to the switching over router as instructed by the <i>GR</i> process for each particular protocol, even though in most cases the peering relationship needs to be rebuilt. Essentially, the peer router will give the switching over router a "grace" period to re-establish the neighbor relationship, while continuing to forward to the routes from that peer.
Navigation	Layer 3 Management > BGP > GR Settings

Fields	• GR Admin Status—select the <i>GR</i> capability status in the <i>BGP</i> speaker. The default option is Disabled. The list contains: – Enabled—enables the <i>GR</i> capability in the <i>BGP</i> speaker. – Disabled—disables the <i>GR</i> capability in the <i>BGP</i> speaker. NOTE: To set the <i>GR</i> parameters, the <i>BGP GR</i> admin status should be disabled. • Restart Time—enter the time, in seconds, for the <i>BGP</i> session to be re-established after a restart. The default value should be less than or equal to Hold Time carried in open message. This value ranges from 1 to 4096 seconds. The default value is 90 seconds. • Selection Deferral timer Value—enter the upper limit time until which a router defers its route selection. This timer value should be large enough for providing all peers of the Restarting Speaker with enough time to send all routes to the Restarting Speaker. This value ranges from 60 to 1800 seconds. The default value is 60. • Stale Timer Interval—enter the time, in seconds, for the <i>BGP</i> session to be re-established after a restart. The default value should be less than or equal to Hold Time carried in open message. This value ranges from 1 to 4096 seconds. The default value is 90 seconds. • Restart support—select the router support for the <i>BGP</i> graceful restart feature. The default option is None. The list contains: – None—sets Restart Support as None which implies that Restart support is not provided for the Graceful Restart feature. – Planned—sets Restart Support as Planned. – Both—sets Restart Support as both planned and unplanned. • Restart Reason—select the router restart reason code of the <i>BGP</i> graceful restart feature. The default option is Software restart. The list contains: – Unknown—sets Restart Reason as unknown e.g. this code is to be used when a system restarts due to unplanned events (restarting after a crash). – Software restart—sets Restart Reason as Software restart; this is to be used where a system restarts due to software restart. – Software upgrade—sets restart reason as software upgrade; to be used where a system restarts due to reloading / upgrading of software.
Buttons	• Apply—modifies attributes for the selected entry and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs.

TCP-AO MKT Configuration

Figure 40: TCP-AO MKT Configuration

TCP-AO MKT Configuration

KEY-ID		*
Receive-Key-ID		*
Crypto Algorithm	HMAC-SHA-1	▼
Password		*
TCP-OPTIONS	INCLUDE	▼
VRF Name	default	▼ *
ADD Reset		

Select	KEY-ID	Receive-Key-ID	Crypto Algorithm	Password	TCP-OPTIONS	Context Name
Apply Delete						

Screen Objective	This screen allows the user to configure <i>TCP-AO MKT</i> (Authentication Option Master Key Tuple) in the specified BGP instance.
Navigation	Layer 3 Management > BGP > TCP-AO Authentication
Fields	• Select—select the neighbor for which the configurations need to be modified. • KEY-ID—enter the local ASN. This value ranges from 1 to 4294967295. The default value is 1. • Receive-Key-ID—enter the Receive Key-id of the <i>MKT</i>. The <i>MKT</i> that is ready at the sender to be used to authenticate received segments is indicated to the peer by filling the receive key id of the <i>MKT</i> of the <i>TCP-AO</i> OPTION in the TCP header. This value ranges from 0 to 255. • Crypto Algorithm—select the crypto Algorithm used for <i>TCP-AO</i> (Authentication Option Master Key Tuple) in the specified BGP instance. <i>MAC</i> or <i>KDF</i> calculation. <i>TCP-AO</i> uses cryptographic algorithms to convert MKTs, which can be shared across connections into unique traffic keys for each connection. These are called Key Derivation Functions (<i>KDFs</i>) and are specified in RFC5926. The default option is hmac-sha-1. The list contains: – HMAC-SHA-1—sets algorithm type as HMAC-SHA-1. – AES-128—sets algorithm type as AES-128.

Fields (cont)	• Password—enter the password/ Master Key corresponding to the <i>MKT</i>. This is an octet string value with the maximum size 80 • TCP-OPTIONS—sets the exclude <i>TCP</i> option which excludes the options other than <i>TCP-AO</i> during <i>MAC</i> calculation. If this is not set, <i>TCP-AO</i> MAC will be calculated on <i>TCP</i> segment including all other <i>TCP</i> options. – Exclude—excludes <i>TCP</i> options other than <i>TCP-AO</i> during <i>MAC</i> calculation. – Include—includes all <i>TCP</i> options; while calculating <i>TCP-AO</i>, <i>MAC</i> will be calculated on <i>TCP</i> segment including all other <i>TCP</i> options. • VRF Name / Context Name—default.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes. • Delete—deletes the selected entry.

Peer Group Configuration

Figure 41: Peer Group Configuration

PeerGroup Configuration

PeerGroup Name

*

Remote AS

0

Hold Time

90

Keep Alive Time

30

Connect Retry Interval

30

Min AS Originator Interval

15

Min Route Advertisement Interval

5

Automatic Start

Disable

▼

Automatic Stop

Disable

▼

Idle Hold Time

60

Damp Peer Oscillations

Disable

▼

Delay Open

Disable

▼

Delay Open Interval

0

Max Prefix Limit

100

Connect Retry Count

5

VRF Name

▼

*

ADD

Reset

Apply

Fields	• Select—select the neighbor for which the configurations need to be modified. • Peer Group Name—enter the Peer Group Name for configuring <i>BGP</i> peer group. The members of this peer group will inherit the characteristics configured with this screen. This value is a string of maximum size 20. NOTE: For Peer Address with external <i>AS</i>, route reflector client cannot be set as Client. • Remote AS—enter the Remote <i>ASN</i> associated with the <i>BGP</i> peer group. This value ranges from 1 to 4294967295. NOTE: When four-byte <i>ASN</i> is enabled, this value ranges from 1 to 4294967295. NOTE: When four-byte <i>ASN</i> is disabled, this value ranges from 1 to 65535. NOTE: Four-byte <i>ASN</i> can be enabled/disabled using Layer3 Management > BGP > Basic Setting > BGP Basic settings screen. • Hold time—enter the timer interval for the Hold Time configured for the BGP speaker with all peers configured for this peer group. This value is placed in an OPEN message sent to the peers by the <i>BGP</i> speaker. This value ranges from 3 to 65535 seconds or can be configured as zero. If it is configured as 0, the Hold Time will be not established with the peer. The default value is 90 seconds. • Keep Alive Time—enter the Keep Alive Time (in seconds) for the <i>BGP</i> speaker with all peers configured for this peer group. The value of this object will only determine the KEEPALIVE messages frequency relative to the Hold Time. The keep-alive value must always be less than the configured hold-time value A reasonable maximum value for this timer is one third of the Hold Time value. If this value is zero (0), no periodical KEEPALIVE messages are sent to the peers after the <i>BGP</i> connection is established. This value ranges from 1 to 21845 seconds. The default value is 30. • Connect Retry Interval—enter the Connect Retry Interval (in seconds) for the peers in this peer group. This is the time interval after which a transport connection with a peer is re-initiated. This value ranges from 1 to 65535 seconds. The default value is 30. • Min AS Originator Interval—enter the AS Originator Interval for the peers in this peer group. This is the time-interval (in seconds) for spacing successive route-updates originating within the same AS. The default value is 15 seconds.

Fields (cont)	• Min Route Advertisement Interval—enter the Min Route Advertisement Interval for the peers in this peer group. This is the time-interval (in seconds) for spacing advertisement of successive external route-updates to the same destination. This value ranges from 1 to 65535 seconds. The default value is 30 seconds for <i>EBGP</i> connections and 5 seconds for <i>IBGP</i> connections. • Automatic Start—select the Automatic Start status for the <i>BGP</i> session with the associated peers in the peer group. The default option is Disable. The list contains: – Disable—disables the <i>BGP</i> session with the associated peer automatically. The <i>BGP</i> session with the peer has to be manually initiated. – Enable—starts the <i>BGP</i> session with the associated peer automatically. The peer session is automatically started in idle state, after a <i>BGP</i> Peer session is brought down either by Auto stop or through reception of invalid <i>BGP</i> message. The <i>BGP</i> session is automatically started after an interval specified by idle hold timer. • Automatic Stop—select the status to enable/disable the auto stop option for stopping the <i>BGP</i> peer and <i>BGP</i> connection automatically. The default option is Disable. The list contains: – Disable—disables the <i>BGP</i> session with the associated peer automatically. When Automatic Stop is disabled, the Connect Retry Count Value is set to 0. – Enable—stops the <i>BGP</i> session with the associated peer automatically. After an automatic stop, the peer connection needs to be re-initiated manually by the administrator. • IdleHold interval—enter the time interval during which the <i>BGP</i> peer is held in idle state prior to the next automatic restart. This value ranges from 1 to 65535 seconds. The default value is 60. <i>The IdleHold Interval can be configured if either:</i> – Automatic start feature is enabled, or – Damp peer oscillation feature is enabled NOTE: <i>If both damp peer oscillation and automatic start features are disabled, the existing value is always set instead of the newly configured value.</i> • Damp Peer Oscillations—select the status of the Damp Peer Oscillation option that specifies that the implementation engages additional logic to dampen the oscillations of <i>BGP</i> peers in the face of series of automatic start and automatic stop operations in the IDLE state. The default option is Disable. The list contains: – Disable—disables the Damp Peer Oscillation option. – Enable—enables the Damp Peer Oscillation option.

Fields (cont)	• Delay Open—select the status of the delay in sending the first OPEN message to the <i>BGP</i> peer for a specific time period. The default option is Disable. The list contains: – Disable—disables the Delay Open option for sending open messages, which implies that open messages are sent to the remote <i>BGP</i> peer without any delay. – Enable—enables Delay Open option for sending open messages to the remote <i>BGP</i> peer for a configured open delay time period. This delay allows the remote peer to send the first open message. • Delay Open Interval—enter the Delay Open Interval which is the amount of time for which the <i>BGP</i> peer should postpone sending the OPEN message to the remote peer. This value ranges from 0 to 65535. The default value is 0. NOTE: This field can be configured only if the Delay Open option is enabled. • Max Prefix Limit—enter the maximum number of address prefixes that the BGP Peer is willing to accept from the neighbor. This value ranges from 1 to 2147483647. The default value is 100. NOTE: The default value is calculated based on the following formula: Maximum number of routes in the routing table / Maximum number of peers supported by <i>BGP</i>. • Connect Retry Count—enter the retry count which specifies the number of times the <i>BGP</i> peer should try to establish a TCP-connect issue with its neighboring peers. If the <i>BGP</i> Peer exceeds the maximum count value, automatic stop event takes place and the BGP Peer is brought to the Idle State. This value ranges from 1 to 50. The default value is 5. • VRF Name / Context Name—default.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes.

Neighbor Configuration—Peer Group 2

Figure 42: Neighbor Configuration—Peer Group 2

Neighbor Configuration

PeerGroup Name
EBGP Multit HOP
EBGP Hop Limit
NEXT HOP
RFL
TCP Send Buffer Size
TCP Recieve Buffer Size
Community Send Status
Extended Community Send Status
PeerGroup Connection Passive
Default Originator
Activate MP Capability
Deactivate MP Capability
In RouteMap Name
Out RouteMap Name
In PrefixList Name
Out PrefixList Name
Orf Type
Orf Mode
Bfd Monitoring
VRF Name

*
Disable ▾

AUTOMATIC ▾
NONCLIENT ▾

Send ▾
Send ▾
Disable ▾
Disable ▾
IPV4unicast ▾
IPV4unicast ▾

☒ Address-Prefix
none ▾
disable ▾
default ▾*

Select	PeerGroup Name	EBGP Multit HOP	EBGP Hop Limit	NEXT HOP	RFL	TCP Send Buffer Size
☒	aa	Disable ▾	1	AUTOMATIC ▾	NONCLIENT ▾	65536

Community Send Status	Extended Community Status	PeerGroup Connection Passive	Default Originator	Activate MP Capability	Deactivate MP Capability	In RouteMap Name	Out RouteMap Name
Send ▾	Send ▾	Disable ▾	Disable ▾	IPV4unicast ▾	IPV4unicast ▾		

In PrefixList Name	Out PrefixList Name	Orf Type	Orf Mode	BFD Monitoring	Context Name
			none ▾	enable ▾	default

Screen Objective	This screen allows the peer group name to configure the parameters for <i>BGP</i> peer associated with the peer group.
Navigation	Layer 3 Management > BGP (cont.) > Peer Group 2
Fields	• Select—select the neighbor for which the configurations need to be modified. • Peer Group Name—enter the Peer Group Name for configuring <i>BGP</i> peer group. The members of this peer group will inherit the characteristics configured with this screen. This value is a string of maximum size 20. • EBGP Multi HOP—select the status of the <i>EBGP</i> Multi HOP. The default option is Disable. The options include: – Disable—disables BGP to establish connection with external peers residing on networks that are not directly connected. If <i>EBGP</i>—Multi HOP is disabled and external BGP peers are indirectly connected, BGP peer session will not be established. – Enable—enables BGP to establish connection with external peers residing on networks that are not directly connected. If <i>EBGP</i> peer are not connected directly, <i>EBGP</i>—Multi HOP is enabled to initiate the connection with that external peer. NOTE: This configuration is effective only when <i>EBGP</i> peers are added to this peer group. • EBGP Hop Limit—enter the <i>EBGP</i> Hop Limit value that is used during connection with external peers. BGP speaker accepts or attempts connection to external peers residing on network that are not directly connected but separated by the configured Hop Limit value. This value ranges from 0 to 255. The default value is 1. NOTE: This configuration is effective only when <i>EBGP</i> peers are added to this peer group. • NEXT HOP—select whether the next hop attribute sent in the update message to the peers in this peer group has to be generated automatically or self. This is useful in non-meshed networks where <i>BGP</i> neighbors may not have direct access to all other neighbors on the same IP subnet. The default option is AUTOMATIC. The list contains: – AUTOMATIC—generates the next hop based on the IP address of the destination and the present next hop in the route information. – SELF—enables <i>BGP</i> to send itself as the next hop for advertised routes.

Fields (cont)	• RFL—select Route Reflector Client (<i>RFL</i>) status of the peer. This status is used to define client and non-client peers when implementing route reflection. The default option is NONCLIENT. The list contains: – NONCLIENT—configures the peer as non-client peer, which denotes that the peer is outside the cluster. – CLIENT—configures the peer as client peer, which denotes that the peer is within the cluster <i>The route reflection mechanism operates as follows:</i> – A cluster system acting as route reflector sends a route to all client peers within the cluster if the route is received from a non-client peer. – The cluster system acting as route reflector sends a route to all non-client peers and all client peers except the originator if the route is received from a client peer. • TCP Send Buffer Size—enter the <i>TCP</i> window size on the sender side for all peers in this peer group. This value ranges from 4096 to 65536. The default value is 65536. • TCP Receive Buffer Size—enter the <i>TCP</i> window size on the receiver side for all peers in this peer group. This value ranges from 4096 to 65536. The default value is 65536. • Community Send Status—select the Community Send Status attribute for the peers in this peer group. The default option is Send. The list contains: – None—sets Community Send Status as none. – Send—sends a community attribute to a <i>BGP</i> neighbor and enables advertisement of community attributes (standard/extended) to peers – DontSend—disables advertisement of standard community attributes to peer. • Extended Community Send Status—select the status of Extended Community Send attribute for the peers in this peer group. The <i>BGP</i> extended community is used to label <i>BGP</i> routing information for controlling the distribution of the information. The default option is send. The list contains: – None—sets Extended Community Send Status as none. – Send—sends a Extended Community attribute to a <i>BGP</i> neighbor and enables advertisement of community attributes (standard/extended) to peers – DontSend—disables advertisement of Extended Community attributes to peer.

Fields (cont)	• Peer Group Connection Passive—select the status of the Peer Group Connection Passive. The default option is Disable. The options include: – Enable—sets the Peer Group Connection as passive. <i>BGP</i> speaker waits for the remote peer to initiate the session with the peer. – Disable—sets the Peer Group Connection as active. <i>BGP</i> speaker initiates the session with the peer. • Default Originator—select the status of the advertisement of the default route to all peers in this peer group. The default option is Disable. The options include: – Enable—enables the advertisement of the default route to all peers in this peer group. – Disable—disables the advertisement of the default route to all peers in this peer group. NOTE: This field overrides the global default route configuration and always sends a default route to the peer with self next-hop. This advertisement occurs irrespective of the presence of default route in <i>FDB</i>. • Activate MP Capability—select the option to activate corresponding MP Capability. If any MP Capability is activated, then this capability should be negotiated while establishing session with the peers in this group. The default option is IPV4unicast. The list contains: – IPV6unicast—activates the corresponding MP Capability for IPV6 unicast address. – IPV4unicast—activates the corresponding MP Capability for IPV4 unicast address. • Deactivate MP Capability—select the option to Deactivate corresponding MP Capability. If any MP Capability is deactivated, then this capability should be negotiated while establishing session with the peers in this group. The default option is IPV4unicast. The list contains: – IPV6unicast—deactivates the corresponding MP Capability for IPV6 unicast address. – IPV4unicast—deactivates the corresponding MP Capability for IPV4 unicast address. • In RouteMap Name—enter the name of the route map for this peer group entry. This value is a string of maximum size 20. • Out RouteMap Name—enter the name of the out route map for this peer group entry. This value is a string of maximum size 20. • In PrefixList Name—enter the In PrefixList Name for the neighbor. This value is a string of maximum size 20. • Out PrefixList Name—enter the Out PrefixList Name for the neighbor. This value is a string of maximum size 20.

Fields (cont)	• ORF Type—click to enable address prefix-based Outbound Route Filter (<i>ORF</i>) for the specified <i>BGP</i> peer group. • ORF Mode—select the <i>ORF</i> Capability Support Mode for the specified peer group entry. The default option is none. The list contains: – none—disables <i>ORF</i> capability. – receive—enables <i>ORF</i> receive capability. – send—enables <i>ORF</i> send capability. – both—enables both send and receive <i>ORF</i> Capability. • BFD Monitoring—select the <i>BFD</i> monitoring status for the <i>BGP</i> peer. The default value is set as disable. The list includes: – Enable—specifies that <i>BFD</i> monitoring is enabled. When enabled <i>BGP</i> will register with <i>BFD</i> for IP path monitoring when the session state becomes established. – Disable—specifies that <i>BFD</i> monitoring is disabled. The <i>BGP</i> de-registers with <i>BFD</i> if it is already registered. • VRF Name / Context Name—default.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes. • Delete—deletes the selected entry.

Peer Addition

Figure 43: Peer Addition

Peer Addition

PeerGroup Name *

Address Family IPV4 ▾

Peer Address *

VRF Name default ▾ *

Select	PeerGroup Name	Peer Address Family	Peer Address	Context Name
☒	aa	IPV4 ▾	10.0.0.0	default

Screen Objective	This screen allows the user to add a configured peer to a peer group.
Note	This screen can be configured only if a peer and a peer group are created. - To create a Peer, go to Layer 3 Management > BGP > Neighbors > Neighbor Configuration screen. - To create a Peer group, go to Layer 3 Management > BGP (cont.) > Peer 1 or Layer 3 Management > BGP (cont.) > Peer Group 2 > Neighbor Configuration
Navigation	Layer 3 Management > BGP (cont.) > Peer Addition with Peer Group
Fields	Select—enter a Peer Group Name. Peer Group Name—enter the Peer Group Name to which the peer has to be added. This value is a string of maximum size 20. Address Family/ Peer Address Family—select the Address Family of the peer. The default option is IPV4. - IPV6—specifies that the peer belongs to the IPV6 Address Family - IPV4—specifies that the peer belongs to the IPV4 Address Family. Peer Address—enter the remote IP address of the <i>BGP</i> peer. VRF Name / Context Name—default.
Buttons	Add—adds and saves new configuration. Delete—deletes the selected entry.

Clear BGP

Figure 44: Clear BGP

Clear BGP

IPV4

☐

IPV6

☐

ALL

☐

EXTERNAL

☐

Address Family

IPV4 ▼

PEER ADDRESS

☒

PEER GROUP

☐

AS NUM

☐

Flap Statistics

☐

Dampening

☐

Soft

None ▼

VRF Name

Apply

Screen Objective	This screen allows the user to reset the <i>BGP</i> connection dynamically for inbound and outbound route policy. The inbound routing tables are updated dynamically or by generating new updates using stored update information.
Navigation	Layer 3 Management > BGP (cont.) > Clear BGP
Fields	IPV4—click to reset the <i>BGP</i> connection dynamically for all IPv4 address family peers. IPV6—click to reset the <i>BGP</i> connection dynamically for all IPv6 address family peers. ALL—click to reset all <i>BGP</i> peers. EXTERNAL—click to reset all external peers. Address Family—select the address family for which the BGP connection needs to be reset. - IPV6—clears all <i>BGP</i> connections in IPv6 Address Family. - IPV4—clears all <i>BGP</i> connections in the IPv4 Address Family. PEER ADDRESS—click the option button to select the PEER ADDRESS for which the <i>BGP</i> Connection needs to be reset and enter the Peer Address.

Fields	• PEER GROUP—click the option button to select the PEER GROUP for which the <i>BGP</i> Connection needs to be reset and enter the Peer Group name. This value is a string of maximum size 20. • AS NUM—click the option button to select the AS number for which the <i>BGP</i> Connection needs to be reset and enter the AS number. • Flap Statistics—click to select the option to clear the route Flap Statistics for the <i>BGP</i>. Enter the required IPv4 / IPv6 address and the Prefix Length to clear the route Flap Statistics. • Dampening—click to select the option to clear the dampening configuration for the <i>BGP</i>. Enter the required IPv4 / IPv6 address and the Prefix Length to clear the Dampening statistics. • Soft—select the Soft clear which is automatically assumed when the route refresh capability is supported. – None—does not initiate inbound soft reconfiguration. – In—initiates 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 – Out—initiates outbound soft configuration which does not have any memory overhead and does not require any pre-configuration. An outbound reconfiguration can be triggered on the other side of the BGP session to make the new inbound policy take effect. – Both—initiates both inbound and outbound soft reconfiguration. – In Prefix-filter—initiates soft reconfiguration of in Prefix-filter. • VRF Name—default.
Buttons	• Add—adds and saves new configuration.

BGP Route Map Settings

Figure 45: BGP Route Map Settings

BGP Route Map Settings

Peer Address

Route Map Direction IN ▾

Route Map Name

VRF Name ▾*

Select	Peer Address	Route Map Direction	Route Map Name	Context Name
☒	10.0.0.0	IN ▾	aa	default

Screen Objective	This screen allows the user to configure the <i>BGP</i> route map for a neighbor.
Note	Route map can be configured only if a neighbor is created using the Layer 3 Management > BGP > Neighbors > Neighbor Configuration screen.
Navigation	Layer 3 Management > BGP (cont.) > Route Map
Fields	Select—click to select the Peer Address for which the configuration needs to be modified or the route map to be deleted. Peer Address—enter the remote IP address of the <i>BGP</i> peer. Route Map Direction—select the direction of the route map. The default option is IN. The list contains. - IN—enables Route Map for inbound routes. This applies the route map rules for incoming routes from the peer. - OUT—enables Route Map for outbound routes. This applies the route map for the advertising routes to the peer. Route Map Name—enter the remote IP address of the <i>BGP</i> peer. VRF Name / Context Name—default.
Buttons	Add—adds and saves new configuration. Reset—resets to default value for respective fields and discards all user inputs. Apply—modifies attributes for the selected entry and saves the changes. Delete—deletes the selected entry.

Peer Orf Config

Figure 46: Peer Orf Config

Peer Orf Config

Select	Peer Address	Orf Type	Send Mode	Receive Mode	Send Mode Rx-Status	Receive Mode Rx-Status	In Prefix List Name	Out Prefix List Name	Vrf Name
☐	10.0.0.0	Address-Prefix	enable ▾	enable ▾	Not Received	Not Received	filter1		default

Screen Objective	This screen allows the user to configure the Outbound Route Filter (<i>ORF</i>) filters.
Navigation	Layer 3 Management > BGP (cont.) > Peer ORF Config
Fields	• Select—click to select the peer address for which the <i>ORF</i> configuration needs to be applied. • Peer Address—enter the remote IP address of the <i>BGP</i> peer. • ORF Type—displays outbound route filter (<i>ORF</i>) Type as address prefix-based for the specified <i>BGP</i> peer group. • Send Mode—select the send mode status for the specified remote IP address of the <i>BGP</i> peer. The default option is enable. The list contains: – enable—enables the <i>ORF</i> filter send mode. – disable—disables the <i>ORF</i> filter send mode. • Receive Mode—select the receive mode status for the specified remote IP address of the <i>BGP</i> peer. The default option is enable. The list contains: – enable—enables the <i>ORF</i> filter receive mode. – disable—disables the <i>ORF</i> filter receive mode. • Send Mode Rx-Status—displays the send mode Rx-Status for the specified remote IP address of the <i>BGP</i> peer. • Receive Mode Rx-Status—displays the receive mode Rx-Status for the specified remote IP address of the <i>BGP</i> peer. • In Prefix List Name—enter In Prefix List Name for neighbor. This value is a string of maximum size 20. • Out Prefix List Name—enter Out Prefix List Name for neighbor. This value is a string of maximum size 20. • VRF Name / Context Name—default.
Buttons	• Apply—modifies attributes for the selected entry and saves the changes.

ORF Filters

Figure 47: ORF Filters

Orf Filters

Peer Addr	Seq No	Action	Address Prefix	Prefix-Len	Min Prefix-Len	Max Prefix-Len	Vrf Name

Screen Objective	This screen displays the <i>ORF</i> (Outbound Route Filtering) entries created already in the system.
Navigation	Layer 3 Management > BGP (cont.) > ORF Filters
Fields	• Peer Addr—displays the remote IP address of the <i>BGP</i> peer. • Seq No—displays the sequence number of an entry. This value ranges from 1 to 4294967295. • Action—displays the filter action of the packet route-update for the associated sequence number. The default option is permit. The list contains: – Permit—allows packet route-update with the associated sequence number value to pass the filter. – Deny—denies the packet route-update with the associated sequence number value to pass the filter • Address Prefix—displays the IPv4 / IPv6 address prefix for the ip prefix-list entry. • Prefix-Len—displays the prefix length for IPv4 / IPv6 address prefix for the IP prefix-list entry. This value ranges from 1 to 32 for IPv4 address and from 0 to 128 for IPv6 address. • Min Prefix-Len—displays the minimum prefix length to be matched. This value ranges from 1 to 32 for IPv4 address and from 0 to 128 for IPv6 address. Minimum prefix length must be greater than prefix length and less than or equal to max prefix length. • Max Prefix-Len—displays the maximum prefix length to be matched. This value ranges from 1 to 32 for IPv4 address and from 0 to 128 for IPv6 address. Maximum prefix length must be greater than prefix length and greater than or equal to min prefix length. • VRF Name / Context Name—default.

Filtering

Figure 48: BGP Filtering Configuration

BGP Filtering Configuration

Common Preference Value

Route Map Name*

Filter Type*

Preference Value (distance only*)

checked	Filter Name	Filter Type	Filter Value
☒	aa	Distance	122

Screen Objective	This screen displays the <i>BGP</i> Filtering Configuration.
Navigation	Layer 3 Management > BGP (cont.) > Filtering
Fields	• Common Preference Value—displays the Common Preference Value. • Route Map Name—displays the sequence number of an entry. This value ranges from 1 to 4294967295. • Filter type—displays the filter type. The default option is permit. The list contains: – Distance – Distribute in – Distribute out • Preference Value (distance only*)—displays the IPv4 / IPv6 address prefix for the ip prefix-list entry. • VRF Name / Context Name—default.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes. • Delete—deletes the selected entry.

20.7. BGP4 (Beta Version)

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

BGP4 (Border Gateway Protocol) provides a set of mechanisms for supporting *CIDR* (Classless Inter - Domain Routing). These mechanisms include support for advertising a set of destinations as an IP prefix and eliminating the concept of network class within *BGP*. *BGP4* also introduces mechanisms which allow aggregation of routes, including aggregation of *AS* paths.

To access **BGP4** screens, go to **Layer 3 Management > BGP4**

Confederation Settings

Figure 49: Confederation Settings

Confederation settings

Peer AS NO

Confederation status

enable

VRF Name

default

ADD

Reset

Select	Peer AS number	Status	Context Name
☒	22	Enable	default

Delete

Screen Objective	This screen allows the user to configure the confederation status of the <i>BGP</i> peer for the specified <i>VRF</i> instance.
Navigation	Layer 3 Management > BGP4 > Confederations

Fields	• Select—select the Peer <i>ASN</i> and delete the confederation. • Peer AS NO—enter the peer <i>ASN</i> for which the confederation status needs to be configured. This value ranges from 1 to 65535. The <i>ASN</i> identifies the BGP router to other routers and tags the routing information passed along. • Confederation status / Status—select the status of the <i>BGP</i> confederation identifier which specifies the confederation to which the autonomous systems belong to. The default option is enable. The list contains: – Enable—configures the <i>BGP</i> confederation identifier which specifies the confederation to which the autonomous systems belong. – Disable—deletes the configured <i>BGP</i> confederation identifier. • VRF Name / Context Name —default.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Delete—deletes the selected entry.

BGP RFD Settings

Figure 50: BGP RFD Settings

BGP RFD Settings

Halflifetime	900
Reuse Value	750
Suppress Value	2000
Maximum suppress time	3600
Decay timer granularity	1
Reuse Timer granularity	15
Reuse Array index	1024
VRF Name	default *

Screen Objective	This screen allows the user to configure <i>RFD</i> (Route Flap Dampening) parameters.

Note	The RFD parameters can be configured only if, - Global admin status of the <i>BGP4</i> is set as disabled using the Layer 3 Management > BGP > Basic Setting > BGP Basic Settings screen. - Local AS of <i>BGP4</i> is configured using the Layer 3 Management > BGP > GP VRF Creation
Navigation	Layer 3 Management > BGP > RFD
Fields	Half life time—enter the time duration 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 dampening algorithm calculates penalty for all 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 2700 seconds. The default value is 900. Reuse Value—enter the reuse value below which the suppressed route will be reused. This value ranges from 100 to 1999. If the penalty for a flapping route falls below this value, the route is reused. The unsuppressing of routes occurs at 10-seconds increments. The default value is 750. NOTE: Reuse Value can be configured only if the Half Life Time value is configured. Suppress Value—enter the suppress value above which the route will be suppressed. The route is suppressed if the penalty associated with the route exceeds this value. This value ranges from 2000 to 3999 seconds. The default value is 2000. NOTE: Suppress value can be configured only if the Half Life Time and Reuse value are set. Maximum Suppress Value—enter the maximum time (in seconds) a route can be suppressed. This value ranges from 1800 to 10800 seconds. The default value is 3600. NOTE: Max-Suppress Time can be configured only if the half life time, reuse value and suppress value are set. Decay timer granularity—enter the timer granularity (in seconds) for performing all decay calculations. This value ranges from 1 to 10800 seconds. The default value is 1. Reuse timer granularity—enter the time interval between evaluations of the reuse lists. This value ranges from 15 to 10800 seconds. The default value is 15. Reuse Array index—enter the size of reuse index arrays. This size determines the accuracy with which suppressed routes can be placed within the set of reuse lists when suppressed for a long time. This value ranges from 256 to 65535. The default value is 1024. VRF Name—default.

Buttons	• Apply—modifies attributes for the selected entry and saves the changes. • Reset—resets to default value for respective fields and discards all user inputs.

Community Filter Configuration

Figure 51: Community Filter Configuration

Community filter configuration

Community value *
Filter Status Permit ▾
Filter Table In ▾
VRF Name default ▾*

Add
Reset

Select	Community Value	Filter Status	Filter Type	Context Name
☒	65587	Permit ▾	In ▾	default

Apply
Delete

Screen Objective	This screen allows the user to configure the incoming / outgoing filter status for a given community value. This filter status allows/ filters the community attribute while receiving or advertising. The rules to filter out the updates are based on the AS from which it is received, <i>NLRI</i> and AS through which it had passed.
Navigation	Layer 3 Management > BGP4 > Comm Filters
Fields	• Select—select the Peer ASN and delete the confederation. • Community value—enter the community value for which the incoming / outgoing filtering policy is to be updated. This value ranges from 65536 to 4294901759 and 4294967041 to 4294967043.

Fields (cont)	• Filter Status—select the incoming / outgoing filtering policy for the community. The default option is Permit. The list contains: – Permit—allows a particular community attributes to be received or advertised in updates. – Deny—filters the routes containing the community attribute value in received or advertised updates. • Filter Table/ Filter Type—select to configure the incoming filter status or outgoing filter status for a given community value. The default option is In. The list contains: – In—configures 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—configures 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. • VRF Name / Context Name—default.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes for the selected entry and saves the changes. • Delete—deletes the selected entry.

Routes Community Set Status Table

Figure 52: Routes Community Set Status Table

Routes Community Set Status Table

Ip Address *

Prefix Length *

Community set Status Modify ▾

VRF Name default ▾ *

ADD Reset

Select	Ip Address	Prefix Length	Community Status	Context Name
☒	100.0.0.1	1	modify ▾	default

Delete

Screen Objective	This screen allows the user to configure the community attribute advertisement policy for a given destination.
Navigation	Layer 3 Management > BGP4 > Comm Policies
Fields	Select—select the community value for which the policy needs to be deleted. IP Address—enter the IP Address for which the community policy needs to be applied. Prefix Length—enter the IP prefix length for the destination. This IP prefix length configures 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. Community set Status—select the community set status for the route. The default option is Modify. The list contains: - Set—sends only the configured additive communities with associated route - SetNone—sends the associated route without communities. - Modify—removes the associated route with received delete communities and adds the configured additive communities. NOTE: This field can be set only if the local AS is configured for the <i>BGP4</i>. VRF Name—default.

Buttons	Add—adds and saves new configuration. Reset—resets to default value for respective fields and discards all user inputs. Delete—deletes the selected entry.

Community Routes

Figure 53: Community Routes

Community Routes

Ip Address

*

Prefix length

*

Community value

*

Route Table

Addition

▼

VRF Name

default

▼

*

ADD

Reset

Select	Ip Address	Prefix Length	Community Value	Table Value	Context Name
☒	100.0.0.1	1	65587	Addition ▼	default

Delete

Screen Objective	This screen allows the user to configure additive / delete communities for a given destination.
Navigation	Layer 3 Management > BGP4 > Comm Routes

Fields	• Select—select the community value for which the community route needs to be deleted. • Ip Address—enter the IP Address of the destination. • Prefix Length—enter the IP prefix length for the destination. This IP prefix length configures 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. • Community Value—enter the community value for which the additive / delete communities need to be configured. This value ranges from 65536 to 4294901759 and 4294967041 to 4294967043. • Route Table—select to configure the additive communities or delete communities for a given destination. The default option is Addition. The list contains: – Addition—adds associated community value to the already existing communities in the route update. – Deletion—removes the community attribute from the route-prefix when it passes through the filter process. • VRF Name—default.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Delete—deletes the selected entry.

Extended Community Filter Configuration

Figure 54: Extended Community Filter Configuration

Extended Community filter configuration

Community value *

Filter Status Permit ▾

Filter Table In ▾

VRF Name ▾*

ADD Reset

Select	Community Value	Filter Status	Filter Type	Context Name
☒	1:0:0:0:64:1:2	Permit ▾	In ▾	default

Delete Apply

Screen Objective	This screen allows the user to configure the incoming / outgoing filter status for a given extended community value.
Navigation	Layer 3 Management > BGP4 > Ext Comm Filters
Fields	• Select—select the Extended Community value for which the filter status needs to be modified or deleted. • Community Value—the extended Community Value for which the input / outgoing filtering policy is to be updated. This field is an Octet string of maximum size 8. • Filter Status—select the incoming / outgoing filtering policy for the extended community. The default option is Permit. The list contains: – Permit—allows a particular extended community attributes to be received or advertised in updates. – Deny—filters the routes containing the extended community attribute value in received or advertised updates. • Filter Table/ Filter Type—select to configure the incoming filter status or outgoing filter status for a given extended community value. The default option is In. The list contains: – In—configures the direction of route-updates on which the extended community filter policy needs to be applied as in. This indicates that the community filter needs to be applied on received routes. – Out—configures the direction of route-updates on which the extended community filter policy needs to be applied as out. This indicates that the community filter needs to be applied on routes advertised to peers. • VRF Name / Context Name —default.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Delete—deletes the selected entry.

Extended Community Set Status Table

Figure 55: Extended Community Set Status Table

Routes Ext-Community Set Status Table

Ip Address

*

Prefix Length

*

Community set Status

Modify

▼

VRF Name

default

▼

*

ADD

Reset

Select	Ip Address	Prefix Length	Community Status	Context Name
☒	10.0.0.0	1	modify ▼	default
Delete				

Screen Objective	This screen allows the user to configure the extended community attribute advertisement policy for a given destination.
Navigation	Layer 3 Management > BGP4 > Ext Comm Policies
Fields	Select—select the community value for which the policy needs to be deleted. IP Address—enter the IP Address of the destination. Prefix Length—enter the IP prefix length for the destination. This field configures 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. Community set Status—select the extended community set status for the route. The default option is Modify. The list contains: - Set—sends only the configured additive communities with associated route. - SetNone—sends the associated route without communities. - Modify—removes the associated route with received delete communities and adds the configured additive communities. NOTE: This field can be set only if the local AS is configured for the BGP4. VRF Name—default.

Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Delete—deletes the selected entry.

Routes Extended Community Table

Figure 56: Routes Extended Community Table

Routes Extended Community Table

Ip Address

Prefix length *

Community value

Route Table Additive ▾

VRF Name default ▾ *

ADD Reset

Select	Ip Address	Prefix Length	Community Value	Route Table	Context Name

Delete

Screen Objective	This screen allows the user to configure additive / deletive extended communities for a given destination.
Navigation	Layer 3 Management > BGP4 > Ext Comm Routes

Fields	• Select—select the IP Address for which the policy needs to be deleted. • IP Address—enter the IP Address of the destination. • Prefix Length—enter the IP prefix length for the destination. This field configures 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. • Community value—enter the extended community value for which the additive / delete communities need to be configured. This field is an octet string of maximum size 8. • Route Table—select to configure the additive / delete extended communities for a given destination. The default option is Additive. The list contains: – Additive—adds associated extended community value with the already existing communities in the route update. – Deletive—removes the extended community attribute from the route-prefix when it passes through the filter process. • VRF Name / Context Name—default.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Delete—deletes the selected entry.

21. Layer 4 Switching Filter

This section describes the Layer 4 Switching Filter Interface.

Figure 1: Layer 4 Switching Filter

Layer 4 Switching Filter

Filter Number

Protocol

TCP

Port Number

Copy-To-Port

Add

Reset

Select	Filter Number	Protocol	Port Number	Copy-To-Port
☒	1	TCP	255	255

Delete

Screen Objective	This screen allows the user to configure the Layer 4 switching details applicable globally for the switch
Navigation	Layer 4 Management > Switch Filter
Fields	Select—select the filter number for which the configuration needs to be deleted. Filter Number—enter the L4 Switching filter rule number that is used to identify uniquely the entry created in the switch. This value ranges from 1 to 65535. Protocol—select the type of protocol to be checked against the packet. The default option is ANY. The list contains: - TCP—specifies that the filter is to be applied for Transmission Control Protocol (<i>TCP</i>) packets. - UDP—specifies that the filter is to be applied for User Datagram Protocol (<i>UDP</i>) packets. - ANY—specifies that the filter is to be applied for any other protocol packets Port Number—enter the L4 port number for which the L4 switching details should be applied. This port switches the packets of type specified in the field Protocol to the port specified in the field Copy-To-Port. This value ranges from 0 to 65535. The default value is 0. NOTE: Only <i>UDP/TCP</i> ports can be configured for L4 switching.

Field (cont)	• Copy-To-Port—enter the port number to which the packets mentioned in the field Protocol should be switched from the port mentioned in the field Port Number. This value ranges from 0 to 65535 to be deleted.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value and discards all user input. • Delete—deletes the selected entry.

Multicast Map

22. Multicast Protocols

This section describes the interfaces of the Multicast protocols.

22.1. IGMP Snooping

This section describes Internet Group Management Protocol (*IGMP*) Snooping configuration.

IGMP (Internet Group Management Protocol) is the protocol used by a host for informing 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. *IGS* (IGMP Snooping) is the process of listening to *IGMP* network traffic (i.e. 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, the other computer can learn the multicast sessions to which the computers on the local network are listening. *IGS* significantly reduces traffic from streaming media and other bandwidth-intensive IP multicast applications.

To access **IGMP Snooping** screens, go to **Multicast > IGMP Snooping**.

The *IGMP* Snooping-related parameters are configured through the screens displayed by the following tabs:

[IGMP Snooping Configuration - Basic Settings](#)

[IGMP Snooping Timer Configuration](#)

[IGMP Snooping VLAN Configuration](#)

[IGMP Snooping Interface Configuration](#)

[IGMP Snooping VLAN Router Port Configuration](#)

[IGMP Snooping VLAN Router Ports](#)

[IGMP Snooping Static Configuration](#)

[MAC Based Multicast Forwarding Table](#)

[Multicast Receiver Table](#)

IGMP Snooping Configuration - Basic Settings

By default, the tab **IGMP Snooping** displays the **IGMP Snooping Configuration** screen.

Figure 1: IGMP Snooping Configuration

IGMP Snooping Configuration

System Control Start ▼
Submit

Select	IGMP Snooping Status	Operational Status	Snooping Mode	Proxy Reporting	Snoop Leave Level	Snoop Report process config-level	Enhanced Mode	Sparse Mode
☒	Enabled ▼	Disabled ▼	Mac Based ▼	Enabled ▼	Vlan Based ▼	Non-RouterPorts ▼	Disabled ▼	Disabled ▼
Select	Proxy Status	Filter Status	Multicast Vlan	Report Forwarding	Query Forwarding	Retry Count	Query Transmit On TC	
☐	Disabled ▼	Disabled ▼	Disabled ▼	Router Ports ▼	Non-Router Ports ▼	2	Disabled ▼	

Apply

Note : To enable IGS, Dynamic Multicast status should be disabled.

Screen Objective	This screen allows the user to configure basic settings such as <i>IGMP</i> snooping status, Operational Status, Snooping Mode, Proxy Reporting, and Snoop Leave level.
NOTE: The fields in second row of the form at the bottom can be modified after clicking the select option in the second row. To configure <i>IGS</i> , <i>GARP</i> (<i>GMRP</i> (Generic Attribute Registration Protocol) Multicast Registration Protocol) must be disabled.	
Navigation	Multicast > IGMP Snooping > Basic Settings
Fields	• Select—select the option button to configure the selected parameters • System Control—select the System Control status of <i>IGS</i> in the switch. The default option is Start. The list contains: – Start—starts the <i>IGMP</i> snooping and allocates the resources required by the <i>IGS</i> module. During the protocol start-up, it creates semaphore, RBTree, hash table, and also initializes the timer task. – Shutdown—all resources are released back to the system and the module stops running. All timers are stopped. The RBTree, hash table, and allocated memory pools are deleted. • IGMP Snooping Status—select the global status of <i>IGS</i> in the switch. The default option is Disabled. The list contains: – Enabled—starts the <i>IGMP</i> Snooping operations. – Disabled—stops performing the <i>IGMP</i> Snooping operations. • Operational Status—displays the Operational status of the <i>IGS</i> (I) in the switch. The default option is disabled. The list contain: – Enabled—indicates that <i>IGS</i> protocol is currently enabled in the system. – Disabled—indicates that <i>IGS</i> protocol is currently disabled in the system.

Fields (cont)	• Snooping Mode—select the <i>IGMP</i> snooping mode. Modes are provided with redundancy support. The default option is <i>MAC-Based</i>. The list contains: – IP based—<i>IGS</i> protocol operation is based on the IP address and group address. This mode is chosen if the hardware supports programming of S, G and *, and G entries – MAC based—hardware supports only <i>MAC</i>-based multicast tables and the snooping protocol operation is based only on the group address. • Proxy Reporting—select the Proxy Reporting status in the switch. <i>IGMP</i> snooping with Proxy Reporting or report suppression actively filters <i>IGMP</i> packets to reduce <i>IGS</i> network traffic. The default option is Enabled. The list contains: – Enabled—switch generates reports and forwards them to the router, based on the available host information. – Disabled—switch acts as transparent snooping bridge. The switch forwards all v3 reports and a single v2 report to the router. • Snoop Leave Level—select the Leave processing mechanism to be implemented at the VLAN level or at port level. 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. The default option is <i>VLAN Based</i>. The list contains: – VLAN Based—configures the leave mechanism at the <i>VLAN</i> level. In <i>VLAN</i>-based leave processing mode, Fast Leave functionality which is configurable per <i>VLAN</i> or normal leave configurations are available for processing Leave messages. – Port Based—configures the Leave mechanism at port level. In Port-Based leave processing mode, the explicit host tracking functionality, the fast leave functionality, or normal leave, which are configurable on an interface, can be used for processing the Leave messages. • Snoop report Process Config Level—incoming report messages. The default option is Non-RouterPorts. The list contains: – Non-RouterPorts—the incoming report messages are processed only in the Non-Router Ports. Report message received in the router ports are not processed. – All-Ports—the incoming report messages are processed in all ports including router ports.

Fields (cont)	Enhanced Mode—select the operating status of snooping module. The default option is Disabled. The list contains: - Enabled—the snooping module operates in Enhanced Mode. This mode enhances the operation of <i>IGMP</i> snooping module to duplicate multicast traffic by learning multicast group entries based on the port and inner <i>VLAN</i>. This mode of operation is applied when the downstream devices are less intelligent or not capable of duplicating Multicast traffic. The module multicasts from an Outer <i>VLAN</i> (<i>SVLAN</i>) to a set of ports & inner <i>VLANs</i> (<i>CVLAN</i>). In this mode, an S-tagged multicast data or a query packet from one port can result in multiple copies of the packet on the same egress port, each with a different C-tag. The Inner <i>VLAN</i> (<i>CVLAN</i>) will typically have a valid value within the designated range. - Disabled—this mode of operation is applied when downstream device can perform duplication of Multicast traffic. In this mode, the module multicasts from an Outer <i>VLAN</i> (<i>SVLAN</i>) to a set of ports. The Inner <i>VLAN</i> (<i>CVLAN</i>) will typically have a value of zero. In this mode, an S-tagged multicast data or query packet from one port can result in multiple packets on separate egress ports, with only one packet on per egress port with an S-tag or with no tag. NOTE: Enhanced mode is in Enabled state only when the Snooping Mode is set as IP Based. Sparse Mode—select whether the snooping module will operate in the Sparse Mode or Non-Sparse Mode. This option is designed to select whether the unknown multicast traffic should be dropped or flooded when there is no interested listener. The default option is disabled. The list contains: - Enabled—the <i>IGS</i> module drops the unknown multicast traffic when there is no listener to the multicast data. - Disabled—the <i>IGS</i> module forwards the unknown multicast traffic. The multicast data gets flooded to the member port of <i>VLAN</i>. NOTE: Sparse mode is in enabled state, only when the Snooping Mode is set as IP Based. Proxy Status—select the status of the proxy in the system. In proxy mode, all reports and queries generated by the switch will be having the switch IP as the source IP. The list contains: - Enabled—enables proxy in the system. The switch acts as a querier for all downstream interfaces and as a host for all upstream interfaces. - Disabled—disables proxy in the system. NOTE: Proxy status can be enabled only if Proxy-reporting is disabled.

Fields (cont)	• Filter Status—select the filter status. The default option is Disabled. The list contains: – Enabled—enables the <i>IGS</i> filtering feature. The channel registration is restricted from addition to the database if it is to be filtered. In transparent snooping, the filtered packet will not be added to the snooping database but will be forwarded upstream. – Disabled—disables the <i>IGS</i> filtering feature. All filter related configurations are allowed but the incoming report will not be subjected to the filter process. <i>IGS</i> module programs the hardware to remove the configured rate limit. It flushes all the registrations learnt through a port if a threshold limit is configured for this interface. • Multicast VLAN—select the Multicast <i>VLAN</i> (<i>MVLAN</i>) status. Multicast <i>VLAN</i> (<i>MVLAN</i>) feature can be used for applications where wide-scale deployment of multicast traffic is necessary. <i>MVLAN</i> registration allows a subscriber on a port to subscribe and unsubscribe to a particular multicast stream on any of the multicast <i>VLANs</i>. <i>MVLANs</i> enable efficient multicast data flow in separate <i>MVLANs</i>, while normal data flows through other/different <i>VLANs</i>. The default option is Disabled. The list contains: – Enabled—enables the Multicast <i>VLAN</i> feature. Router sends a single copy of the data for the particular <i>MVLAN</i>, instead of forwarding a separate copy of the multicast data to each <i>VLAN</i>. This saves the network bandwidth. – Disabled—disables the multicast <i>VLAN</i> feature. With <i>MVLAN</i> disabled, a separate copy of the multicast data has to be forwarded from the router. • Report Forwarding—select whether the report must be forwarded to all ports or only to router ports. The port which receives the query message from the router is a router port. The default option is Router Ports. The list contains: – Router Ports—forwards reports only to the router ports. – All Ports—forwards reports to all ports of the <i>VLAN</i>. – Non-edge—forwards the reports to non-edge ports detected by spanning tree protocol. • Query Forwarding—select whether the query to be forwarded to the entire member ports of the <i>VLAN</i> or to Non-router Ports. The default option is Non-Router Ports. The list contains: – All Ports—the query messages are forwarded to all the member ports of the <i>VLAN</i>. – Non-Router Ports—the query messages are forwarded only to the non-router ports. • Retry Count—enter the maximum number of group specific queries sent on a port on reception of an <i>IGMPv2</i> leave message. This value ranges between 1 and 5. The default value is 2.

Fields (cont)	NOTE: When the switch receives leave message on a port, it sends group specific query to check if there are any other interested receivers for the group. The Retry Count defines the maximum number of queries sent by the switch before deleting the port from the group membership information in the forwarding database. If the maximum retry count exceeds the Retry Count, the port will be deleted from the multicast group membership information in the forwarding database and received leave message will be forwarded onto the router ports if there are no interested receivers for the group. • Query Transmit on TC—select path redundancy for <i>IGMP</i> Snooping queries transmission to be enabled or disabled whenever topology changes. The default option is Disabled. The list contains: – Enabled—provides path redundancy while preventing undesirable loops in the network. When enabled, it allows the path to exchange information so that only one of them will handle a given message that is being sent between two computers within the network. – Disabled—path redundancy is disabled, and it leads to flooding of data.
Buttons	• Submit—modifies attributes and saves the changes. • Apply—modifies attributes for the selected entry and saves the changes.

IGMP Snooping Timer Configuration

Figure 2: IGMP Snooping Timer Configuration

IGMP Snooping Timer Configuration

Router Port PurgeInterval (Secs)	125
Group-Member Port Purge Interval (Secs)	260
Report Forward Interval (Secs)	5
Group Query Interval (Secs)	2
Apply Reset	

Screen Objective	This screen allows the user to set Router Port Purge Interval, Group-Member Port Purge Interval, Report Forward Interval, and Group Query Interval.
Navigation	Multicast > IGMP Snooping > Timer
Fields	• Router Port Purge Interval (Secs)—enter the time interval after which the learnt router port will be purged. This option is to determine the aliveness of router ports. This value ranges from 60 to 600 seconds. The default value is 125 seconds. NOTE: For each router port learnt, the timer runs for the configured port purge time interval. When the timer expires, the learnt router port entry is purged. If control messages are received from the router before the timer expiry, the timer restarts.

Fields (cont)	• Group Member Port Purge Interval (Secs)—enter the time interval after which a learnt port entry is purged if <i>IGMP</i> reports are not received on a port. This value ranges from 130 to 1225 seconds. The default value is 260 seconds NOTE: For each port on which report has been received, this timer runs for the configured time. This timer will be restarted whenever a report message is received from a host on the specific port. If the timer expires, the learnt port entry will be purged from the multicast group. • Report Forward Interval (Secs)—enter the time interval within which the next report messages for the same multicast group will not be forwarded. This timer is used when both proxy and proxy-reporting is disabled. This option is to perform Join Aggregation of <i>IGMP</i> membership report. This value ranges from 1 to 25 seconds. The default value is 5 seconds. NOTE: This is the interval (in seconds) within which report messages for the same multicast group will not be forwarded. The Report Forward Interval is per multi-cast group. This timer is started as soon as a report message for that group is forwarded out. Within this ReportForwardInterval, if another report for the same group arrives, that report will not be forwarded. • Group Query Interval (Secs)—enter the interval value for which the snooping switch waits for the membership reports from the interested receivers for the given multicast group after sending out query messages. This value ranges from 2 to 5 seconds. The default value is 2 seconds parameters
Buttons	• Apply—modifies attributes and saves the changes. • Reset—resets to default value and discards all user input.

IGMP Snooping VLAN Configuration

Figure 3: IGMP Snooping VLAN Configuration

IGMP Snooping Vlan Configuration

VLAN ID

IGMP Snooping Status

Operating Version

Fast Leave

Querier Status

Startup Query Count

Startup Query Interval(secs)

Querier Interval(secs)

Other Querier Present Interval(secs)

Router Port List

Blocked Router Port List

Multicast Vlan Profile

Max Response Code

Add

Reset

Select	VLAN ID	IGMP Snooping Status	Configured Version	Current Version	Fast Leave	Configured Querier Status	Current Querier Status
☒	1	Enabled	Version 3	v3	Disabled	Disabled	Disabled

Startup Query Count	Startup Query Interval(secs)	Querier Interval(secs)	Other Querier Present Interval(secs)	Router Port List	Blocked Router Port List	Multicast Vlan Profile	Max Response Code
2	31	125	255	NONE	NONE	0	100

Apply

Delete

Screen Objective	This screen allows the user to configure <i>IGMP</i> Snooping on specific <i>VLANs</i> .
Navigation	Multicast > IGMP Snooping > VLAN Configuration
Fields	VLAN ID—select the <i>VLAN</i> Identifier that uniquely identifies a specific <i>VLAN</i> from the list already in the system. The <i>IGMP</i> snooping configuration is performed for this specific <i>VLAN</i> ID. IGMP Snooping Status—select the status of <i>IGMP</i> snooping on the specified <i>VLAN</i>. The default option is Disabled. The list contains: - Enabled—<i>IGS</i> is enabled on the specified <i>VLAN</i>. A switch will listen for <i>IGMP</i> messages from the host connected on those interfaces and build the software. This ensures that only the ports that require a given multicast stream actually receive it - Disabled—<i>IGS</i> is disabled on the specified <i>VLAN</i>.

Fields (cont)	• Operating Version/ Configured Version—select the Operating Version of <i>IGS</i> for the specified VLAN. The default option is Version 3. The list contains: – Version 1—the port list connected to listeners of multicast groups is built based on <i>IGMP</i> membership reports, query, and Leave messages. – Version 2—the port list connected to listeners of Multicast groups is built based on <i>IGMP</i> membership reports, query, and Leave messages, with added support for low leave latency; low leave latency is a reduction in the time it takes for a multicast router to learn that there is no longer any member of a particular group present on an attached network. – Version 3—the port list is based on source filtering information sent by <i>IGMPv3</i> hosts in their membership reports to build Source-Specific Multicast (<i>SSM</i>) groups. Support for source filtering is the ability for a system to report interest in receiving packets only from specific source addresses or from other than specific source addresses sent to a particular multicast address. • Fast Leave—select the Fast Leave status of <i>IGS</i>. The default option is Disabled. The list contains: – Enabled—on receipt of a single Leave message, the port information is immediately removed from the multicast group entry. The switch immediately removes the port from the forwarding table without sending a group specific query. The Fast Leave functionality does not verify if other interested receivers are still present for the multicast group on the same port. – Disabled—normal Leave functionality gets enabled. The switch checks if there are any interested receivers for the group by sending a group specific query before removing the port from the forwarding table. • Querier Status/ Configured Querier Status—select whether the switch is configured as a querier in a VLAN. The default option is Disabled. The list contains: – Enabled—the switch starts acting as a querier and sends query messages until it receives best querier information. The switch sends general queries at regular time intervals. This querier message takes part in querier election. – Disabled—the switch is configured as non-querier, does not propagate any general query messages, and does not take part in querier election. • Startup Query Count—enter the number of queries to be sent during start-up of querier election process at the interval of start-up query interval. This value ranges from 2 to 5. The default value is 2. • Startup Query Interval (secs)—enter the interval (in seconds) between the start-up general query messages sent by the switch (querier) during the start-up of querier election process. This value ranges from 15 to 150 seconds. The default value is 32 seconds. NOTE: This value should be less than or equal to one fourth of query interval value configured for the <i>VLAN</i>.

Fields (cont)	• Querier Interval (secs)—enter the time period between which the general queries are sent by <i>IGMP</i> snooping, when the switch is configured as querier on a <i>VLAN</i>. The switch waits for the configured time period after sending a general query message. On the expiry of this query interval, the switch again sends the general query message and restarts the timer. This value range between 6 and 600 seconds. The default value is 125 seconds. • Other Querier Present Interval (secs)—enter the time period (in seconds) that must pass before a multicast router decides that there is no longer another multicast router which should be the querier. This value ranges from 120 to 1215 seconds. The default value is 255 seconds. NOTE: This value must be $\geq ((\text{Robustness Variable} * \text{Query Interval}) + (\text{Query Response Interval}/2))$. NOTE: The Robustness Variable tunes <i>IGMP</i> to expected losses on a link. <i>IGMPv3</i> is robust to (Robustness Variable—1) packet losses. • Router Port List—enter the static Router Port List for <i>VLAN</i>. When the snooping switch receives a Router advertisement message through a port, the port is identified as router port and is added in the router port list. The default option is None. • Blocked Router Port List—enter the list of ports which are configured statically as blocked router ports. For a blocked router port, the software discards queries, <i>PIM</i> (Protocol Independent Multicast) / <i>DVMRP</i> (Distance Vector Multicast Routing Protocol), and Data Messages and prevents the port from ever becoming a router port. The blocked router port feature does not involve any hardware programming. Multicast data is dropped for a blocked router port. Reports are not forwarded to a blocked router port. Reports coming from a blocked router port are not processed. The default option is None. NOTE: A port cannot be configured as a blocked router port if it is already configured as static router port. • Multicast VLAN Profile—select the multicast profile identification configured for a particular <i>VLAN</i> and used for multicast <i>VLAN</i> classification. When any untagged report or Leave message is received, and the Group & Source address in the received packet matches any rule in this profile, the received packet is classified to be associated with the <i>VLAN</i> to which this profile is mapped. • Max Response Code—enter the maximum response code advertised in queries which are sent over this <i>VLAN</i>. This value ranges from 0 to 255 tenths of a second. The default value is 100. • Current Version—displays the working <i>IGMP</i> Version on the <i>VLAN</i>. • Current Querier Status—displays the current querier status in the <i>VLAN</i>. The value can be enabled or disabled.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

IGMP Snooping Interface Configuration

Figure 4: IGMP Snooping Interface Configuration

IGMP Snooping Interface Configuration

Interface Index
 Leave Mode
 Threshold Limit Type
 Threshold Limit
 Rate Limit
 Filter Profile

Interface Index	Leave Mode	Threshold Limit Type	Threshold Limit	Rate Limit	Filter Profile Id
1	Normal	None	0	100	1

Figure 54-5: IGMP Snooping Interface Configuration

Screen Objective	This screen allows the user to set Router Port Purge Interval, Group-Member Port Purge Interval, Report Forward Interval and Group Query Interval.
Navigation	Multicast > IGMP Snooping > Interface Configuration
Fields	• Interface Index—select the interface index of the port from the list of interfaces. • Leave Mode—select the mechanism to be used for processing leave messages in the downstream interface. The default option is Normal Leave. The list contains: – Explicit Tracking—leave messages are processed using the explicit tracking mechanism. On receipt of the leave message, the switch uses its learnt data-base to determine whether the specified multicast group has a single receiver or multiple receivers attached to the port. The switch removes the port from the multicast group entry only when no other receivers are present in the same group. – Fast Leave—leave messages are processed using the Fast Leave mechanism. On receipt of a single leave message the port is immediately removed from the group entry. The fast leave functionality does not verify if other interested receivers are still present in the multicast group on the same port. Hence the feature can be used effectively only in a point-to-point connection. – Normal Leave—a group or group-specific query is sent on the interface when a leave message is received. Once snooping switch sends the leave message for a multicast group, the snooping switch sends out query messages and waits specified time for the membership reports from the interested receivers for the given multicast group. NOTE: This field can be configured only when Snoop Leave Level is set to Port Based

Fields (cont)	• Threshold Limit Type—select the type of limit to be applied for the interface. The threshold limit will be applied when reports are received from the downstream interface. The default option is None. The list contains: – None—no limiting is done. – Groups—limits the <i>IGMP</i> report message based on the group registration allowed per downstream interface. – Channels—limit is applied only for <i>IGMPv3</i> Include and Allow reports based on the S&G registration that are allowed per downstream interface. • Threshold Limit—enter the maximum number of unique entries (channel or group) which can be learned simultaneously on the interface. The software allows the configuration of threshold limit per downstream interface. Downstream interface refers to a physical port in the default mode of operation or to a combination of inner <i>VLAN</i> and physical port in the enhanced mode of operation of the switch. This value ranges from 0 to 4294967295. The default value is 0. NOTE: This field can be configured only when the Threshold Limit Type is set. • Rate Limit—enter the rate limit for a downstream interface in number of <i>IGMP</i> packets per second. The MDL rate limit per port will eliminate bursts or attacks coming from the specific physical port and exhausting the system resources. This value ranges from 0 to 4294967295 with default value of 4294967295. • Filter Profile ID—select the Filter Profile ID. This unique identifier configured by the administrator for a particular Internet address type identifies each of the profile entries. This ID is configured for the downstream interface - default of 0.
Buttons	• Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

IGMP Snooping VLAN Router Port Configuration

Figure 5: IGMP Snooping VLAN Router Port Configuration

IGMP Snooping Vlan Router Port Configuration

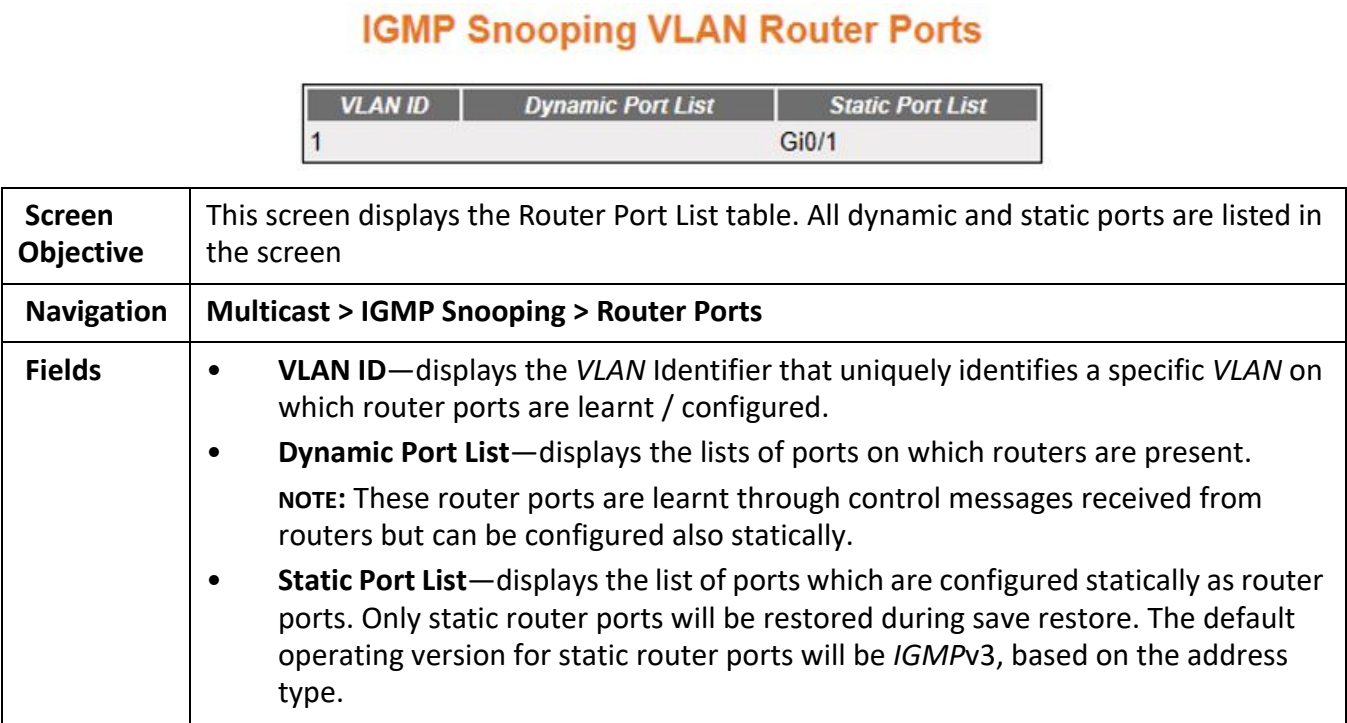
VLAN ID	vlan1 ▾
Router Port List *	
V1/V2 Rtr Port Purge Interval	
Static Router Port Version	▾
Add Modify Delete	

VLAN ID	Router Port	Router Port Config Version	Router Port Version	V1/V2 Router Port Purge Interval	V3 Router Port Purge Interval
1	Gi0/1	version v3	version v3	125	125

Screen Objective	This screen allows the user to configure the details of the router port.
Navigation	Multicast > IGMP Snooping > Router Port Configuration
Fields	• VLAN ID—select the <i>VLAN</i> Identifier that uniquely identifies a specific <i>VLAN</i> from a list of already specified in the system. The IGMP snooping configuration is performed for the entered <i>VLAN</i> ID. • Router Port List—enter the router port/port list for the <i>VLAN</i> specified in <i>VLAN</i> ID field. When the snooping switch receives a router advertisement message through a port, the port is learnt as router port. These ports are part of this router port list. User can enter the router port/port-list on which he wants to configure the purge interval / version. • V1/V2 Router Port Purge Interval—enter the time interval after which the switch assumes that there are no v1/v2 routers present on the upstream port. For each router port learnt, this timer runs for 'RouterPortPurgeInterval' seconds. When the time is over, the learnt router port entry is purged. If control messages are received from the router before the timer expiry, then the timer is restarted. This value ranges from 60 to 600. The default value is 125. • Static Router Port Version—select the operating version of the IGMP proxy on the upstream router port. The default option is Version 3. The list contains: – Version1—indicates that the operating version of <i>IGMP</i> proxy is version 1 – Version2—Indicates that the operating version of <i>IGMP</i> proxy is version 2 – Version3—Indicates that the operating version of <i>IGMP</i> proxy is version 3 • Router Port—displays the interface index of the port which is defined as an upstream router port. When the snooping switch receives a Router advertisement message through a port, the port is identified as router port. • Router Port Configuration Version—displays the configured version of the <i>IGMP</i> Proxy on the upstream router port. The default value is Version 3. • Router Port Version—displays the operating version of the <i>IGMP</i> proxy on the upstream router port. The default value is Version 3. • Router Port—displays the time interval after which the switch assumes that there are no IGMPv3 routers present on the upstream port. When the timer expires, the learnt router port entry is purged. If control messages are received from the router before the timer expiry, the timer is restarted. This value ranges from 60 to 600. The default value is 125. NOTE: For each V3 router port learnt, the timer runs for time interval calculated based on the formula “V3 Router port purge Interval = ((V3 Querier Query Interval * Robustness variable) + Max ResponseTime) seconds.
Buttons	• Add—adds and saves new configuration. • Modify—modifies attributes and saves the changes. • Delete—deletes the selected entry.

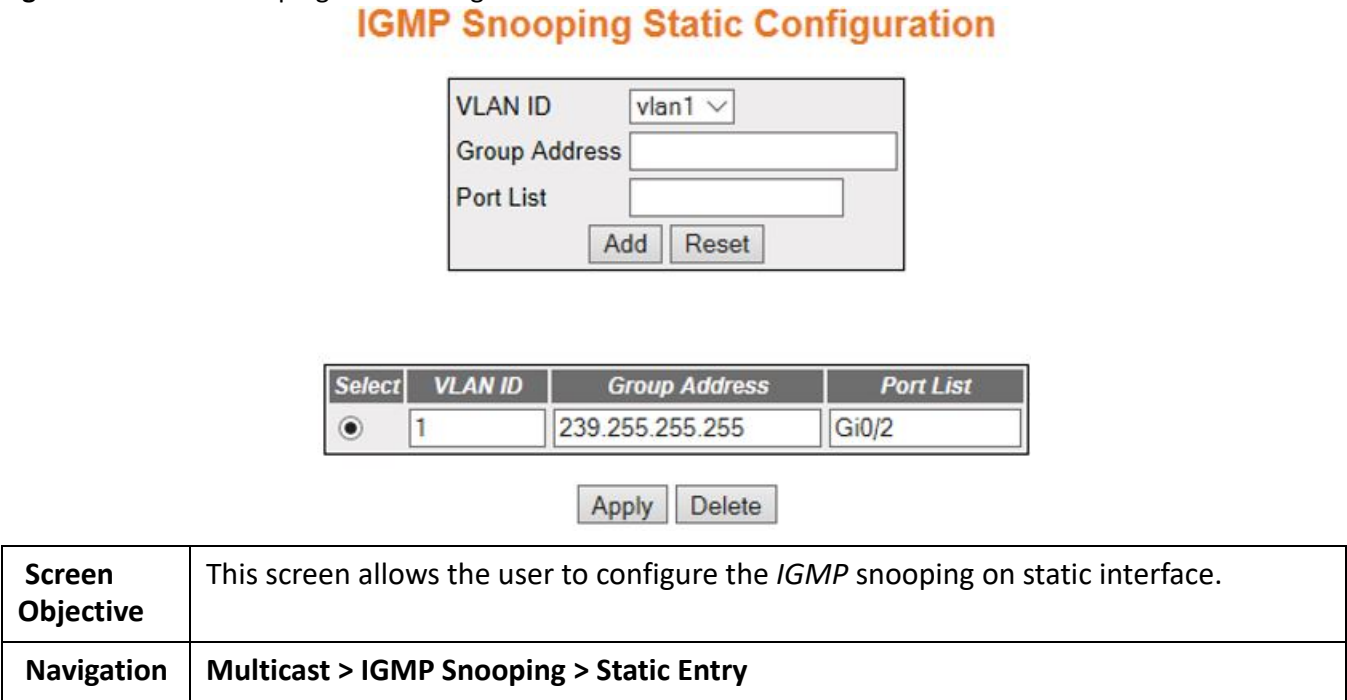
IGMP Snooping VLAN Router Ports

Figure 6: IGMP Snooping VLAN Router Ports



IGMP Snooping Static Configuration

Figure 7: IGMP Snooping Static Configuration



Fields	• VLAN ID—displays the <i>VLAN</i> Identifier that uniquely identifies a specific <i>VLAN</i> on which router ports are learnt / configured. • Group Address—enter the Group <i>MAC</i> Multicast address that is learnt. • Port List—enter the learnt ports list for which the multicast data packets for the group will be forwarded.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user inputs. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

MAC Based Multicast Forwarding Table

Figure 8: MAC Based Multicast Forwarding Table

MAC Based Multicast Forwarding Table

VLAN ID	Group MAC Address	Port List

Screen Objective	This screen displays the <i>IGMP</i> group information such as <i>MAC</i> -based or <i>IP</i> -based Multicast Forwarding Table. Multicast Forwarding table is populated with a list of ports interested in receiving multicast traffic to avoid flooding of multicast data traffic.
NOTE: When snooping is disabled on the port, all entries in the group table and forwarding table are deleted for the port.	
Navigation	Multicast > IGMP Snooping > FWD Information
Fields	• VLAN ID—displays the <i>VLAN</i> Identifier that uniquely identifies a specific <i>VLAN</i>. The <i>MAC</i> based multicast forwarding entry is displayed for the requested <i>VLAN ID</i>. • Group Address—displays the Group <i>MAC</i> Multicast address that is learnt. • Port List—displays the learnt ports' list for which the multicast data packets for the group will be forwarded.

Multicast Receiver Table

Figure 9: Multicast Forwarding Table

Multicast Receiver Table

Vlan Id	Group IP	Port	Host IP	Source IP	Filter Mode

Screen Objective	This screen displays a multicast report sent by each host in a multicast group requesting data from a specific source.
Navigation	Multicast > IGMP Snooping > Mcast Receiver Info
Fields	• VLAN ID—displays the VLAN Identifier that uniquely identifies a specific <i>VLAN</i>. The <i>MAC</i>-based multicast forwarding entry is displayed for the requested <i>VLAN ID</i>. • Group ID—displays the multicast group IP address for which the receiver has sent a request to join the group. • Port—displays the port on which the multicast receiver has sent a join request. • Host IP—displays the IP address of the multicast receiver that has sent a request to join the multicast group. • Source IP—displays the unicast source IP address of the data source that sends multicast data to the group. • Filter Mode—displays the mode that has been registered by the multicast receiver for the unicast source IP address specified. The list contains: – Include—reception of packets sent to the specified multicast address is requested <i>*only*</i> from those IP source addresses listed in the source-list parameter. – Exclude—reception of packets sent to the given multicast address is requested from all IP source addresses <i>*except*</i> those listed in the source-list parameter.

22.2. IGMP

This section describes Internet Group Management Protocol (*IGMP*) configuration.

IGMP (Internet Group Management Protocol) is a group membership management protocol used to report group memberships to any immediate neighboring multicast switch. A host uses the *IGMP* to inform a switch when it joins or leaves an Internet Multicast group.

To access **IGMP** screens, go to **Multicast > IGMP**.

The *IGMP* related parameters are configured through the screens displayed by the following tabs:

[IGMP Configuration](#)

[IGMP Interface Configuration](#)

[IGMP Group Configuration](#)

[IGMP Membership Information](#)

[IGMP Group List Configuration](#)

IGMP Configuration

By default, the tab **IGMP** displays the **IGMP Configuration** screen.

Figure 10: IGMP Configuration

IGMP Configuration

Global Status	Enabled ▾
Global limit	0
Current GroupCount	0
Apply Reset	

Screen Objective	This screen allows the user to configure the <i>IGMP</i> Status.
Navigation	Multicast > IGMP > Basic Settings
Fields	• Global Status—specifies the global status of the <i>IGMP</i> protocol in the switch. The default option is Disabled. The list contains: – Enabled—enables the <i>IGMP</i> globally. – Disabled—removes all dynamic multicast entries, stops all timers for route entries, and disables <i>IGMP</i> on all <i>IGMP</i> enabled interfaces. • Global Limit—enter the total number of multicast groups that are allowed globally. The default value is 0. The value ranges from 0 to 255. NOTE: This field can be configured only if <i>IGMP</i> Global Status is enabled. If the current group count reaches the global limit, no membership reports are honored for any interface
Fields	• Current Group Count—displays the current count of added groups added. a value from 0 to 255. NOTE: If the current group count reaches the global limit, no membership reports are honored for any interface. The current group count is incremented for each valid membership report and decremented for each leave report if global limit is configured.
Buttons	• Apply—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user input

IGMP Interface Configuration

Figure 11: IGMP Interface Configuration

IGMP Interface Configuration

Interface: loopback5

IGMP Admin Status: Disabled

Operating Version: Version 2

Fast Leave: Disabled

Channel Tracking: Disabled

Query Interval:

Query Response Time:

Robustness Value:

Interface GroupLimit:

GroupList ID:

GroupCurrent Count:

Join RateLimit:

Select	Interface	IGMP Admin Status	Operating Version	Fast Leave	Channel Tracking	Query Interval	Query Response Time	Robustness Value	Interface GroupLimit	GroupList ID	GroupCurrent Count	Join RateLimit
☐	vlan1	Disabled	Version 2	Disabled	Disabled	125	100	2	0	0	0	0
☒	loopback5	Enabled	Version 2	Enabled	Disabled	125	100	2	0	0	0	0

Screen Objective	This screen allows the user to configure the <i>IGMP</i> Interfaces.
Navigation	Multicast > IGMP > Interface Configuration
Fields	Select—select the interface for which the configuration needs to be modified or deleted. Interface—select the interface for which <i>IGMP</i> is enabled. IGMP Admin Status—select the <i>IGMP</i> admin status for the interface. The default option is Disabled. The list contains: - Enabled—enables the <i>IGMP</i> on the interface. - Disabled—disables <i>IGMP</i> on the interface. Operating Version—select the version of <i>IGMP</i> which is running on the interface. For <i>IGMP</i> to function correctly, all routers on a LAN must be configured to run the same version of <i>IGMP</i>. The default option is Version 2. The list contains Version 1, Version 2, and Version 3.

Fields (cont)	• Fast Leave—select the status of the Fast Leave feature of the <i>IGMPv3</i> protocol. The default option is Disabled. The list contains: – Enabled—provides immediate intimation to the Multicast Routing Protocol on the last member leaving the group. – Disabled—does not support Fast Leave feature NOTE: The Fast Leave feature must be enabled only on the interfaces where there is a single host. The Fast Leave feature can be enabled on interface having more than one host only if all hosts are in Version3 mode. • Channel Tracking—select the status of channel tracking feature of the <i>IGMPv3</i> protocol. Channel tracking is the ability of a system to keep track of each individual host that is joined to a particular multicast group or channel. The default option is Disabled. The list contains: – Enabled—enables the router to keep track of each individual host that is joined to a particular multicast group or channel. – Disabled—disables explicit channel tracking feature support. NOTE: This configuration is effective only if <i>IGMP</i> is enabled on the interface. Channel Tracking status can be enabled only if the <i>IGMP</i> version is selected as version3. • Query Interval—enter the frequency at which <i>IGMP</i> Host-Query packets are transmitted on the interface. This value ranges from 1 to 65535 seconds. The default value is 125 seconds. • Query Response Time—enter the maximum response time for <i>IGMP</i> queries. This value ranges from 1 to 255. The default value is 100 seconds. • Robustness Value—enter the Robustness value on this interface. The Robustness value allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy (having a high rate of packet loss), the Robustness Value may be increased. <i>IGMP</i> is robust to packet losses. This value ranges from 1 to 255. The default value is 2. • Interface Group Limit—enter the total number of multicast groups that can be allowed for this interface. If <i>IGMP</i> interface current group count reaches this Interface Limit value, no membership reports will be honored on this interface except the group list mapped to this interface. This value ranges from 0 to 255. • Group List ID—enter the except group list id for an interface. This group list is exempted for limiting on this interface. This value ranges from 0 to 4294967295. NOTE: This field can be configured only if Interface Group Limit is configured. • Group Current Count—displays the current count of groups that are added to the interface. This counter is incremented for each valid membership report on this interface and decremented for leave report if Interface Group Limit is configured for this interface. This value ranges from 0 to 255. • Join Rate Limit—enter the Join Rate Limit for a downstream interface in units of the number of <i>IGMP</i> packets per second. This value ranges from 100 to 1000. The default value is 0.

Buttons	• Add—adds and saves new configuration. • Reset—resets to default value and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

IGMP Group Configuration

Figure 12: IGMP Group Configuration

IGMP Group Configuration

Interface loopback5 *

Group Address *

Source Address

Add
Reset

Select	Interface	Group Address	Filter Mode
☒	loopback5	239.250.250.250	Exclude
Delete			

Screen Objective	This screen allows the user to configure <i>IGMP</i> Multicast groups.
Navigation	Multicast > IGMP > Group Information
Fields	• Select—select the interface for which the configuration needs to be deleted. • Interface—select the interface from the list of interfaces for which the entry contains information for an IP multicast group address. • Group Address—enter the IP multicast group address. • Source Address—enter the IP Source address where multicast data packets originate. • Filter Mode—specifies the state in which the interface is currently set. This indicates the relevance of the corresponding source list entries for <i>IGMPv3</i> interfaces. This is a read-only field. The default option is Exclude. The list contains: – Include—specifies the Filter Mode as Include. – Exclude—specifies the Filter Mode as Exclude.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value and discards all user input. • Delete—deletes the selected entry.

IGMP Membership Information

Figure 13: IGMP Membership Information

IGMP Membership Information	
Interface Group Address Source Address Reporter Address	
Screen Objective	This screen displays the source list entries corresponding to each interface filter mode record. NOTE: - The <i>IGMP</i> Source information can be displayed only when the operating version is configured as IGMPv3. <i>IGMP</i> Membership Information page is maintained for displaying explicitly tracked group information along with the source and reporter address. - This page displays group information only for explicit tracking enabled <i>IGMP</i> interfaces. Channel Tracking can be enabled using the <i>IGMP</i> Interface Configuration screen.
Navigation	Multicast > IGMP > Source Information
Fields	Interface—select the interface from the list of interfaces for which the entry contains information for an IP multicast group address. Group Address—enter the IP multicast group address. Source Address—enter the IP Source address. Reporter Address—displays the IP Address of the host requesting multicast group information. When tracking is enabled, it displays the IP address of the host for individual membership entry.

IGMP Group List Configuration

Figure 14: IGMP Membership Information

IGMP GroupList Configuration

GroupList ID

*

Group IP Address

*

Mask

*

Add

Reset

Select	GroupList ID	Group IP Address	Mask
☒	250	239.255.255.1	239.255.255.1

Delete

Screen Objective	This screen allows the user to configure the <i>IGMP</i> group list information.
Navigation	Multicast > IGMP > Grouplist Information
Fields	• Group List ID—enter the global group list Identifier. The value ranges from 1 to 4294967295. • Group IP Address—enter the multicast group IP address. 239.255.255.250 entered in the example. • Mask—enter the subnet mask address of the <i>IGMP</i> group.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value and discards all user input. • Delete—deletes the selected entry.

22.3. IGMP Proxy

This section describes Internet Group Management Protocol (*IGMP*) Proxy configuration.

NOTE: This web page is visible in WEBUI, but is not supported for this release.

IGMP Proxy enables the system to issue *IGMP* host messages on behalf of the discovered hosts. *IGMP* proxy provides queue interface and socket interface options to receive and transmit the *IGMP* control packets and multicast data packets.

IGMP proxy device performs router portion of *IGMP* on the downstream interfaces and host portion of *IGMP* on the upstream interfaces. *IGMP* proxy device consolidates the reports received in the downstream interfaces, and sends a summarized report on to the upstream interface.

To access **IGMP Proxy** screens, go to **Multicast > IGMP Proxy**.

The *IGMP* Proxy-related parameters are configured through the screens displayed by the following tabs:

[IGMP Proxy Configuration](#)

[IGMP Upstream Interface Configuration](#)

[IGMP Proxy MRoute Configuration](#)

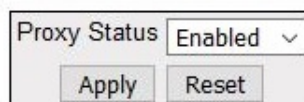
[IGMP Proxy Next Hop Configuration](#)

IGMP Proxy Configuration

By default, the tab **Basic Settings** displays the **IGMP Proxy Configuration** screen.

Figure 15: IGMP Proxy Configuration

IGMP Proxy Configuration



The screenshot shows a configuration panel for IGMP Proxy. It features a 'Proxy Status' dropdown menu currently set to 'Enabled'. Below the dropdown are two buttons: 'Apply' and 'Reset'.

Screen Objective	This screen allows the user to configure the <i>IGMP</i> Status.
Navigation	Multicast > IGMP Proxy > Basic Settings
Fields	• Proxy Status—enables/ Disables <i>IGMP</i> Proxy in the Switch. The default option is Disabled. The list contains: – Enabled—starts <i>IGMP</i> proxy module. – Disabled—stops <i>IGMP</i> proxy module. NOTE: <i>IGMP</i> proxy can be enabled only when the multicast routing protocol <i>PIM</i> is disabled.
Buttons	• Apply—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user input.

IGMP Upstream Interface Configuration

Figure 16: IGMP Upstream Interface Configuration

IGMP Proxy Upstream Interface Configuration

Interface	vlan1 ▾
Configured Version	Version 3 ▾
Version Purge Interval	
Add Reset	

Select	Interface Index	Operating Version	Configured Version	Version Purge Interval

Screen Objective	This screen allows the user to configure the <i>IGMP</i> Proxy Upstream Interfaces.
Navigation	Multicast > IGMP Proxy > Upstream Interface

Fields	• Interface—specifies the Layer 3 <i>VLAN</i> Interface, which is defined as an upstream interface. • Interface Index—specifies the index value of the Layer 3 <i>VLAN</i> Interface, which is defined as an upstream interface. This is a read-only field. This value ranges from 1 to 65535. • Configured Version—specifies the configured version of the <i>IGMP</i> Proxy device on the upstream interface. The options are Version 1, Version 2, and Version 3. Default is Version 3. • Version Purge Interval—specifies the interval (in seconds) after which the upstream interface <i>IGMP</i> operating version will be changed to configured <i>IGMP</i> version. This value ranges from 60 to 600 seconds. • Operating Version—indicates the operating version of the <i>IGMP</i> Proxy device on the upstream interface. This is a read-only field. The options are Version 1, Version 2, and Version 3.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

IGMP Proxy MRoute Configuration

Figure 17: IGMP Proxy MRoute Configuration

IGMP Proxy MRoute Information

Source Group Upface Index	
Screen Objective	This screen allows the user to view the multicast routing information for the registered group members. MRoute stands for multicast static route.
Navigation	Multicast > IGMP Proxy > MRoute Information
Fields	• Source—indicates the Unicast Source IP address of the data source that sends multicast datagrams for the registered multicast groups. • Group—indicates the IP multicast group address for which multicast registrations are received. • Upstream Interface Index—indicates the index value of the upstream interface on which IP multicast datagrams are received for the registered group address.

IGMP Proxy Next Hop Configuration

Figure 18: IGMP Proxy Next Hop Configuration

IGMP Proxy NextHop Information

Source Address	Group Address	NextHop Iface Index	NextHop State

Screen Objective	This screen allows the user to view the list of outgoing interfaces for the multicast forwarding entries.
Navigation	Multicast > IGMP Proxy > Next Hop Information
Fields	• Source—indicates the Unicast Source IP address of the data source that sends multicast datagrams for the registered multicast groups. • Group Address—indicates the IP multicast group address for which multicast registrations are received. • Next Hop Upstream Interface Index—indicates the index value of the interface on which multicast registrations for the group are received. • Next Hop State indicates the state of the outgoing interface on which the multicast registrations have been received. The options are: – Forwarding—denotes that the entry is created. – Prune—prune messages are used to prevent future messages from propagating to routers without group membership information (RFC 3973).

22.4. PIM

This section describes Protocol Independent Multicast (*PIM*) configuration.

PIM (Protocol Independent Multicast) is a multicast routing protocol designed to provide scalable inter-domain multicast routing across the Internet. *PIM* provides multicast routing and forwarding capability to a router that runs the IP protocol along with *IGMP*. *PIM* supports a plane-separated architecture for the control and forwarding planes. *PIM* is independent of the underlying unicast routing protocol and uses the information from the unicast routing protocol.

To access **PIM** screens, go to **Multicast > PIM**.

The PIM related parameters are configured through the screens displayed by the following tabs:

[PIM Basic Settings](#)

[PIM Component Configuration](#)

[PIM Interface Configuration](#)

[PIM Candidate RP Configuration](#)

[PIM Static RP Configuration](#)

[PIM Global Configuration](#)

[PIM DM Global Configuration](#)

[PIM Route Configuration](#)

[PIM RP Configuration](#)

[PIM High Availability](#)

[PIM Elected RP Information](#)

[PIM DF Information](#)

PIM Basic Settings

By default, the tab **Basic Settings** displays the **PIM Basic Settings** screen.

Figure 19: PIM Basic Settings

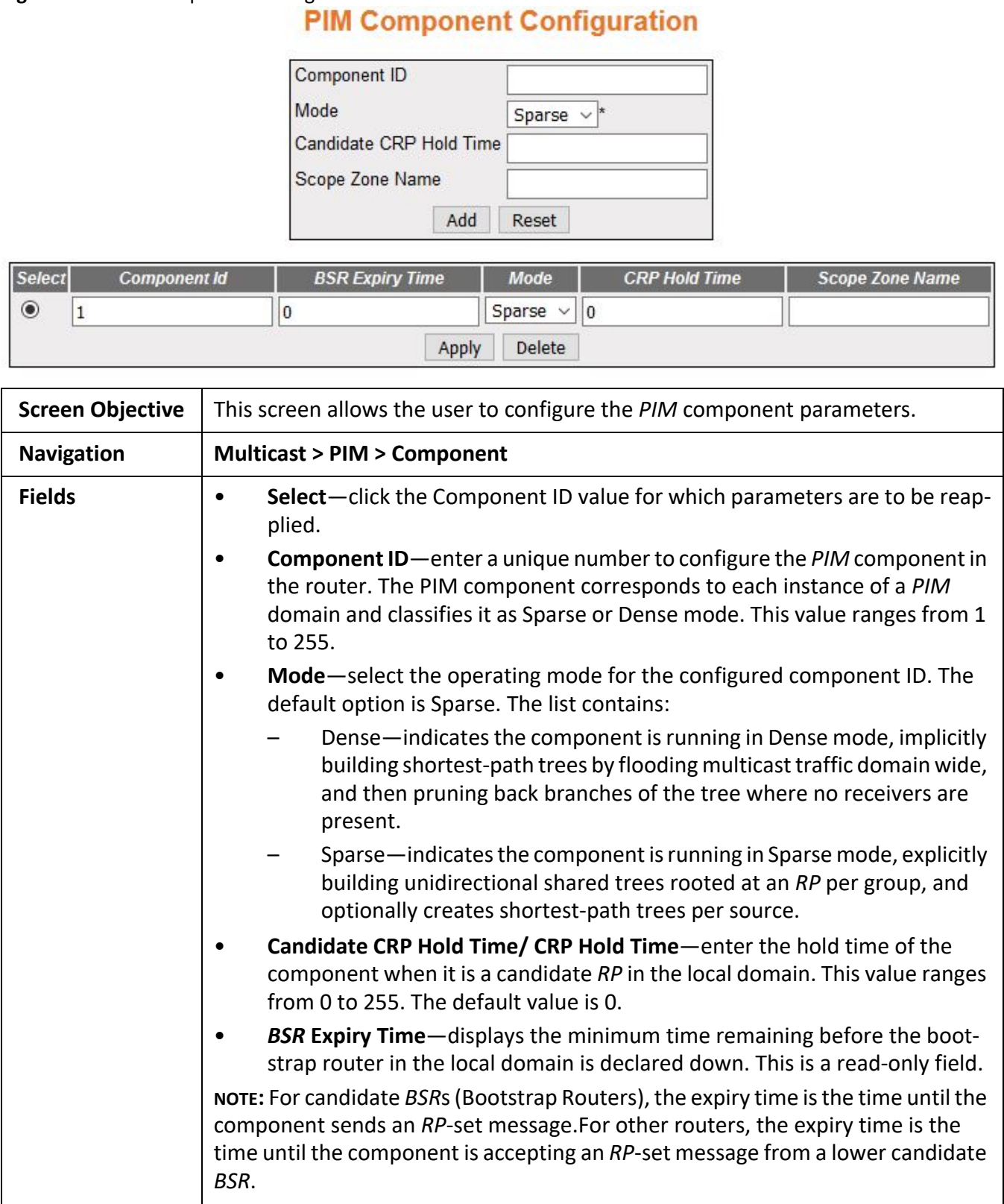


Screen Objective	This screen allows the user to configure the <i>PIM</i> basic settings.
NOTE: <i>PIM</i> is enabled only when <i>IGMP</i> . Proxy is disabled.	
Navigation	Multicast > PIM > Basic Settings
Fields	• PIM Status—select the <i>PIM</i> status in the switch. The default value is Disabled. The list contains. – Enabled—enables <i>PIM</i> globally in the switch. – Disabled—disables <i>PIM</i> globally in the switch. • PIMv6 Status—select the <i>PIMv6</i> status in the switch. The default value is Disabled. The list contains: – Enabled—enables <i>PIMv6</i> globally in the switch. – Disabled—disables <i>PIMv6</i> globally in the switch. • PIM PMBR Status—select the <i>PIM</i> Multicast Border Router (<i>PMBR</i>) Status. A <i>PMBR</i> integrates two different <i>PIM</i> domains (either <i>PIM-SM</i> or <i>PIM-DM</i>) and also connects a <i>PIM</i> domain to another multicast routing domain(s). The default value is Disabled. The list contains: – Enabled—enables <i>PIM PMBR</i> in the switch. – Disabled—disables <i>PIM PMBR</i> globally in the switch. • PIM Router Mode—select the mode of the <i>PIM-SM</i> router. The list contains: – <i>SSM Only</i>—<i>SSM</i> only mode of the <i>PIM-SM</i> router. – <i>SM, SSM</i>—<i>SM_SSM</i> mode of the <i>PIM-SM</i> router.

Fields	NOTE: This parameter can be set only if <i>PIM</i> is started globally in the switch. The family of <i>PIM</i> protocols includes dense-mode (<i>DM</i>), sparse-mode (<i>SM</i>), source specific multicast (<i>SSM</i>), and bidirectional (<i>Bidir</i>) <i>PIM</i>. <i>Bidir PIM</i> is to be used for a many-to-many applications model. • PIM Static RP Status—select the static configuration of <i>RP</i> status. A rendezvous point (<i>RP</i>) is required only in networks running <i>PIM-SM</i>. The protocol is described in RFC 2362. Static configuration allows additional structuring of the multicast traffic by directing the multicast join/prune messages to statically configured <i>RPs</i>. The list contains: – Enabled—enables <i>PIM Static RP Status</i> in the switch. – Disabled—disables <i>PIM Static RP Status</i> in the switch. NOTE: This parameter can be set only if <i>PIM</i> is started globally in the switch. • PIM Bidir Status—select the static configuration of <i>RP</i> status. A <i>RP</i> is required only in networks running <i>PIM-SM</i>. The protocol is described in RFC 2362. Static configuration allows additional structuring of the multicast traffic by directing the multicast join/prune messages to statically configured <i>RPs</i>. The list contains: – Enabled—enables <i>PIM Bidir Status</i> in the switch. – Disabled—disables <i>PIM Bidir Status</i> in the switch. NOTE: This parameter can be set only if <i>PIM</i> is started globally in the switch. • PIM RPF Status—select the <i>PIM RPF</i> (Reverse Path Forwarding) status in the router. The list contains: – Enabled—enables <i>PIM RPF Status</i> in the switch. – Disabled—disables <i>PIM RPF status</i> in the switch. NOTE: This parameter can be set only if <i>PIM</i> is started globally in the switch.
Buttons	• Apply—modifies attributes and saves the changes.

PIM Component Configuration

Figure 20: PIM Component Configuration



Fields (cont)	• Scope Zone Name—enter the Scope Zone Name. The maximum length of the string is 64. NOTE: Scope is a 4-bit value that describes the scope of an IPv6 address. A unicast address can possibly have 2 scopes (Linklocal and Global) only, and a multicast address can have a maximum of 11 scopes. The Scope Zone Name should be the same as that of the zone created in the ipv6 scope zone command. If ipv6 scope-zone is created as scopeA1, then the scope zone name should be scopeA1. (note that the string is without space).
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

PIM Interface Configuration

Figure 21: PIM Interface Configuration

PIM Interface Configuration

Interface	vlan1 ▾
Address Type	▾
Hello Interval	30
Join Prune Interval	60
C-BSR Preference	-1
Component Id	1
Add Reset	

Select	Interface	AddrType	Address	MaskLen	DR Addr	Hello Int	JP Int	C-BSR Pref	Comp Id
☐		IPv6	0000:0000:0000:0000:00	0	0000:0000:0000:0000:00	30	60	-1	1
☒	vlan1	IPv4	192.168.10.1	24	192.168.10.1	30	60	-1	1

Screen Objective	This screen allows the user to configure the <i>PIM</i> component parameters.
Navigation	Multicast > PIM > Interface
Fields	• Select—click the interface for which <i>PIM</i> interface parameters are to be reapplied. • Interface—select the index value of the <i>PIM</i> interface. • Address Type—specifies the address type of the <i>PIM</i> interface. The available option is IPv4. • Address—displays the IP address.

Fields (cont)	• Mask Length—displays the IP mask length for the configured IP address. This value ranges from 0 to 32 for an IPv4 address. • DR Address—displays the <i>DR</i> (Designated Router) address. • Hello Interval—enter the frequency at which <i>PIM</i> Hello messages are transmitted. This value ranges from 1 to 255 seconds with a default of 30 secs. • Join Prune Interval—enter frequency at which <i>PIM</i> Join/Prune messages are transmitted. The value is from 1 to 255 secs and a default of 60 secs. • C-BSR Preference—enter the preference value for the local interface as a C-BSR. This value ranges from 1 to 255. The default value is 1. • Component ID—to configure the <i>PIM</i> component, enter an unique number, which corresponds to each instance of a <i>PIM</i> domain and classifies it as Sparse or Dense mode. This value is from 1 to 255.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

PIM Candidate RP Configuration

Figure 22: PIM Candidate RP Configuration

Candidate RP Configuration

Component Id

1

*

Address Type

▼

Group Address

*

Group Mask length

*

RP Address

*

Priority

192

PIM Mode

▼

Add

Reset

Select	Component Id	Address Type	Group Address	Group Mask Length	RP Address	Priority	PIM Mode
Delete							

Screen Objective	This screen allows the user to configure <i>PIM</i> information for a Candidate <i>RP</i> for IP multicast groups. A Candidate <i>RP</i> is a router configured to send periodic Candidate-RP-Advertisement messages to the candidate Bootstrap Router (<i>BSR</i>), and processes Join/Prune or Register messages for the advertised group prefix, when it is elected as <i>RP</i> .

NOTE: To configure this screen:

- *PIM* module is enabled globally.
- *PIM* mode is set as sparse.
- *PIM* query interval and IP address must be configured.

Navigation	Multicast > PIM > Candidate PR
Fields	• Select—click the Component ID value for which parameters to be reapplied. • Component ID—to configure the <i>PIM</i> component, enter an unique number, which corresponds to each instance of a <i>PIM</i> domain and classifies it as Sparse or Dense mode. This value is from 1 to 255. • Address Type—specifies the address type of the <i>PIM</i> interface. The available option is IPv4. • Group Address—enter the IP multicast group address, for which the switch advertises itself as Candidate RP which contains the multicast routing information. • Group Mask Length—enter the subnet mask, which when combined with the group address gives the group prefix. This value ranges from 0 to 32 for IPv4. • RP Address—enter the IP address of the Candidate <i>RP</i>. • Priority—enter the priority of the Candidate <i>RP</i>. The priority value ranges from 0 to 255. The default value is 192. • PIM Mode—select PIM Mode of the group for which the Candidate <i>RP</i> is configured. The list contains: – Sparse—specifies that the Candidate <i>RP</i> is running in Sparse mode. – <i>Bidir</i>—specifies that the Candidate <i>RP</i> is running in <i>Bidir</i> mode. NOTE: To set <i>PIM</i> Mode as <i>Bidir</i>, Bidirectional <i>PIM</i> should be enabled in <i>PIM</i> Basic Settings screen (Multicast > <i>PIM</i>)
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value and discards all user input. • Delete—deletes the selected entry.

PIM Static RP Configuration

Figure 23: PIM Static RP Configuration

Static RP Configuration

Component Id

1

*

Address Type

▼

Group Address

*

Group Mask Length

*

RP Address

*

Embedded RP

▼

PIM Mode

▼

Add

Reset

Select	Component Id	Address Type	Group Address	Group Mask Length	RP Address	Embedded RP	PIM Mode
Apply Delete							

Screen Objective	This screen allows the user to configure <i>PIM</i> information for static <i>RP</i> for IP multicast groups.
NOTE: To configure this screen: - PIM module is enabled globally. - PIM mode is set as sparse.	
Navigation	Multicast > PIM > Static RP
Fields	Select—click the Component ID value for which parameters to be reapplied. Component ID—enter a unique number to configure the <i>PIM</i> component in the router. The PIM component corresponds to each instance of a <i>PIM</i> domain and classifies it as Sparse or Dense mode. This value ranges from 1 to 255. Address Type—specifies the address type of the <i>PIM</i> interface. The available option is IPv4. Group Address—enter the IP multicast group address, for which the switch advertises itself as Candidate <i>RP</i> which contains the multicast routing information. Group Mask Length—enter the subnet mask, which when combined with the group address gives the group prefix. This value ranges from 0 to 32 for IPv4. RP Address—enter the IP address of the Static-<i>RP</i>. Embedded RP—select the status of the Embedded <i>RP</i>. The default option is Disable. The list contains: - Enable—enables the Embedded <i>RP</i> feature. - Disable—disables the Embedded <i>RP</i> feature NOTE: To set PIM Mode as <i>Bidir</i>, Bidirectional PIM should be enabled in PIM Basic Settings screen (Multicast > PIM)

Fields	• PIM Mode—select <i>PIM</i> Mode of the group for which the Candidate <i>RP</i> is configured. The list contains: – Sparse—specifies that the Candidate <i>RP</i> is running in Sparse mode. – <i>Bidir</i>—specifies that the Candidate <i>RP</i> is running in Bidir mode. NOTE: To set PIM Mode as <i>Bidir</i>, Bidirectional <i>PIM</i> should be enabled in <i>PIM</i> Basic Settings screen (Multicast > PIM)
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value and discards all user input. • Apply—modifies attributes and saves the changes. • Delete—deletes the selected entry.

PIM Global Configuration

Figure 24: PIM Global Configuration

PIM Global Configuration

Bidirectional PIM Configurations

Offer Interval (0-20,000,000)

Offer Limit (3-100)

Shortest Path Tree

Group Threshold (0-2,147,483,647)

Source Threshold (0-2,147,483,647)

Switching Period (0-2,147,483,647)

RP Threshold (0-2,147,483,647)

RP Switching Period (0-2,147,483,647)

Screen Objective	This screen allows the user to configure the <i>PIM</i> component parameters.
NOTE: To configure this screen: • <i>PIM</i> module is enabled globally. • <i>PIM</i> mode is set as sparse.	
Navigation	Multicast > PIM > Global
Fields	• Offer Interval—enter the time interval between the Designated Forwarder (DF) election Offer messages to be sent. The default value is 100 milli seconds. This value ranges from 1 to 20000000 milliseconds. • Offer Limit—enter the <i>Bidir</i>-PIM Offer Limit, the number of unanswered offers before the router changes as the DF, which is a value in the range from 3 to 100. The default value is 3.

Fields (cont)	• Group Threshold—enter a <i>BPS</i> (Bits-per-second) value that initiates the source specific counters for a particular group when the threshold of data rate for any group is exceeded. It is based on number of packets. The default value is 0. This value ranges from 0 to 2147483647. • Source Threshold—enter a <i>BPS</i> value that initiates the switching to shortest path tree when the threshold of data rate or the number of packets for any source is exceeded. It ranges from 0 to 2147483647. The default value is 0. • Switching Period—enter the time period (in seconds) over which the data rate is to be monitored for switching to shortest path tree. The default value is 0. This value ranges from 0 to 2147483647. The same period is used for monitoring the data rate for both source and group. To switch to shortest path tree (<i>SPT</i>), this period must be configured. The <i>SPT</i> is used for multicast transmission of packets with the shortest path from sender to recipients. • RP Threshold—enter the threshold at which the <i>RP</i> initiates switching to source specific shortest path tree. This value ranges from 0 to 2147483647. This value ranges from 0 to 2147483647. The default value is 0. To switch to <i>SPT</i>, this threshold must be configured, and the switching is based on the number of registered packets received • RP Switching Period—enter the time period (in seconds) over which <i>RP</i> monitors register packets for switching to the source specific shortest path tree. The default value is 0. This value ranges from 0 to 2147483647. <i>RP</i>-tree is a pattern in which multicast packets are sent to a <i>PIM</i>-SM router by unicast and then forwarded to actual recipients from <i>RP</i> to switch to <i>SPT</i>; this period must be configured.
Buttons	• Apply—modifies attributes and saves the changes.

PIM DM Global Configuration

Figure 25: PIM Global Configuration

PIM DM Global Configuration

SR Origination Status	Enabled ▾
Refresh Interval	
SR Processing Status	Enable ▾
Source Active Interval	210
Apply Reset	

Screen Objective	This screen allows the user to configure the <i>PIM</i> component parameters.
NOTE: This screen displays only if <i>PIM</i> module is enabled globally.	
Navigation	Multicast > PIM > DM

Fields	• SR Origination Status—select the Origination Status of the State Refresh (SR) message. The default option is Disabled. The list contains: – Disabled—does not generate the SR message. – Enabled—generates the SR message. • Refresh Interval—enter the interval between origination and sending out of successive SRM (State Refresh Messages) control messages by the router. This value ranges from 4 to 100. • SR Processing Status—select the processing status of a SR message. The default value is Disable. The list contains: – Disable—disables the processing and forwarding of a SRM, that is, the router drops the SRM if received. In addition, the router will not advertise the SR capability in Hello messages. – Enable—enables the SRM processing and forwarding. On enabled, this router advertises itself as SR-capable in Hello messages. • Source Active Interval—enter the time period (in seconds) for which the SR control messages are generated by the router after a data packet is received. The default value is 210 seconds. This value ranges from 120 to 210 seconds.
Buttons	• Add—adds and saves new configuration. • Reset—resets to default value and discards all user input.

PIM Route Configuration

Figure 26: PIM Route Configuration

PIM Route Information

ComponentID	AddrType	Group	Source	Mask	Vector	Upstream Neighbour	Incoming Interface	Pim Mode

Screen Objective	This screen allows the user to configure the <i>PIM</i> component parameters.
Navigation	Multicast > PIM > Route Info
Fields	• Component ID—enter a unique number to configure the <i>PIM</i> component. The PIM component corresponds to each instance of a <i>PIM</i> domain and classifies it as Sparse or Dense mode. This value ranges from 1 to 255. • Address Type—specifies the address type of the <i>PIM</i> interface— IPv4. • Group—displays the IP multicast group address for which the multicast routing information is displayed. • Source—displays the network address of the source. • Mask—displays the network mask of the source.

Fields (cont)	• Vector—displays <i>PIM</i> Reverse Path Forwarding vector (<i>RPF</i>) value. • Upstream Neighbour—displays the address of the upstream neighbor from which IP datagram sent to the multicast address are received • Incoming Interface—specifies the value of <i>IfIndex</i> (Upstream Interface Configuration) for the interface on which IP datagram sent to the multicast address are received. This is a read-only field. • PIM Mode—select <i>PIM</i> Mode of the group for which the Candidate <i>RP</i> is configured. The list contains: – Sparse—specifies that the Candidate <i>RP</i> is running in Sparse mode. – <i>Bidir</i>—specifies that the Candidate <i>RP</i> is running in <i>Bidir</i> mode.

PIM RP Configuration

Figure 27: PIM RP Configuration

PIM RP Information

Component	AddrType	Group	MaskLen	Candidate RP	Hold Time	Expiry Time	Pim Mode

Note : Pim Mode values

2: Sparse

4: Bidir

Screen Objective	This screen displays the PIM information for candidate <i>RP</i> s for IP multicast groups. The <i>PIM</i> information is obtained from received candidate <i>RP</i> advertisements, if the local router is <i>BSR</i> . The PIM information is obtained from received <i>RP</i> set messages if the local router is not <i>BSR</i> .
NOTE: This screen displays only if PIM module is enabled globally.	
Navigation	Multicast > PIM > RP Info
Fields	• Component ID—enter a unique number to configure the <i>PIM</i> component. The <i>PIM</i> component corresponds to each instance of a <i>PIM</i> domain and classifies it as Sparse or Dense mode. This value ranges from 1 to 255. • Address Type—specifies the address type of the <i>PIM</i> interface—IPv4. • Group—displays the IP multicast group address for which the information about the candidate <i>RP</i> is displayed. • Mask Length—displays the multicast group address mask. • Candidate RP—displays the IP address of the Candidate <i>RP</i>. • Hold Time—displays the time remaining for the advertisement of a Candidate <i>RP</i> to be aged out. This value range is from 0 to 255 seconds. This value is 0 for the local router that is not configured as <i>BSR</i>.

Fields	• Expiry Time—displays the minimum time remaining for the candidate <i>RP</i> to be declared as down. This value is 0 for the local router that is BSR. • PIM Mode—select PIM Mode of the group for which the Candidate <i>RP</i> is configured. The list contains: – Sparse—specifies that the Candidate <i>RP</i> is running in Sparse mode. – <i>Bidir</i>—specifies that the Candidate <i>RP</i> is running in <i>Bidir</i> mode

PIM High Availability

Figure 28: PIM High Availability

PIM High Availability

Pim HotStandby AdminStatus	Disabled ▾
Pim HotStandby Status	Init ▾
Pim HotStandby BulkUpdate Status	NotStarted ▾
Forwarding Table EntryCount	0

Screen Objective	This screen displays the <i>PIM</i> High Availability (<i>HA</i>) information for IP multicast groups.
NOTE: This screen displays only if <i>PIM</i> module is enabled globally.	
Navigation	Multicast > PIM > PIM HA
Fields	• PIM Hot Standby Admin Status—displays the status of the Hot Standby feature. The list contains: – Enabled—indicates the admin status is enabled. – Disabled—indicates the admin status is disabled. • PIM Hot Standby Status—displays the status of the PEER node. The list contains: – ActiveNodePeerUp—indicates standby-node is up. – ActiveNodePeerDown—indicates standby-node is down. • Pim Hot Standby Bulk Update Status—displays the synchronisation status between the active node and stand-by node. The list contains: – InProgress—active node is updating the info to standby. – Completed—active and standby node have synchronized the data. – NotStarted—active node doesn't start the synchronization yet. – Aborted—bulk update stopped while in progress. • Forwarding Table Entry Count—displays the number of entries available in forwarding path (data plane).

PIM Elected RP Information

Figure 29: Elected RP Information

PIM Elected RP Information	
ComponentID AddrType Group Mask RP Priority Hold Time	
Screen Objective	This screen displays the <i>PIM</i> Elected <i>RP</i> Information for IP multicast groups.
NOTE: This screen displays only if <i>PIM</i> module is enabled globally.	
Navigation	Multicast > PIM > Elected RP
Fields	• Component ID—enter a unique number to configure the <i>PIM</i> component. The <i>PIM</i> component corresponds to each instance of a <i>PIM</i> domain and classifies it as Sparse or Dense mode. This value ranges from 1 to 255. • Address Type—specifies the address type of the <i>PIM</i> interface— IPv4. • Group—displays the IP multicast group address for which the information about the candidate <i>RP</i> is displayed. • Mask—displays the multicast group address mask. • RP—displays the <i>RP</i> Address of the DF Election row. • Priority—displays the priority of the interface which will be advertised as a Candidate-<i>RP</i>. The priority value ranges from 0 to 255. The default value is 192. • Hold Time—displays the time remaining for the advertisement of a Candidate <i>RP</i> to be aged out. This value ranges from 0 to 255 seconds. This value is 0 for the local router that is not configured as <i>BSR</i>.

PIM DF Information

Figure 30: PIM DF Information

PIM DF Information	
AddrType RP Interface State Winner Uptime WinMetric WinMetricPref MsgCount	
Screen Objective	This screen displays the <i>PIM</i> <i>DF</i> (Designated Forwarder) information for IP multicast groups.
NOTE: This screen appears only if <i>PIM</i> module is enabled globally.	
Navigation	Multicast > PIM > DF Info

Fields	• Address Type—specifies the address type of the <i>PIM</i> interface— IPv4. • RP—displays the <i>RP</i> Address of the <i>DF</i> Election row. • Interface—displays the index value of the <i>PIM</i> interface. • State—displays the election state of the router for the specified <i>RP</i> address and interface. The options are offer, win, lose, or back off. • Winner—displays the address of the <i>DF</i> election winner for the specified <i>RP</i> address and interface. • Uptime—displays the uptime of the <i>DF</i> election winner for the specified <i>RP</i> address and interface. • Winner Metric—displays the address of the <i>DF</i> election winner for the specified <i>RP</i> address and interface. • Winner Metric Preference—displays the metric preference of the <i>DF</i> election winner for the specified <i>RP</i> to reach the <i>RP</i>. • Message Count—displays the number of <i>DF</i> messages sent by the router for the specified <i>RP</i> and interface.

22.5. IPv4 Multicasting

This section describes IPv4 Multicasting configuration.

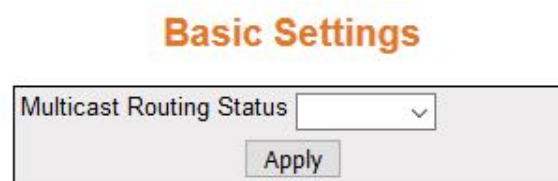
IP Multicasting is the transmission of an IP datagram to a "host group", a set of zero or more hosts identified by a single IP destination address. A multicast datagram is delivered to all members of its destination host group with the same "best-efforts" reliability as regular unicast IP datagrams, i.e., the datagram is not guaranteed to arrive intact at all members of the destination group or in the same order relative to other datagrams.

Reference: RFC 1112, "Host Extensions for IP Multicasting", <https://tools.ietf.org/html/rfc1112>

To access **IPv4 Multicasting** screens, go to **Multicast > IPv4 Multicasting**.

Basic Settings

Figure 31: Basic Settings



Screen Objective	This screen allows the user to configure the IPv4 Multicasting status.
Navigation	Multicast > IGMP > Basic Settings

Fields	• Multicast Routing Status—select the IPv4 Multicasting status of the switch. The default is Disabled. The drop-down list contains: – Enabled—enables IPv4 Multicasting. – Disabled—disables IPv4 Multicasting.
Buttons	• Apply—modifies attributes and saves the changes..

Interface Settings

Figure 32: Interface Settings

Interface Settings

Select	Interface Index	TTL	Protocol	Rate Limit	In Mcast Octets	Out Mcast Octets	HCIn Mcast Octets	HCOut Mcast Octets

Apply

Screen Objective	This screen allows the user to configure the Interface Settings .
Navigation	Multicast > IGMP > Interface Settings
Fields	• Select—select the index to modify the attributes of the selected entry. • Interface Index—enter the Interface Index. • TTL—enter the <i>TTL</i> (time to live). The <i>TTL</i> field in the IP header has a double significance in multicast. As always, it controls the live time of the datagram to avoid it being looped forever due to routing errors. Routers decrement the <i>TTL</i> of every datagram as it traverses from one network to another and when its value reaches 0 the packet is dropped. • Protocol • Rate Limit • In Mcast Octets • Out Mcast Octets • HCIn Mcast Octets • HCOut Mcast Octets
Buttons	• Apply—modifies attributes and saves the changes.

22.6. TAC

The Taxonomy Access Control (*TAC*) profile configuration is as shown below.

To access **TAC** screens, go to **Multicast > TAC**.

TAC Profile Configuration

Figure 33: TAC Profile Configuration

TAC Profile Configuration

Profile Id

Internet Address Type

Add

Reset

Configure Trace Options

Select	Profile ID	Internet Address Type	Profile Description	Profile Action	Port Reference Count	Vlan Reference Count	Profile Status
Apply Delete							

Screen Objective	This screen allows the user to configure the TAC Profile. TAC allows the user administrator to control access to nodes indirectly by controlling which roles can access which categories.
Navigation	Multicast > TAC Profile Configuration
Fields	Select—select the index to modify the attributes of the selected entry. Profile ID—enter the Profile ID. Internet Address Type—select Internet Address Type- IPv4. Profile Description Profile Action Port Reference Count VLAN Reference Count Profile Status
Buttons	Apply—modifies attributes and saves the changes.

23. 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. *RMON* provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

To access **RMON** screens, go to **RMON**.

The **Basic Settings** related parameters are configured through the screens displayed by the following tabs:

- [RMON Basic Settings](#)
- [RMON Alarm Configuration](#)
- [Ethernet Statistics Configuration](#)
- [Event Configuration](#)
- [History](#)

23.1. RMON Basic Settings

By default, the tab **RMON** displays the **RMON Basic Settings** screen.

Figure 1: RMON Basic Settings



Screen Objective	This screen allows the user to configure the <i>RMON</i> status. Once the status is enabled, monitoring of remote networks starts and data for storage in the table is collected.
Navigation	RMON > Basic Settings
Fields	RMON Status Map Name—select the <i>RMON</i> status of the switch. The default is Disabled. The drop-down list contains: - Enabled—enables <i>RMON</i> in the switch. - Disabled—disables <i>RMON</i> of the switch. When disabled, the <i>RMON</i>'s network monitoring is called off.
Buttons	Apply—modifies attributes and saves the changes.

23.2. RMON Alarm Configuration

Figure 2: RMON Alarm Configuration

RMON Alarm Configuration

Index *

Interval *

Variable *

Sample type ▾

Rising Threshold *

Falling Threshold *

Rising Event Index *

Falling Event Index *

Owner

Select	Index	Interval	Variable	Sample Type	Alarm Value	Startup Alarm	Rising Threshold	Falling Threshold	Rising Event Index	Falling Event Index	Owner	Status
Apply												

- Note:** 1. Variable has to be valid OID. Eg: 1.3.6.1.2.1.16.1.1.1.5.2
 2. Before setting the threshold values, corresponding ethernet index and events has to be created.
 3. Falling Threshold value has to be lesser than Rising Threshold value.
 4. To delete an entry, select a row, mark status as "Invalid" and give Apply

Screen Objective	This screen allows the user to configure <i>RMON</i> alarm settings. The Alarm group periodically takes statistical samples from variables in the probe and compares them to thresholds that have been configured. This is done to raise an alarm when the specified alarm condition occurs.
NOTE: RMON Events must be configured before Alarms can be configured	
Navigation	RMON > Alarms
Fields	Select—select the index to modify the attributes of the selected entry. Index—enter the value of <i>RMON</i> alarm table index. The index value uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular level for a <i>MIB</i> object in the device. This value ranges from 1 to 65535. Interval—enter the time interval in seconds for which the alarm monitors the <i>MIB</i> object variable. It is during this interval the data is sampled and compared with the rising and falling thresholds. This value ranges from 1 to 65535. Variable—enter the <i>MIB</i> object variable for which the alarm is set. For successful configuration, the variable has to be a valid Object ID. NOTE: This Object ID value refers to the OID of a particular variable in the <i>RMON MIB</i> that is to be monitored by the alarm entry. Sample Type—select the sample type to be compared against the thresholds. The default option is Absolute value. The list contains:

Fields(cont)	– Absolute value—compares the value of the selected variable directly with the thresholds at the end of the sampling interval. – Delta value—subtracts the value of the selected variable at the last sample from the current value and compares the difference with the thresholds at the end of the sampling interval. • Rising Threshold—enter the Rising Threshold value. This value ranges from 0 to 2147483647. NOTE: If the start-up alarm is set as Rising alarm or Rising Or Falling 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. • Falling Threshold—enter the Falling Threshold value. This value ranges from 0 to 2147483647. NOTE: The Falling Threshold value should be lesser than the Rising threshold value. If the start-up alarm is set as Falling alarm or Rising Or Falling 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. • Rising Event Index—enter the index of the event to be raised when the Rising threshold is reached. This value ranges from 1 to 65535. NOTE: The value of this field is same as Event Index in <i>RMON</i> Events Configuration. • Falling Event Index—enter the index of the event to be raised when the Falling threshold is reached. This value ranges from 1 to 65535. NOTE: The value of this field is same as Event Index in <i>RMON</i> Events Configuration. • Owner—enter the entity details that configured this entry and is using the resources assigned to it. • Alarm Value—displays the value of 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. • Startup Alarm—displays the alarm that is sent when the entry is set as valid for the first time. The list contains: – RisingAlarm—denotes that the first sample after the entry becoming valid is greater than or equal to the rising threshold. – FallingAlarm—denotes that the first sample after the entry becoming valid is less than or equal to the falling threshold. – RisingOrFallingAlarm—denotes that either Rising or Falling Alarm is sent based on the sample in comparison with the rising and falling threshold.

Fields (cont)	• Status—select the required status of alarm. The list contains: – Valid—sets the status as Valid if the entry is completely created. – Under Creation—sets the status as Under Creation if the entry is created and not completely configured – Entries in this state are not fully active. Entries exists in the “Under Creation” state until the management station has finished configuring the entry and sets this object to valid or invalid state. – Invalid—sets the status as Invalid if the entry is removed. It also effectively disassociates the mapping identified with the entry. NOTE: While creating a new <i>RMON</i> alarm entry, for invalid configurations, an error message is displayed, and the status is set as Under Creation.
Buttons	• Apply—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes and saves the changes.

23.3. Ethernet Statistics Configuration

Figure 3: Ethernet Statistics Configuration

Ethernet Statistics Configuration

Index *
Data Source *
Owner

Select	Index	Data Source	Drop Events	Octets	Packets	Broadcast Packets	Multicast Packets	Owner	Status
☒	2	1.3.6.1.2.1.2.2.1.1.1	0	0	0	0	0	iS5Com	Valid ▾

Note:1. Data Source has to be valid OID. Eg: 1.3.6.1.2.1.2.2.1.1.1 or 1.3.6.1.2.1.17.7.1.4.2.1.2.1

2. To delete an entry, select a row, mark status as "Invalid" and give Apply

Screen Objective	This screen contains statistics measured by the probe for each monitored interface on the device. The statistics in this group reflects all packets on the local network segment attached to the identified interface
Navigation	RMON > Ethernet Statistics
Fields	• Select—select the index to modify the attributes of the selected entry. • Index—enter the Ethernet Statistics index that uniquely identifies an entry in the Ethernet Statistics table. This value ranges from 1 to 65535.

Fields (cont)	• Data Source—enter the <i>SMNP</i> object ID of the variable on which the statistics is being collected. This object identifies the instance of the <i>ifIndex</i> object. For successful configuration the Data Source has to be a valid Object ID. NOTE: For e.g. 1.3.6.1.2.1.2.2.1.1.1 Index or 1.3.6.1.2.1.17.7.1.4.2.1.2.1 Index. Here, the value of Index depends upon the number of ports/VLAN created. • Owner—enter the details of the entity that configured this entry and is using the resources assigned to it. • Drop Events—displays the number of events in which the packets were dropped by the probe due to lack of resources. This number does not specify the number of packets dropped but the number of times the packets were dropped • Octets—displays the total number of octets of data received from the network (excluding the framing bits but including <i>FCS</i> octets). This can be used as a reasonable estimate of 10-Megabit Ethernet utilization. • Packets—displays the total number of packets received from the network. This includes bad packets, broadcast packets and multicast packets received. • Broadcast Packets—displays the total number of packets received that were directed to the broadcast address. • Multicast Packets—displays the total number of packets that were directed to the multicast address. • Status—select the required status of event. The list contains: – Valid—sets the status as Valid if the entry is completely created. – Under Creation—sets the status as Under Creation if the entry is created and not completely configure NOTE: Entries in this state are not fully active. Entries exists in the Under Creation state until the management station has finished configuring the entry and sets this object to valid or invalid state. – Invalid—sets the status as Invalid if the entry is removed. It also effectively disassociates the mapping identified with the entry.
Buttons	• Apply—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes and saves the changes.

23.4. Event Configuration

Figure 4: Event Configuration

Event Configuration

Event Index *

Description *

Type ▾

Community *

Owner

Select	Event Index	Description	Type	Community	Owner	Last Time Sent	Status
☒	34	event1	None ▾			0	Valid ▾

Note: To delete an entry, select a row, mark status as "Invalid" and Apply changes

Screen Objective	This screen contains statistics measured by the probe for each monitored interface on the device. The statistics in this group reflects all packets on the local network segment attached to the identified interface
Navigation	RMON > Events
Fields	• Select—select the index to modify the attributes of the selected entry. • Event Index—enter a number that uniquely identifies an entry in the Event Configuration table. Each such entry defines one event that is to be generated when appropriate conditions occur. This value ranges from 1 to 65535. • Description—enter a brief description of the event—a string of maximum size 127. NOTE: This field value accepts only Characters and number. • Type—select the type of event to be configured. This is the type of notification that the probe makes about this event. The list contains: – Log—creates an entry in the log table for each event. – SNMP Trap—sends an <i>SMNP</i> trap to one or more management stations. – Log and Trap—creates an entry in the log table and sends an <i>SMNP</i> trap. – None—sets the event type as None—no notifications are sent. NOTE: This field value accepts only Characters and number. • Community—enter <i>SMNP</i> community string to which the <i>SMNP</i> trap is to be sent. NOTE: This is relevant when an <i>SMNP</i> trap is requested for an event. • Owner—enter the entity that configured this entry and is using the resources assigned to it. • Last Time Sent—displays the time this event entry last generated an event. If this entry has not generated any events, the value will be zero.

Fields (cont)	• Status—select the required status of an event. The list contains: – Valid—sets the status as Valid if the entry is completely created. – Under Creation—choose if an entry is created but not quite configured. NOTE: Entries in this state are not fully active and exist in this state until the management station has finished configuring the entry and the object is set to valid or invalid state. • Invalid—sets the status as Invalid if the entry is removed. It also effectively disassociates the mapping identified with the entry.
Buttons	• Apply—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes and saves the changes.

23.5. History

Figure 5: History Control Configuration

History Control Configuration

Index *

Data Source *

Buckets Requested

Interval

Owner

Add Reset

Select	Index	Data Source	Buckets Requested	Buckets Granted	Interval	Owner	Status
☒	1	1.3.6.1.2.1.2.2.1.1.1	50	50	1800	Monitor	Valid ▾
Apply							

Note: 1. Data Source has to be a valid OID. Eg: 1.3.6.1.2.1.2.2.1.1.1 or 1.3.6.1.2.1.17.7.1.4.2.1.2.1
2. To delete an entry, select a row, mark status as "Invalid" and give Apply

Screen Objective	This screen allows the user to configure <i>RMON</i> history settings. The History module controls the periodic statistical sampling of the data collected by statistics module from various types of networks. This module stores the sample collected from the etherstat table in etherHistory table.
Navigation	RMON > History
Fields	• Select—select the index to modify the attributes of the selected entry. • Index—enter an integer value to identify an 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.

Fields (cont)	• Data Source—enter the <i>SMNP</i> object ID of the variable on which the statistics is being collected. This object identifies the instance of the <i>ifIndex</i> object. For successful configuration the Data Source has to be a valid Object ID. NOTE: For e.g. 1.3.6.1.2.1.2.2.1.1.1 Index or 1.3.6.1.2.1.17.7.1.4.2.1.2.1 Index. Here, the value of Index depends upon the number of ports/VLAN created. • Buckets Requested—enter the number of buckets to be configured for collecting the <i>RMON</i> statistics, that 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 entry. This value ranges from 1 to 65535. The default value is 50. • Interval—enter the time interval (in seconds) over which the data is sampled for each bucket to collect the statistics. This value ranges from 1 to 3600 seconds. The default value is 1800 seconds. • Owner—enter the details of the entity that configured this entry and is using the resources assigned to it. • Buckets Granted—displays the number of buckets granted for collecting the <i>RMON</i> statistics. This is the number of discrete sampling intervals over which data shall be saved in the part of the media-specific table associated with this History Control Entry. This value ranges from 1 to 65535. This is a read-only field. • Status—select the required status of event. The list contains: – Valid—sets the status as Valid if the entry is completely created. – Under Creation—sets the status as Under Creation if the entry is created and not completely configure NOTE: Entries in this state are not fully active. Entries exists in the Under Creation state until the management station has finished configuring the entry and sets this object to valid or invalid state. – Invalid—sets the status as Invalid if the entry is removed. It also effectively disassociates the mapping identified with the entry.
Buttons	• Apply—modifies attributes and saves the changes. • Reset—resets to default value for respective fields and discards all user input. • Apply—modifies attributes and saves the changes.

Statistics Map

24. Statistics

The **Statistics** link allows the user to view the various displays screens for the configurations applied to the system.

To access **Statistics** screens, click **Statistics**.

The various statistics screens for the different modules are available through the following links:

[*Interface*](#)

[*TCP/UDP*](#)

[*VLAN*](#)

[*MSTP*](#)

[*RSTP*](#)

[*PVRST*](#)

[*Link Aggregation*](#)

[*LLDP*](#)

[*802.1x*](#)

[*RADIUS*](#)

[*QoS*](#)

[*IGMP Snooping*](#)

[*IP*](#)

[*RIP*](#)

[*OSPF*](#)

[*IGMP*](#)

[*IGMP Proxy*](#)

[*IPv4 Multicasting*](#)

[*RMON*](#)

[*PTP*](#)

[*SNMP Agent*](#)

24.1. Interface

The **Interface** link allows the user to view the interface related statistics screens.

The following statistics screens are available.

[Interface Clear](#)

[Interface Statistics](#)

[Ethernet Statistics](#)

By default, the tab **Interface** displays the **Interface Statistics** screen.

Interface Clear

This screen allows the user to clear the interface counters for a particular interface or for all interfaces.

Figure 1:

Figure 2: Interface Clear

Clear Interface Statistics

Clear Interface Counters ☐ All
☒ Interface

Interface Gi0/1 ▼

Apply

Property	Description
Screen Objective	This screen allows the user to clear the interface counters for a particular interface or for all interfaces.
Navigation	Statistics > Interface > Interface Clear
Buttons	Apply —adds and saves new configuration.

Interface Statistics

This screen displays the management information applicable to all interfaces available in the switch.

Figure 3:

Figure 4: Interface Statistics**Interface Statistics**

Index	MTU	Speed (Bits Per Second)	Received Octets	Received Unicast Packets	Received Nunicast Packets	Received Discards	Received Errors	Received Unknown Protocols	Transmitted Octets	Transmitted Unicast Packets	Transmitted Nunicast Packets	Transmitted Discards	Transmitted Errors
Gi0/1	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/2	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/3	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/4	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/5	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/6	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/7	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/8	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/9	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/10	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/11	1500	1000000000	16206557	94580	55513	0	0	0	72244626	105783	37338	0	0
Gi0/12	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/13	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/14	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/15	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/16	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/17	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/18	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/19	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/20	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/21	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/22	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/23	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/24	1500	1000000000	0	0	0	0	0	0	0	0	0	0	0
Ex0/1	1500	4294967295	0	0	0	0	0	0	0	0	0	0	0
Ex0/2	1500	4294967295	0	0	0	0	0	0	0	0	0	0	0
Ex0/3	1500	4294967295	0	0	0	0	0	0	0	0	0	0	0
Ex0/4	1500	4294967295	0	0	0	0	0	0	0	0	0	0	0

Description	Properties
Screen Objective	This screen displays the management information applicable to all interfaces available in the switch.
Navigation	Statistics > Interface > Interface

Ethernet Statistics

This screen displays the statistics for a collection of Ethernet-like interfaces attached to the ISS.

Figure 5:

Figure 6: Ethernet Statistics

Ethernet Statistics

Index	Alignment Errors	FCS Errors	Single Collision Frames	Multiple Collision Frames	SQE Test Errors	Deferred Transmissions	Late Collisions	Excess Collisions	Transmitted Internal MAC Errors	Carrier Sense Errors	Frame Too Long	Received Internal MAC Errors	Ether ChipSet	Symbol Errors	Duplex Status
Gi0/1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/3	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/4	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Full-Duplex ▼
Gi0/5	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/6	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/7	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/8	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/9	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/10	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/11	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/12	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/13	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/14	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/15	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/16	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/17	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/18	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/19	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/20	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/21	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/22	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/23	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Gi0/24	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex ▼
Ex0/1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Full-Duplex ▼
Ex0/2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Full-Duplex ▼
Ex0/3	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Full-Duplex ▼
Ex0/4	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Full-Duplex ▼

Property	Description
Screen Objective	This screen displays the statistics for a collection of Ethernet-like interfaces attached to the ISS.
Navigation	Statistics > Interface > Ethernet

24.2. TCP/UDP

The **TCP/UDP** link allows the user to view the *TCP* and *UDP* statistics screens.

The following statistics screens may be viewed.

[TCP Statistics](#)

[TCP Listeners](#)

[TCP Connections](#)

[UDP Statistics](#)

[UDP Connections](#)

By default, the tab *TCP/UDP* displays the *TCP Statistics* screen.

TCP Statistics

This screen displays *TCP* related statistics details such as Min and Max Retransmission Timeout, Max Connections, etc. These statistics details allow the user to know the status of packets transferred using *TCP*.

Figure 7:

Figure 8: TCP Statistics

TCP Statistics

Context Id	RTO Algorithm Used	Min Retransmission Timeout	Max Retransmission Timeout	Max Connections	Active Opens	Passive Opens	Attempts Fail	Estab Resets	Current Estab	Input Segments	Output Segments	Retransmitted Segments	Input Errors	TCP Segments with RST flag Set	HC Input Segments	HC Output Segments
default	VANJACOBSON	50	2000	500	0	11961	0	2	1	96269	107773	81	10	1	96269	107773

Property	Description
Screen Objective	This screen displays <i>TCP</i> related statistics details such as Min and Max Retransmission Timeout, Max Connections, etc. These statistics details allow the user to know the status of packets transferred using <i>TCP</i> .
Navigation	Statistics > TCP > TCP Statistics

TCP Listeners

This screen displays information from the *TCP* listeners table, such as Local IP.

Figure 9:

Figure 10: TCP Listeners**Tcp Listeners**

Context Id	Local IP Address Type	Local Ip	Local Port
default	IPv4 ▾	0.0.0.0	22
default	IPv4 ▾	0.0.0.0	80
default	IPv4 ▾	0.0.0.0	443

Property	Description
Screen Objective	This screen displays information from the <i>TCP</i> listeners table, such as Local IP.
Navigation	Statistics > TCP > TCP Listeners

TCP Connections

This screen displays the information describing the status of the currently available *TCP* connections such as Remote IP, Local IP, their remote ports, states, etc.

Figure 11:**Figure 12:** TCP Connections**Tcp Current Connections**

Context Id	Local IP Address Type	Local Ip	Local Port	Remote IP Address Type	Remote IP	Remote Port	TCP State
0	IPv4 ▾	0.0.0.0	22	IPv4 ▾	00:00:00:00	0	Listen ▾
0	IPv4 ▾	0.0.0.0	80	IPv4 ▾	00:00:00:00	0	Listen ▾
0	IPv4 ▾	0.0.0.0	443	IPv4 ▾	00:00:00:00	0	Listen ▾
0	IPv4 ▾	192.168.10.1	80	IPv4 ▾	c0:a8:0a:0a	58875	Established ▾

Property	Description
Screen Objective	This screen displays the information describing the status of the currently available <i>TCP</i> connections such as Remote IP, Local IP, their remote ports, states, etc.
Navigation	Statistics > TCP > TCP Connections

UDP Statistics

This screen displays *UDP* related statistics details which allow the user to know the status of packets transferred using *UDP*.

Figure 13:

Figure 14: UDP Statistics

UDP Statistics

InDatagrams	18
No of Ports	12087
InErrors	12087
OutDatagrams	18
HC InDatagrams	18
HC OutDatagrams	18

Property	Description
Screen Objective	This screen displays <i>UDP</i> related statistics details which allow the user to know the status of packets transferred using <i>UDP</i> .
Navigation	Statistics > TCP > UDP Statistics

UDP Connections

This screen displays Local and Remote IP Address and Port type information about all current available UDP connections.

Figure 15:

Figure 16: UDP Connections**Udp Current Connections**

Local IP Address Type	Local Ip	Local Port	Remote IP Address Type	Remote Ip	Remote Port
IPv4 ▾	0.0.0.0	68	IPv4 ▾	0.0.0.0	0
IPv4 ▾	0.0.0.0	161	IPv4 ▾	0.0.0.0	0
IPv4 ▾	0.0.0.0	162	IPv4 ▾	0.0.0.0	0
IPv4 ▾	0.0.0.0	514	IPv4 ▾	0.0.0.0	0
IPv4 ▾	0.0.0.0	520	IPv4 ▾	0.0.0.0	0
IPv4 ▾	0.0.0.0	6123	IPv4 ▾	0.0.0.0	0
IPv4 ▾	0.0.0.0	6125	IPv4 ▾	0.0.0.0	0
IPv4 ▾	0.0.0.0	7000	IPv4 ▾	0.0.0.0	0
IPv4 ▾	0.0.0.0	9000	IPv4 ▾	0.0.0.0	0
IPv4 ▾	0.0.0.0	49152	IPv4 ▾	0.0.0.0	0
IPv4 ▾	0.0.0.0	49153	IPv4 ▾	0.0.0.0	0
IPv4 ▾	0.0.0.0	61812	IPv4 ▾	0.0.0.0	0
IPv4 ▾	0.0.0.0	61813	IPv4 ▾	0.0.0.0	0

Property	Description
Screen Objective	This screen displays Local and Remote IP Address and Port type information about all current available UDP connections.
Navigation	Statistics > TCP > UDP Connections

24.3. VLAN

The **VLAN** link allows the user to view the *VLAN* statistics screens.

The following statistics screens are available.

[Current Database](#)

[Port Statistics](#)

[Multicast Table](#)

[Counter Statistics](#)

[Capabilities](#)

[FDB Entries](#)

By default, the tab **VLAN** displays the **VLAN Current Database** screen.

Current Database

This screen displays the information for a *VLAN* that is configured or is dynamically created as a result of *GVRP* requests received. The information displayed includes the member ports, untagged ports, *VLAN* name and the status of that *VLAN* entry.

Figure 17:

Figure 18: Current DB

VLAN Current Database

VLAN ID	VLAN FDB ID	Member Ports	Untagged Ports	Status
1	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, Fx0/1, Fx0/2, Fx0/3, Fx0/4	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, Fx0/1, Fx0/2, Fx0/3, Fx0/4	Permanent

Property	Description
Screen Objective	This screen displays the information for a <i>VLAN</i> that is configured or is dynamically created as a result of <i>GVRP</i> requests received. The information displayed includes the member ports, untagged ports, <i>VLAN</i> name and the status of that <i>VLAN</i> entry.
Navigation	Statistics > VLAN > Current DB

Port Statistics

This screen displays the *VLAN*-related Port Statistics for all interfaces. The details include *VLAN* ID, number of valid frames received in the interface from the *VLAN*, number of valid frames transmitted through the interface to the *VLAN*, and number of frames discarded.

Figure 19: Port Statistics

VLAN Port Statistics

Port	VLAN ID	Received Frames	Transmitted Frames	Received Discards	Received Overflow	Transmitted Overflow	Transmitted Overflow Discards
Gi0/1	1	0	0	0	0	0	0
Gi0/2	1	0	0	0	0	0	0
Gi0/3	1	0	0	0	0	0	0
Gi0/4	1	0	0	0	0	0	0
Gi0/5	1	0	0	0	0	0	0
Gi0/6	1	0	0	0	0	0	0
Gi0/7	1	0	0	0	0	0	0
Gi0/8	1	0	0	0	0	0	0
Gi0/9	1	0	0	0	0	0	0
Gi0/10	1	0	0	0	0	0	0
Gi0/11	1	0	0	0	0	0	0
Gi0/12	1	0	0	0	0	0	0
Gi0/13	1	0	0	0	0	0	0
Gi0/14	1	0	0	0	0	0	0
Gi0/15	1	0	0	0	0	0	0
Gi0/16	1	0	0	0	0	0	0
Gi0/17	1	0	0	0	0	0	0
Gi0/18	1	0	0	0	0	0	0
Gi0/19	1	0	0	0	0	0	0
Gi0/20	1	0	0	0	0	0	0
Gi0/21	1	0	0	0	0	0	0
Gi0/22	1	0	0	0	0	0	0
Gi0/23	1	0	0	0	0	0	0
Gi0/24	1	0	0	0	0	0	0
Ex0/1	1	0	0	0	0	0	0
Ex0/2	1	0	0	0	0	0	0
Ex0/3	1	0	0	0	0	0	0
Ex0/4	1	0	0	0	0	0	0

Property	Description
Screen Objective	This screen displays the <i>VLAN</i> -related Port Statistics for all interfaces. The details include <i>VLAN</i> ID, number of valid frames received in the interface from the <i>VLAN</i> , number of valid frames transmitted through the interface to the <i>VLAN</i> , and number of frames discarded.
Navigation	Statistics > VLAN > Port Statistics

Multicast Table

This screen displays the information describing the status of the currently available *TCP* connections such as Remote IP, Local IP, their remote ports, states, etc.

Figure 20:

Figure 21: VLAN Multicast Table

VLAN Multicast Table

VLAN ID	Address	Egress Ports	Ports Learnt
1	01:00:5e:00:00:01	Gi0/9	None

Property	Description
Screen Objective	This screen displays the information describing the status of the currently available <i>TCP</i> connections such as Remote IP, Local IP, their remote ports, states, etc.
Navigation	Statistics > VLAN > Multicast Table

Counter Statistics

This screen displays the unicast / broadcast statistics details for all *VLANs* (both active and shutdown) created in the system. *VLAN* Counter Statistics collection can be enabled /disabled using the Counter Status field. By default, the statistics collection for *VLAN* is Disabled.

Figure 22:

Figure 23: Counter Statistics

VLAN Counter Statistics

Select	Context	VLAN ID	Unicast Frames Rx	Mcast/Bcast Frames Rx	Unknown Unicast Flooded	Unicast frames Tx	Broadcast frames Tx	Received Frames	Received Bytes	Transmitted Frames	Transmitted Bytes	Discarded Frames	Discarded Bytes	Counter Status
☒	0	1	0	0	0	0	0	0	0	0	0	0	0	Disabled ▾

Apply

Property	Description
Screen Objective	This screen displays the unicast / broadcast statistics details for all <i>VLANs</i> (both active and shutdown) created in the system. <i>VLAN</i> Counter Statistics collection can be enabled /disabled using the Counter Status field. By default, the statistics collection for <i>VLAN</i> is Disabled.
Navigation	Statistics > VLAN > Counter Statistics

Property	Description
Related screens	- VLAN Basic Settings screen (Layer 2 Management > VLAN > Basic Settings) - Static VLAN Configuration screen (Layer 2 Management > VLAN > Static VLANs) - VLAN Port mac MAP screen (Layer 2 Management > VLAN > Port MAC Map)
Buttons	Apply—adds and saves new configuration.

Capabilities

This screen displays the list of *VLAN* features supported in the switch.

Figure 24:

Figure 25: Capabilities

VLAN Capabilities

Extended filtering services Traffic classes Static Entry Individual port IVL capable SVL capable Hybrid capable Configurable Pvid Tagging

Property	Description
Screen Objective	This screen displays the list of <i>VLAN</i> features supported in the switch.
Navigation	Statistics > VLAN > Capabilities

FDB Entries

This screen displays information about a specific *MAC* address/ *VLAN* ID/ Port or all entries created in the *FDB* (Forwarding Database) table. These entries contain *MAC* address, member ports, receiver ports, and the status of entry.

Figure 26:

Figure 27: FDB Entries

VLAN FDB Entries

VLAN ID ☒

MAC Address ☐

Port ☐

All ☐

VLAN ID	MAC Address	Port	Status
1	54:e1:ad:07:0d:87	11	Learned

Property	Description
Screen Objective	This screen displays information about a specific about a specific <i>MAC</i> address/ <i>VLAN</i> ID/ Port or all entries created in the <i>FDB</i> table. These entries contain <i>MAC</i> address, member ports, receiver ports, and the status of entry.
Navigation	Statistics > VLAN > FDB Entries
Buttons	Show—shows the configuration. Reset—resets to default value for respective fields and discards all user inputs.

24.4. MSTP

The **MSTP** link allows the user to view the *MSTP* statistics screens.

Statistics screens are available through the following tabs.

Information

CIST Port Statistics

MSTI Port Statistics

By default, the tab **MSTP** displays the **MSTP Information** screen.

Information

This screen shows information pertinent to the Multiple Spanning Tree protocol (*MSTP*).

Figure 28:

Figure 29: Information

MSTP Information

Context Id	Bridge Address	CIST Root	Regional Root	CIST Root Cost	Regional Root Cost	Root Port	Hold Time	Max Age	Forward Delay	Config Digest	CIST Time Since Topology Change	Topology Changes
0	00:00:00:00:00:00	00:00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00:00	0	0	0	0	0	0	0	0	0

Property	Description
Screen Objective	This screen shows information pertinent to the <i>MSTP</i> .
Navigation	Statistics > MSTP > Information

CIST Port Statistics

This screen displays the various *MSTP* statistics involved in the ports available in the system.

Figure 30:

Figure 31: CIST Port Statistics

MSTP CIST Port Statistics

Clear Counters

Apply

Port	Received MST BPDUs	Received RST BPDUs	Received Config BPDUs	Received TCN BPDUs	Transmitted MST BPDUs	Transmitted RST BPDUs	Transmitted Config BPDUs	Transmitted TCN BPDUs	Received Invalid MST BPDUs	Received Invalid RST BPDUs	Received Invalid Config BPDUs	Received Invalid TCN BPDUs	Protocol Migration Count

Property	Description
Screen Objective	This screen displays the various <i>MSTP</i> statistics involved in the ports available in the system
Navigation	Statistics > MSTP > CIST Port Statistics

Property	Description
Fields	Clear Counters—select the option to update or clear the statistics for the interfaces on which <i>MSTP</i> is enabled.
Buttons	Apply—adds and saves new configuration.

Note: The parameters in the screen are not populated with values (the screen is blank) if the *MSTP* System Control status is set as Shutdown for the context selected using the Context Selection screen.

MSTI Port Statistics

This screen displays the various *MSTP* statistics involved in the ports available in the system.

Figure 32:

Figure 33: MSTI Port Statistics

MSTP CIST Port Statistics

Clear Counters

Port	Received MST BPDUs	Received RST BPDUs	Received Config BPDUs	Received TCN BPDUs	Transmitted MST BPDUs	Transmitted RST BPDUs	Transmitted Config BPDUs	Transmitted TCN BPDUs	Received Invalid MST BPDUs	Received Invalid RST BPDUs	Received Invalid Config BPDUs	Received Invalid TCN BPDUs	Protocol Migration Count

Property	Description
Screen Objective	This screen displays the various <i>MSTP</i> statistics involved in the ports available in the system
Navigation	Statistics > MSTP > MSTI Port Statistics

This screen displays statistics only if, the *MSTP* System Control status is set as Start for the context selected using the Context Selection screen. *MSTP* Instance is created using is created using the VLAN Mapping screen.

24.5. RSTP

The **RSTP** link allows the user to view the *RSTP* statistics screens.

RSTP statistics screens are available through the following tabs.

[Information](#)

Port Statistics

By default, the tab **RSTP** displays the **RSTP Information** screen.

Information

This screen shows the *RSTP* information on the bridges that supports the Spanning Tree protocol.

Figure 34:

Figure 35: RSTP Information

RSTP Information

Context Id	Protocol Specification	Time Since Topology Change	Designated Root	Root Brg Priority	Root Cost	Root Port	Max Age	Hello Time	Hold Time	Forward Delay
0	3	3	80.00.e8.e8.75.90.0b.01	32768	0	0	20	2	1	15

Property	Description
Screen Objective	This screen shows the <i>RSTP</i> information on the bridges that supports the Spanning Tree protocol.
Navigation	Statistics > RSTP > Information

NOTE: This screen displays the configuration details only for the context for which the *RSTP* System Control status is set as Start.

Port Statistics

This screen displays the *RSTP* statistics involved with each of the port available in the system like the role, state, transition state machine, various packet statistics, etc.

Figure 36:

Figure 37: Port Statistics

RSTP Port Statistics

Port	Received RST BPDUs	Received Configuration BPDUs	Received TCN	Transmitted RST BPDUs	Transmitted Configuration BPDUs	Transmitted TCN	Received Invalid RST BPDUs	Received Invalid Configuration BPDUs	Received Invalid TCN BPDUs	Protocol Migration Count	Effective Port State	EdgePort Oper Status	Link Type	PseudoRootId
Gi0/1	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/2	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/3	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/4	0	0	0	7397	0	0	0	0	0	0	Enable ▾	True ▾	P2P ▾	80:00:e8:e8:75:90:03:41
Gi0/5	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/6	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/7	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/8	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/9	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/10	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/11	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/12	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/13	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/14	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/15	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/16	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/17	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/18	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/19	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/20	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/21	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/22	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/23	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Gi0/24	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	Shared ▾	80:00:e8:e8:75:90:03:41
Ex0/1	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	P2P ▾	80:00:e8:e8:75:90:03:41
Ex0/2	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	P2P ▾	80:00:e8:e8:75:90:03:41
Ex0/3	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	P2P ▾	80:00:e8:e8:75:90:03:41
Ex0/4	0	0	0	0	0	0	0	0	0	0	Disable ▾	False ▾	P2P ▾	80:00:e8:e8:75:90:03:41

Property	Description
Screen Objective	This screen displays the <i>RSTP</i> statistics involved with each of the port available in the system like the role, state, transition state machine, various packet statistics, etc.
Navigation	Statistics > RSTP > Port Statistics
Fields	Clear Counters—select the option to update or clear the statistics for the interfaces on which <i>RSTP</i> is enabled.
Buttons	Apply—select the required entry to clear the counters.

NOTE: The parameters in the screen are not populated with values (the screen is blank) if the *RSTP* System Control status is set as Shutdown for the context selected using the Context Selection screen.

24.6. PVRST

The **PVRST** link allows the user to view the *PVRST* statistics.

PVRST statistics screens are available through the following tabs.

Information

Instance Information

Port Statistics

Instance Port Statistics

By default, the tab **PVRST** displays the **Basic Information** screen.

Information

This screen displays the *PVRST* information such as received *PVRST BPDUs*, maintained by every for port for each and every *PVRST* instance.

Figure 38:

Figure 39: Information

Basic Information

Context Id	0
Address	00:00:00:00:00:00

Property	Description
Screen Objective	This screen displays the <i>PVRST</i> information like Received <i>PVRST BPDUs</i> , maintained by every for port for each and every <i>PVRST</i> instance.
Navigation	Statistics > PVRST > Information

NOTE: The parameters in the screen are not populated with the values (the screen is blank) if the *PVRST* System Control status is set as Shutdown for the context selected using the Context Selection screen.

Instance Information

This screen displays the instance specific information, such as Root Cost, for the *PVRST* instances available in the switch.

Figure 40:

Figure 41: Instance Information

Instance Information

Context Id	Instance	Designated Root	Root Cost	Root Port	Max Age	Hello Time	Hold Time	Forward Delay	Time Since Topology Change	Topology Changes	Bridge Priority

Property	Description
Screen Objective	This screen displays the instance specific information, such as Root Cost, for the <i>PVRST</i> instances available in the switch.
Navigation	Statistics > PVRST > Instance Information

NOTE: The parameters in the screen are not populated with values (the screen is blank) if the *RSTP* System Control status is set as Shutdown for the context selected using the Context Selection screen.

Port Statistics

This screen displays the various *PVRST* info statistics involved with each port available in the system such as Received Invalid *PVRST* info *BPDUs*, Received Invalid Configuration *BPDUs* and so on.

Figure 42:

Figure 43: Port Statistics

Port Statistics

Port	Received Invalid PVRST BPDUs	Received Invalid Configuration BPDUs	Received Invalid TCN BPDUs

Property	Description
Screen Objective	This screen displays the various <i>PVRST</i> info statistics involved with each port available in the system such as Received Invalid <i>PVRST</i> info <i>BPDUs</i> , Received Invalid Configuration <i>BPDUs</i> and so on.
Navigation	Statistics > PVRST > Port Status

NOTE: The parameters in the screen are not populated with the values (the screen is blank) if the *PVRST* info System Control status is set as Shutdown for the context selected using the Context Selection screen.

Instance Port Statistics

This screen displays the *PVRST* information like Received *PVRST BPDUs* maintained by every for port for each and every *PVRST* instance.

Figure 44:

Figure 45: Instance Port Statistics

Instance Port Statistics								
Instance	Port	Received Pvrst BPDUs	Received Config BPDUs	Received TCN BPDUs	Transmitted Pvrst BPDUs	Transmitted Config BPDUs	Transmitted TCN BPDUs	Protocol Migration Count

Property	Description
Screen Objective	This screen displays the <i>PVRST</i> information like Received <i>PVRST BPDUs</i> , maintained by every for port for each and every <i>PVRST</i> instance.
Navigation	Statistics > PVRST > Instance Port Statistics

NOTE: The parameters in the screen are not populated with the values (the screen is blank) if the *PVRST* System Control status is set as Shutdown for the context selected using the Context Selection screen.

24.7. MRP

The **MRP** link allows the user to view the *MRP* statistics screens.

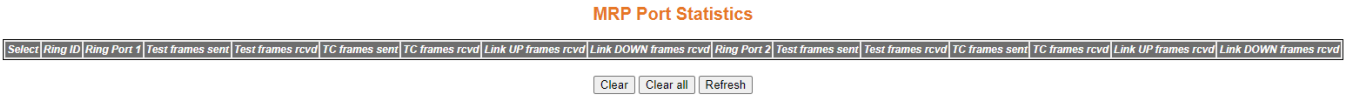
MRP statistics screens are available by navigating to statistics and then to the *MRP* option.

MRP Statistics

This screen displays the *MRP* statistics.

Figure 46:

Figure 47: MRP Statistics



Property	Description
Screen Objective	This screen displays the <i>MRP</i> statistics.
Navigation	Statistics > MRP > Port Statistics
Buttons	Clear—select the required entry to clear the counters. Clear All—clear all of the counters. Refresh —refresh all of the counters.

24.8. Link Aggregation

The **Link Aggregation** link allows the user to view the Link Aggregation (*LA*) statistics.

Link Aggregation statistics screens are available through the following tabs.

[Link Aggregation Port Statistics](#)

[Link Aggregation Neighbour Statistics Information](#)

By default, the tab **Link Aggregation** displays the **Link Aggregation Port Statistics** screen.

Link Aggregation Port Statistics

This screen shows the displays the Link Aggregation (*LA*) Protocol statistics for each port on the device.

Figure 48:

Figure 49: Link Aggregation Port Statistics**Link Aggregation Port Statistics**

Port	Received PDUs	Received Marker PDUs	Received Marker Response	Received Unknown PDUs	Received Illegal PDUs	Transmitted PDUs	Transmitted Marker PDUs	Transmitted Marker Response
Gi0/1	0	0	0	0	0	0	0	0
Gi0/2	0	0	0	0	0	0	0	0
Gi0/3	0	0	0	0	0	0	0	0
Gi0/4	0	0	0	0	0	0	0	0
Gi0/5	0	0	0	0	0	0	0	0
Gi0/6	0	0	0	0	0	0	0	0
Gi0/7	0	0	0	0	0	0	0	0
Gi0/8	0	0	0	0	0	0	0	0
Gi0/9	0	0	0	0	0	0	0	0
Gi0/10	0	0	0	0	0	0	0	0
Gi0/11	0	0	0	0	0	0	0	0
Gi0/12	0	0	0	0	0	0	0	0
Gi0/13	0	0	0	0	0	0	0	0
Gi0/14	0	0	0	0	0	0	0	0
Gi0/15	0	0	0	0	0	0	0	0
Gi0/16	0	0	0	0	0	0	0	0
Gi0/17	0	0	0	0	0	0	0	0
Gi0/18	0	0	0	0	0	0	0	0
Gi0/19	0	0	0	0	0	0	0	0
Gi0/20	0	0	0	0	0	0	0	0
Gi0/21	0	0	0	0	0	0	0	0
Gi0/22	0	0	0	0	0	0	0	0
Gi0/23	0	0	0	0	0	0	0	0
Gi0/24	0	0	0	0	0	0	0	0
Ex0/1	0	0	0	0	0	0	0	0
Ex0/2	0	0	0	0	0	0	0	0
Ex0/3	0	0	0	0	0	0	0	0
Ex0/4	0	0	0	0	0	0	0	0

Property	Description
Screen Objective	This screen shows the displays the Link Aggregation (LA) Protocol statistics for each port on the device
Navigation	Statistics > Link Aggregation > Link Aggregation Port Statistics

Link Aggregation Neighbour Statistics Information

This screen displays the Neighbor statistics for each port on the device.

Figure 50:

Figure 51: LA Neighbour Statistics Information

LA Neighbour Statistics Information

Port	Partner SystemID	Oper Key	Partner Port Priority
Gi0/1	00:00:00:00:00:00	0	0
Gi0/2	00:00:00:00:00:00	0	0
Gi0/3	00:00:00:00:00:00	0	0
Gi0/4	00:00:00:00:00:00	0	0
Gi0/5	00:00:00:00:00:00	0	0
Gi0/6	00:00:00:00:00:00	0	0
Gi0/7	00:00:00:00:00:00	0	0
Gi0/8	00:00:00:00:00:00	0	0
Gi0/9	00:00:00:00:00:00	0	0
Gi0/10	00:00:00:00:00:00	0	0
Gi0/11	00:00:00:00:00:00	0	0
Gi0/12	00:00:00:00:00:00	0	0
Gi0/13	00:00:00:00:00:00	0	0
Gi0/14	00:00:00:00:00:00	0	0
Gi0/15	00:00:00:00:00:00	0	0
Gi0/16	00:00:00:00:00:00	0	0
Gi0/17	00:00:00:00:00:00	0	0
Gi0/18	00:00:00:00:00:00	0	0
Gi0/19	00:00:00:00:00:00	0	0
Gi0/20	00:00:00:00:00:00	0	0
Gi0/21	00:00:00:00:00:00	0	0
Gi0/22	00:00:00:00:00:00	0	0
Gi0/23	00:00:00:00:00:00	0	0
Gi0/24	00:00:00:00:00:00	0	0
Ex0/1	00:00:00:00:00:00	0	0
Ex0/2	00:00:00:00:00:00	0	0
Ex0/3	00:00:00:00:00:00	0	0
Ex0/4	00:00:00:00:00:00	0	0

Property	Description
Screen Objective	This screen displays the Neighbor statistics for each port on the device.
Navigation	Statistics > Link Aggregation > Link Aggregation Neighbour Statistics Information

24.9. LLDP

The **LLDP** (Link Layer Discovery Protocol) link allows the user to view the *LLDP* statistics.

LLDP statistics screens are available through the following tabs.

Traffic Information

Statistics Information

Error Information

By default, the tab **LLDP** displays the **Traffic Information** screen.

Traffic Information

This screen displays the Traffic information.

Figure 52:

Figure 53: Traffic Information

Traffic Information

Interface	Frames out	Entries Aged	Frames In	Frames Rx in Error	Frames Discarded	Unreconized TLVs	Total TLVs Discarded	PDU length error Drops
Gi0/1	3152	0	118	0	0	0	0	0
Gi0/2	3152	0	118	0	0	0	0	0
Gi0/3	3152	0	118	0	0	0	0	0
Gi0/4	3152	0	118	0	0	0	0	0
Gi0/5	3152	0	118	0	0	0	0	0
Gi0/6	3152	0	118	0	0	0	0	0
Gi0/7	3152	0	118	0	0	0	0	0
Gi0/8	3152	0	118	0	0	0	0	0
Gi0/9	3152	0	118	0	0	0	0	0
Gi0/10	3152	0	118	0	0	0	0	0
Gi0/11	3152	0	118	0	0	0	0	0
Gi0/12	3152	0	118	0	0	0	0	0
Gi0/13	3152	0	118	0	0	0	0	0
Gi0/14	3152	0	118	0	0	0	0	0
Gi0/15	3152	0	118	0	0	0	0	0
Gi0/16	3152	0	118	0	0	0	0	0
Gi0/17	3152	0	118	0	0	0	0	0
Gi0/18	3152	0	118	0	0	0	0	0
Gi0/19	3152	0	118	0	0	0	0	0
Gi0/20	3152	0	118	0	0	0	0	0
Gi0/21	3152	0	118	0	0	0	0	0
Gi0/22	3152	0	118	0	0	0	0	0
Gi0/23	3152	0	118	0	0	0	0	0
Gi0/24	3152	0	118	0	0	0	0	0
Ex0/1	3152	0	118	0	0	0	0	0
Ex0/2	3152	0	118	0	0	0	0	0
Ex0/3	3152	0	118	0	0	0	0	0
Ex0/4	3152	0	118	0	0	0	0	0

Clear LLDP Counters

Property	Description
Screen Objective	This screen allows the user to view or clear the <i>LLDP</i> counters on specified interface. This includes the following for each interface: • Total Frames Out • Total Entries Aged • Total Frames In • Total Frames Received in Error • Total Frames Discarded • Total TLVS Unrecognized • Total TLVs Discarded • PDU Length error drops
Navigation	Statistics > LLDP > Traffic
Buttons	• Clear LLDP Counters—clears the <i>LLDP</i> counters on all interfaces.

Statistics Information

This screen displays the *LLDP* remote table statistics information.

Figure 54:

Figure 55: Statistics Information

Statistics Information

Remote Table Last Change Time	40930500
Remote Table Inserts	6
Remote Table Deletes	5
Remote Table Drops	0
Remote Table Ageouts	0
Remote Table Updates	0

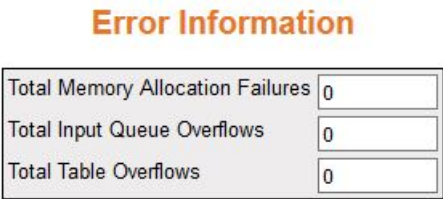
Property	Description
Screen Objective	This screen displays the <i>LLDP</i> remote table statistics information.
Navigation	Statistics > LLDP > Statistics

Error Information

This screen displays the *LLDP* remote table statistics information.

Figure 56:

Figure 57: Error Information



Property	Description
Screen Objective	This screen displays the <i>LLDP</i> remote table statistics information.
Navigation	Statistics > LLDP > Errors

24.10. 802.1x

The **802.1x** link allows the user to view the *802.1x* statistics.

802.1x statistics screens are available through the following tabs.

[802.1x Session Statistics](#)

[802.1x Supplicant Statistics Information](#)

[MAC Session Statistics](#)

By default, the tab **802.1x** displays the **Traffic Information** screen.

802.1x Session Statistics

This screen displays the session statistics for an authenticator *PAE* (Port Access Entity). It shows the current values collected for each session that is still in progress or the final values for the last valid session on each port where there is no current active session.

Figure 58:

Figure 59: 802.1x Session Statistics

802.1x Session Statistics

Port	Session ID	Received Frames	Transmitted Frames	Session Time (secs)	Session Terminate Cause	User Name
Gi0/1	31:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/2	32:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/3	33:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/4	34:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/5	35:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/6	36:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/7	37:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/8	38:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/9	39:2d:30	243595	390190	429600	Not Terminated Yet	4e:6f:20:55:73:65:72
Gi0/10	31:30:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/11	31:31:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/12	31:32:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/13	31:33:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/14	31:34:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/15	31:35:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/16	31:36:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/17	31:37:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/18	31:38:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/19	31:39:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/20	32:30:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/21	32:31:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/22	32:32:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/23	32:33:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Gi0/24	32:34:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Ex0/1	32:35:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Ex0/2	32:36:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Ex0/3	32:37:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72
Ex0/4	32:38:2d:30	0	0	75430400	Admin Disabled	4e:6f:20:55:73:65:72

Property	Description
Screen Objective	This screen displays the session statistics for an authenticator <i>PAE</i> (Port Access Entity). It shows the current values collected for each session that is still in progress or the final values for the last valid session on each port where there is no current active session.
Navigation	Statistics > 802.1x > Session Stats

802.1x Supplicant Statistics Information

This screen displays the Supplicant Session Statistics.

Figure 60:

Figure 61: 802.1x Supplicant Statistics Information

802.1x Supplicant Session Statistics

Port	Eapol FrRx	Eapol FrTx	Eapol Start FrTx	Eapol Logoff FrTx	Eapol Respld FrTx	Eapol Resp FrTx	Eapol Reqld FrRx	Eapol Req FrRx	Invalid Eapol FrRx	Eap LenErr FrRx	Last Eapol FrVersion	Last Eapol FrSource
Gi0/1	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/2	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/3	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/4	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/5	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/6	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/7	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/8	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/9	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/10	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/11	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/12	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/13	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/14	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/15	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/16	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/17	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/18	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/19	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/20	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/21	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/22	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/23	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/24	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Ex0/1	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Ex0/2	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Ex0/3	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Ex0/4	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00

Property	Description
Screen Objective	This screen displays the Supplicant Session Statistics.
Navigation	Statistics > 802.1x > Supp-Session Stats

MAC Session Statistics

This screen displays the MAC Session statistics.

Figure 62:

Figure 63: MAC Session Statistics

MAC Session Statistics

Select	Supplicant MacAddr	Frames Rx	Frames Tx	Session ID	Session Terminate Cause	User Name

Property	Description
Screen Objective	This screen displays the MAC Session statistics.
Navigation	Statistics > 802.1x > MAC-Session Stats

24.11. RADIUS

This screen displays the *RADIUS* Server statistics.

Figure 64:

Figure 65: RADIUS Server Statistics

Radius Server Statistics

Index	Radius Server Address	UDP Port Number	Round Trip Time	No of Request Packets	No of Retransmitted Packets	No of Access-Accept Packets	No of Access-Reject Packets	No of Access-Challenge Packets	No of Malformed Access Responses	No of Bad Authenticators	No of Pending Requests	No of Time Outs	No of Unknown Types

Property	Description
Screen Objective	This screen displays the <i>RADIUS</i> Server statistics.
Navigation	Statistics > RADIUS

24.12. QoS

The **QoS** (Quality of Service) link allows the user to view the *QoS* statistics screens.

QoS statistics screens are available through the following tabs. By default, the tab **QoS** displays the **Policer Stats** screen.

[QoS Policer Statistics](#)

[QoS CoS Statistics](#)

QoS Policer Statistics

This screen displays the *QoS* Policer statistics.

Figure 66:

Figure 67: QoS Policer Statistics

QoS PolicerStats	
ConformPkts ConformOctets ExceedPkts ExceedOctets ViolatePkts ViolateOctets	
Property	Description
Screen Objective	This screen displays the <i>QoS Policer</i> statistics.
Navigation	Statistics > QoS > Policer Statistics

QoS CoS Statistics

This screen displays the *QoS CoS* Statistics information

Figure 68:**Figure 69:** QoS CoS

QoS CoS Stats							
CoSQEnQPkts	CoSQEnQBytes	CoSQDeQPkts	CoSQDeQBytes	CoSDiscardPkts	CoSQDiscardBytes	CoSQStatsOccupancy	CoSQStatsCongMgmtAlgoDrop
00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00

Property	Description
Screen Objective	This screen displays the <i>QoS CoS</i> Statistics information
Navigation	Statistics > QoS > Cos Stats

24.13. IGMP Snooping

The **IGMP Snooping** (Internet Group Management Protocol) allows the user to view the *IGMP* Snooping related statistics.

IGMP Snooping-related statistics screens are available through the following tabs.

[IGMP Snooping Clear Statistics](#)

[IGMP Snooping V1/V2 Statistics](#)

[IGMP Snooping V3 Statistics](#)

By default, the tab **IGMP Snooping** displays the **IGMP Snooping Clear Statistics** screen.

IGMP Snooping Clear Statistics

This screen clears the *IGMP VLAN* counters for a particular VLAN.

Figure 70:

Figure 71: IGMP Snooping Clear Statistics

IGMP Snooping Clear Statistics

Clear Vlan Counters
☐ All
☒ Vlan ID

Vlan ID

Property	Description
Screen Objective	This screen clears the <i>IGMP VLAN</i> counters for a particular <i>VLAN</i> .
Navigation	Statistics > IGMP Snooping > IGS Clear Statistics
Buttons	Apply—clears the counters.

IGMP Snooping V1/V2 Statistics

This screen displays the *IGMP* snooping statistics pertaining to *IGMP* Snooping v1 & v2.

Figure 72:

Figure 73: IGMP Snooping V1/V2 Statistics

IGMP Snooping V1/V2 Statistics

VLAN ID	General Queries Received	Group Queries Received	Group and Source Queries Received	IGMP Reports Received	IGMP Leaves Received	IGMP Packets Dropped	General Queries Transmitted	Group Queries Transmitted	IGMP Reports Transmitted	IGMP Leaves Transmitted

Property	Description
Screen Objective	This screen displays the <i>IGMP</i> snooping statistics pertaining to <i>IGMP</i> Snooping v1 & v2.

Property	Description
Navigation	Statistics > IGMP Snooping > IGS Statistics

IGMP Snooping V3 Statistics

This screen displays the *IGMP* snooping statistics pertaining to *IGMP* snooping v3.

Figure 74:

Figure 75: IGMP Snooping V3 Statistics

IGMP Snooping V3 Statistics

VLAN ID	V3 Reports Received	IS_INCL Messages Received	IS_EXCL Messages Received	TO_INCL Messages Received	TO_EXCL Messages Received	ALLOW Messages Received	BLOCK Messages Received	V3 Reports Sent

Property	Description
Screen Objective	This screen displays the <i>IGMP</i> snooping statistics pertaining to <i>IGMP</i> snooping v3.
Navigation	Statistics > IGMP Snooping > IGS V3 Statistics

24.14. IP

The **IP** allows the user to view the IPv4-related statistics screens.

IPv4-related statistics screens are available through the following tabs.

[ARP Cache](#)

[ICMP Statistics](#)

[IPv4 Interface Specific Statistics](#)

[IPv4 System Specific Statistics](#)

By default, the tab **IP** displays the **ARP Cache** screen.

ARP Cache

This screen displays the *ARP* (Address Resolution Protocol) cache related statistics information, such as *MAC* address for all interfaces of the switch.

Figure 76:

Figure 77: ARP Cache

ARP Cache

Interface	MAC Address	IP Address	Media Type
vlan1	54:e1:ad:07:0d:87	192.168.10.10	Dynamic

Property	Description
Screen Objective	This screen displays the <i>ARP</i> (Address Resolution Protocol) cache related statistics information, such as <i>MAC</i> address for all interfaces of the switch.
Navigation	Statistics > IP > ARP Cache

ICMP Statistics

This screen displays the *ICMP* transmission and reception related statistics information such as Received Redirect, Transmitted Error, etc.

Figure 78:**Figure 79:** ICMP Statistics

ICMP Statistics

Received Message	0
Received Error	0
Receive Destination Unreachable	0
Received Redirect	0
Received Echo Requests	0
Received Echo Replies	0
Receive Source Quenches	0
Transmitted Message	3
Transmitted Error	0
Transmitted Destination Unreachable	3
Transmitted Redirect	0
Transmitted Echo Requests	0
Transmitted Echo Replies	0
Transmitted Source Quenches	0

Property	Description
Screen Objective	This screen displays the <i>ICMP</i> transmission and reception related statistics information such as Received Redirect, Transmitted Error, etc.
Navigation	Statistics > IP > ICMP Statistics

IPv4 Interface Specific Statistics

This screen displays IPv4 interface specific statistics information (e.g. HClInOct).

Figure 80:

Figure 81: IPv4 Interface Specific Statistics

IPv4 Interface Specific Statistics															
VersionType	Iface	HCRcvd	HClInOct	Hdr Errs	InNoRoutes	Adr Errs	UnknownProtos	Truncd Pkts	HCFowardDatagrams	Reasm Reqds	Reasm OKs	Reasm Fails	Discdrs	HClInDelivers	
IPv4	37	44532	3776777	21	0	0	0	0	0	0	0	0	0	44146	

HCOut Rqst	HCOut FwdDgms	Out Discards	Out FragRqds	Out FragOKs	Out FragFails	Frag Creates	HCOut Transmits	HCOutOct	HCRcvd Mcast Pkts	HCRcvd Mcast Octs	HCSend Mcast Pkts	HCSend Mcast Octs	HCRcvd Bcast Pkts	HCSend Bcast Pkts	DisConty time	Refresh Rate
35186	0	0	0	0	0	0	35186	23397436	2224	151083	0	0	0	0	0	1000

Property	Description
Screen Objective	This screen displays IPv4 interface specific statistics information (e.g. HClInOct).
Navigation	Statistics > IP > IPv4 IfSp Stats

IPv4 System Specific Statistics

This screen displays IPv4 specific global statistics information such as HCRcvd.

Figure 82:

Figure 83: IPv4 System Specific Statistics

IPv4 System Specific Statistics															
VersionType	HCRcvd	HCInOct	Hdr Errs	InNoRoutes	Adr Errs	UnknownProtos	Trunctd Pkts	HCForwardDatagrams	Reasm Reqs	Reasm OKs	Reasm Fails	Discdrs	HCInDelivers		
IPv4	44757	3796452	21	0	0	0	0	0	0	0	0	0	44371		

HCOut Rqst	HCOut FwdDgms	Out Discards	Out FragRqds	Out FragOks	Out FragFails	Frag Creates	HcOut Transmits	HCOutOct	HCRcvd Mcast Pkts	HCRcvd Mcast Octs	HCSend Mcast Pkts	HCSend Mcast Octs	HCRcvd Bcast Pkts	HCSend Bcast Pkts	DisConty time	Refresh Rate
35383	0	0	0	0	0	0	35383	23536738	1838	151083	0	0	0	0	0	1000

Property	Description
Screen Objective	This screen displays IPv4 specific global statistics information such as HCRcvd.
Navigation	Statistics > IP > IPv4 SysSp Stats

24.15. RIP

This screen displays the collection of statistics pertaining to *RIP*.

Figure 84:**Figure 85:** RIP Interface Statistics

RIP Interface Statistics

Context Id	IP Address	Received Bad Packets	Received Bad Routes	Triggered Updates	Periodic Updates

Property	Description
Screen Objective	This screen displays the collection of statistics pertaining to <i>RIP</i> .
Navigation	Statistics > RIP

24.16. OSPF

The *OSPF* link allows the user to view the *OSPF*-related statistics screens.

OSPF-related statistics screens are available through the following tabs.

[OSPF Route Information](#)[Link State Database](#)[Redundancy Information](#)

By default, the tab **OSPF** displays the **OSPF Route Information** screen.

OSPF Route Information

This screen displays the collection of statistics pertaining to *OSPF* Route Information.

Figure 86:

Figure 87: OSPF Route Information

OSPF Route Information

Context Name	IP Address	Subnet Mask	TOS	Gateway	Type	Area ID	Cost	Type 2 Cost	Interface

Property	Description
Screen Objective	This screen displays the collection of statistics pertaining to <i>OSPF</i> Route Information.
Navigation	Statistics > OSPF > OSPF Route Information

Link State Database

This screen displays the collection of statistics pertaining to *OSPF* Link State Database.

Figure 88:

Figure 89: OSPF Link State Database

OSPF Link State Database

Context Id	Area ID	Type	Link State ID	Router ID	Sequence	Checksum	Age

Property	Description
Screen Objective	This screen displays the collection of statistics pertaining to <i>OSPF</i> Link State Database.
Navigation	Statistics > OSPF > Link State Database

Redundancy Information

This screen the collection of statistics pertaining to *OSPF* Redundancy Information.

Figure 90:

Figure 91: OSPF Redundancy Information

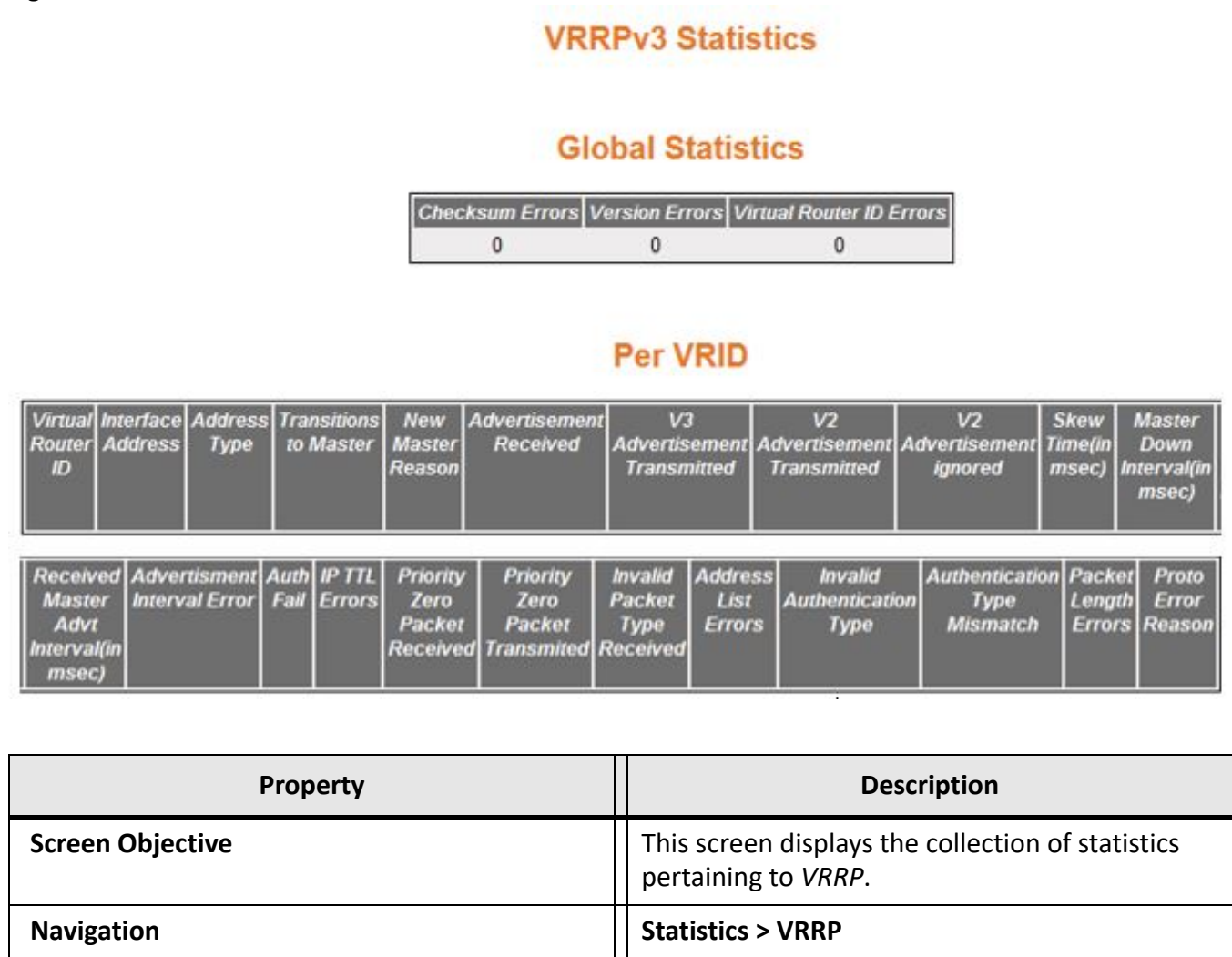
OSPF Redundancy Information

HotStandby Admin State	Disabled
HotStandby State	Active StandbyDown
HotStandby Bulk Update Status	Not Started
No Of Hellos Synced	0
No Of LSAs Synced	0

Property	Description
Screen Objective	This screen the collection of statistics pertaining to <i>OSPF</i> Redundancy Information.
Navigation	Statistics > OSPF > Redundancy Information

24.17. VRRP

This screen displays the collection of statistics pertaining to *VRRP*.

Figure 92: VRRPv3 Statistics

24.18. IGMP

This screen displays the collection of statistics pertaining to *IGMP*.

Figure 93:**Figure 94:** IGMP Statistics

IGMP Statistics

Interface	General queries received	Group queries received	Group and source queries received	V1/V2 reports received	V3 reports received	General queries transmitted	Group queries transmitted	Group and source queries transmitted

Property	Description
Screen Objective	This screen displays the collection of statistics pertaining to <i>IGMP</i> .
Navigation	Statistics > IGMP

24.19. IGMP Proxy

This screen displays the collection of statistics pertaining to *IGMP* Proxy.

Figure 95:

Figure 96: IGMP Proxy Statistics

IGMP Proxy Statistics

Interface	V1/V2 reports transmitted	V3 reports transmitted	V2 Leaves transmitted

Property	Description
Screen Objective	This screen displays the collection of statistics pertaining to <i>IGMP</i> .
Navigation	Statistics > IGMP Proxy

24.20. IPv4 Multicasting

The *IPv4* Multicasting link allows the user to view the *IPv4*-related statistics screens through the following tabs.

[Route Statistics](#)

[VRRP](#)

By default, the tab **IPv4 Multicasting** displays the **Route Statistics** screen.

Route Statistics

This screen displays the collection of statistics pertaining to *IPv4* Multicasting.

Figure 97:

Figure 98: Route Statistics**Route Statistics**

Group	Source	Source Mask	Upstream Neighbour	Incoming Interface Index	Up Time(sec)	Expiry Time(sec)	Received Packets	Dropped Packets	Received Octets	MRoute Protocol	Route Protocol	Route Address	Route Mask	Route Type	Received HC Octets

Property	Description
Screen Objective	This screen displays the collection of statistics pertaining to IPv4 Multicasting.
Navigation	Statistics > IPv4 Multicasting > Route Statistics

Next Hop Statistics

This screen displays the collection of statistics pertaining to *IPv4* Multicasting.

Figure 99:**Figure 100:** Next Hop Statistics**Next Hop Statistics**

Group	Source	Source Mask	Outgoing Interface Index	Next-Hop Address	State	Up Time(sec)	Expiry Time(sec)	Next-Hop Routing Protocol	Packets Forwarded

Property	Description
Screen Objective	This screen displays the collection of statistics pertaining to <i>IPv4</i> Next Hop Statistics.
Navigation	Statistics > IPv4 Multicasting > Next Hop Statistics

24.21. RMON

This screen displays the collection of statistics pertaining to *RMON*.

Figure 101:

Figure 102: RMON Ethernet Statistics

RMON Ethernet Statistics																
Index	Data Source	Drop Events	Packets	Octets	Broadcast Packets	Multicast Packets	CRC Errors	Under Size Packets	Over Size Packets	Fragments	Jabbers	Collisions	Out FCS Errors	64 Octets	65-127 Octets	128-255 Octets
2	1.3.6.1.2.1.2.1.1.1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
256-511 Octets	512-1023 Octets	1024-1518 Octets	Overflow Packets	Overflow Octets	Overflow 64 Octets	Overflow 65-127 Octets	Overflow 128-255 Octets	Overflow 256-511 Octets	Overflow 512-1023 Octets	Overflow 1024-1518 Octets						
0	0	0	0	0	0	0	0	0	0	0						

Property	Description
Screen Objective	This screen displays the collection of statistics pertaining to <i>RMON</i> .
Navigation	Statistics > RMON

NOTE: This screen displays the statistics only if the Ethernet Statistics are configured using RMON > Ethernet Statistics screen.

24.22. PTP

This screen displays the *PTP* Ports statistics information.

Figure 103:

Figure 104: PTP Port Statistics

PTP Port Statistics											
Context	Domain	Port	Sync Messages Received Count	Discarded PTP Message Count	Transmitted Sync Message Count	Received Peer Delay Request Message Count	Transmitted Peer Delay Request Message Count	Received Peer Delay Response Message Count	Transmitted Peer Delay Response Message Count	Transmitted Peer Delay Response Follow Up Message Count	Received Peer Delay Response Follow Up Message Count
0	254	1	0	0	0	0	0	0	0	0	0
0	254	2	0	0	0	0	0	0	0	0	0
0	254	3	0	0	0	0	0	0	0	0	0
0	254	4	0	0	0	0	0	0	0	0	0
0	254	5	0	0	0	0	0	0	0	0	0
0	254	6	0	0	0	0	0	0	0	0	0
0	254	7	0	0	0	0	0	0	0	0	0
0	254	8	0	0	0	0	0	0	0	0	0
0	254	9	0	0	0	0	0	0	0	0	0
0	254	10	0	0	0	0	0	0	0	0	0
0	254	11	0	0	0	0	0	0	0	0	0
0	254	12	0	0	0	0	0	0	0	0	0
0	254	13	0	0	0	0	0	0	0	0	0
0	254	14	0	0	0	0	0	0	0	0	0
0	254	15	0	0	0	0	0	0	0	0	0
0	254	16	0	0	0	0	0	0	0	0	0
0	254	17	0	0	0	0	0	0	0	0	0
0	254	18	0	0	0	0	0	0	0	0	0
0	254	19	0	0	0	0	0	0	0	0	0
0	254	20	0	0	0	0	0	0	0	0	0
0	254	21	0	0	0	0	0	0	0	0	0
0	254	22	0	0	0	0	0	0	0	0	0
0	254	23	0	0	0	0	0	0	0	0	0
0	254	24	0	0	0	0	0	0	0	0	0

Property	Description
Screen Objective	This screen displays the <i>PTP</i> Ports statistics information.
Navigation	Statistics > PTP

24.23. SNMP Agent

This screen displays the statistics information related to *SNMP* Agent.

Figure 105:

Figure 106: SNMP Statistics

SNMP Statistics	
SNMP Packets Input	32
BAD SNMP Version Errors	0
SNMP Unknown Community Name	64
SNMP Get Request PDU's	0
SNMP Get Next PDU's	0
SNMP Set Request PDU's	0
SNMP Packet Output	32
SNMP Too Big Errors	0
SNMP No Such Name Errors	1
SNMP Bad Value Errors	0
SNMP General Errors	0
SNMP Trap PDU's	0
SNMP Manager-Role Output Packets	0
SNMP Inform Responses Received	0
SNMP Inform Request Generated	0
SNMP Inform Messages Dropped	0
SNMP Inform Requests awaiting Acknowledgement	0

Property	Description
Screen Objective	This screen displays the statistics information related to <i>SNMP</i> Agent.
Navigation	Statistics > SNMP > Agent

NOTE: This screen can be viewed only if the option Agent is selected in the *SNMP* Agent Control Settings screen.

24.24. Serial

This screen displays the Serial Port statistics information.

Figure 107:

Figure 108: Serial Port Statistics**Serial Port Statistics**

<i>Port</i>	<i>Rx</i>					<i>Tx</i>		
	<i>Char Count</i>	<i>Frame Count</i>	<i>Char Discard</i>	<i>Framing Errors</i>	<i>Parity Errors</i>	<i>Char Count</i>	<i>Frame Count</i>	<i>Char Discarded</i>
Se0/9	0	0	0	0	0	0	0	0
Se0/10	0	0	0	0	0	0	0	0
Se0/11	0	0	0	0	0	0	0	0
Se0/12	0	0	0	0	0	0	0	0

Property	Description
Screen Objective	This screen displays the Serial Port statistics information.
Navigation	Statistics > Serial

PoE

25. Power over Ethernet (PoE)

25.1. Power Over Ethernet

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.

25.2. PoE Global Configuration

Use the **PoE Global Configuration** dialog box to enable *PoE* on the switch, configure the maximum power draw and the detection mode of the *PoE* devices.

To access **PoE Global Configuration** screen, go to **PoE > Global Configuration**.

PoE Global Configuration

Figure 1: PoE Global Configuration

PoE Global Configuration

Global Status	Disabled ▾
Main Power	720 *
Detect Mode	Legacy ▾ *
Apply	

Screen Objective	This screen allows the user to configure the global settings of <i>PoE</i> .
Navigation	PoE > Global Configuration
Global Status	Enable/Disable the PoE ports across the entire switch.
Main Power	This is the total available power provided by the external <i>PoE</i> power supply. It is manually entered by the user and should be a value between 100 and 6000 (Watts).
Detect Mode	Legacy or Strict. This determines how a PoE device is discovered by the switch.
Buttons	Apply—modifies attributes and saves the changes.

25.3. PoE Port Settings

Use the **PoE Port Settings** dialog box to configure *PoE* settings on individual ports.

To access **PoE Port Settings** screen, go to **PoE > PoE Port Settings**.

PoE Port Settings

Figure 2: PoE Global Port Settings

PoE Port Settings

Select	Port Group	Port Number	Admin Status	Max Pairs	Power Priority	Detection Status	Power Classifications	Power Consumption	MPS Absent Counter	Invalid Signature Counter	Power Denied Counter	Overload Counter	Short Counter
☐	1	1	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	2	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	3	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	4	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	5	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	6	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	7	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	8	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	9	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	10	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	11	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	12	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	13	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	14	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	15	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	16	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	17	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	18	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	19	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	20	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	21	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	22	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	23	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0
☐	1	24	Disabled ▼	Two ▼	low ▼	Other Fault	Class 0	0.00 W	0	0	0	0	0

Screen Objective	This screen allows the user to configure the port settings for <i>PoE</i> .
Navigation	PoE > PoE Port Settings
Admin Status	Enable/Disable the <i>PoE</i> capabilities of the port. If the port is enabled, it will auto detect end devices for <i>PoE</i> capability. If the port is disabled <i>PoE</i> , capability will be disabled.
Max Pairs	Use this drop down to specify if <i>PoE</i> power is to provided on up to two or four wire pairs. 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 <i>PoE</i> power; however, to ensure power consumption limits, the adjacent port (odd/even combination) needs to be disabled before this can be set.
Power Priority	Priority related configuration. The <i>PoE</i> 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 <i>PoE</i> 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.
Buttons	• Apply—modifies attributes and saves the changes. • Select—this radial button selects the port where changes should be made and applied to.

Advanced Security Features

26. Security

The **Security** features listed in this section are exclusive to the iMX950 and include the interfaces needed to enable *IPSec*, *NAT*, and *Firewall*.

26.1. NAT

This section describes Network Address Translation (*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. 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.

Address translation allows hosts in a private network to transparently communicate with destinations on an external network and vice versa.

NAT binds addresses in private network with addresses in global network and vice versa to provide transparent routing for the datagrams traversing between address realms. 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.

To access **NAT** screens, go to **Layer 3 Management > Security > NAT**.

NAT Global Configuration

Figure 1: NAT Global Configuration

NAT Global Configuration

NAT Status	Enabled ▾
NAT Debug Level	▾
Typical Number of Entries	300 ▴ ▾
Total Number of Translations	0
Number of Active Sessions	0
Apply	

Screen Objective	This screen allows the user to configure the <i>NAT</i> Global Configuration.
Navigation	Layer 3 Management > Security > NAT > NAT Global Configuration
Fields	• NAT Status—select the status of <i>NAT</i>. The default option is disabled. The list contains: – Enabled – Disabled • NAT Debug Level—select the status of <i>NAT</i>. The list contains: – None—configures <i>NAT</i> debug to none. – All—configures <i>NAT</i> debug to all level.s • Total Number of Entries—enter number of entries. • Total Number of Translations—enter number of translations. • Number of Active Sessions—enter number of active sessions.
Buttons	• Apply—select to safe the configuration.

Static SNAT Configuration

Figure 2: Static SNAT Configuration

Static SNAT Configuration

Interface	vlan55 ▾ *
Source IP Address	*
Translated Source IP Address	*
Add Reset	

Select	Interface	Source IP Address	Translated Source IP Address
Delete			

Screen Objective	This screen allows the user to configure the static mapping between local IP address and translated IP address on a particular interface.
Navigation	Layer 3 Management > Security > NAT > Static SNAT Configuration
Fields	• Interface—select the interface for which the <i>NAT</i> configuration needs to be modified or deleted. • Source IP Address—enter the Source IP address for the host from the private inside network • Translated Source IP Address—enter the IP address that should be used for the packets sent from the host to the outside network.
Buttons	• Add—adds and saves new configuration. • Reset—resets the configuration. • Delete—delete the selected entry.

Dynamic SNAT Configuration

Figure 3: Dynamic SNAT Configuration

Dynamic SNAT Configuration

Interface vlan55 *

Network IP Address *

Network Mask *

Translated IP Start *

Translated IP End *

Add
Reset

Select	Interface	Network IP	Network Mask	Translated IP Start	Translated IP End
☐	Gi0/4	192.168.10.0	255.255.255.0	80.0.0.10	80.0.0.20

Delete

Screen Objective	This screen allows the user to enable <i>DNAT</i> for all protocols (<i>TCP/UDP</i>) and ports on a particular interface.
Navigation	Layer 3 Management > Security > NAT > Dynamic SNAT Configuration
Fields	Interface—select the interface for which the <i>NAT</i> configuration needs to be modified or deleted. Network IP Address—enter the network IP address for the host from the private inside network Network Mask—enter the network mask for the host from the private inside network Translated IP Start—enter the translated IP start address that should be used for the packets sent from the host to the outside network. Translated IP End—enter the translated IP end address that should be used in the packets sent from the host to the outside network.
Buttons	Add—adds and saves new configuration. Reset—resets the configuration. Delete—delete the selected entry.

NAPT Configuration

Figure 4: NAT Configuration

NAPT Configuration

Interface vlan55 *

Usage NAPT for all Packets *

Add

Reset

Select	Interface	Source IP Address	Source Mask	Source Port	Protocol	Translated IP Address	Translated Port	Status

Delete

NAPT Configuration

Interface vlan55 *

Usage Network Translation *

Source IP Address

Source Mask

Add

Reset

Select	Interface	Source IP Address	Source Mask	Source Port	Protocol	Translated IP Address	Translated Port	Status

Delete

NAPT Configuration

Interface vlan55 *

Usage Single IP Translation *

Source IP Address

Source Port Number

0

Translated Source IP Address

Translated Port Number

0

Protocol TCP

Add

Reset

Select	Interface	Source IP Address	Source Mask	Source Port	Protocol	Translated IP Address	Translated Port	Status

Delete

Screen Objective	This screen allows the user to enable Network Address Port Translation (NAPT) for a particular interface with options for network translation and single IP translation.
Navigation	Layer 3 Management > Security > NAT > NAPT Configuration

Fields	• Select—click to select the entry for which the <i>NAPT</i> configuration needs to be modified or deleted. • Interface—select the interface for which the <i>NAPT</i> configuration needs to be modified or deleted. • Usage—specify the <i>NAPT</i> scope by selecting option from the drop-down list: – NAPT for all Packets – Network Translation NOTE: If this option is selected, 2 new fields appear and are available for entering data: Source IP Address and Source Mask. – Single IP Translation NOTE: If this option is selected, 4 new fields appear and are available for entering data: Source IP Address, Source Port Number, Translated Source IP Address, and Translated Port Number. • Source IP Address—enter / displays the actual IP address of the host connected to inside network. • Source Mask—enter / displays the mask for the host from the private inside network. • Source Port Number—select /displays the source port number used as a source transport identifier. • Protocol—select a protocol to be used for transport identifier from the drop-down list/ displays the protocol used for the packets. There are 2 options: – TCP—choose Transmission Control Protocol (<i>TCP</i>) to deliver and receive an ordered and error-checked stream of information packets over the network – UDP—choose User Datagram Protocol (<i>UDP</i>) to deliver a faster stream of information without error-checking. • Translated IP Address—enter / displays the translated IP address that should be used as destination IP address for the packets. • Translated Port Number Port—enter / displays the translated port number used as destination transport identifier for the packets. • Status—displays the status of the <i>NAPT</i> Configuration.
Buttons	• Add—adds and saves new configuration. • Reset—resets the configuration. • Delete—delete the selected entry.

Destination NAT Configuration

Figure 5: Destination NAT Configuration**Destination NAT Configuration**

Interface	Gi0/1 *
Destination IP Address	*
Destination Port Number	0 *
Translated IP Address	*
Translated Port Number	0 *
Protocol	TCP *
Add Reset	

Select	Interface	Destination IP Address	Destination Port Number	Translated IP Address	Translated Port Number	Protocol
Delete						

Screen Objective	This screen allows the user to configure the destination <i>NAT</i> configuration on a selected interface.
Navigation	Layer 3 Management > Security > NAT > Destination NAT Configuration
Fields	• Interface—select the interface for which the <i>NAT</i> configuration needs to be modified or deleted. • Destination IP Address—enter / displays the destination IP address. • Destination Port Number—select / displays the number of destination port number used as transport identifier. • Translated IP Address—enter / displays the translated IP start address for the packets. • Translated Port Number—select / displays the number of destination port used as transport identifier. • Protocol—select a protocol from the drop-down list/ displays the protocol used for the packets. There are 2 options: – TCP—choose Transmission Control Protocol (<i>TCP</i>) to deliver and receive an ordered and error-checked stream of information packets over the network – UDP—choose User Datagram Protocol (<i>UDP</i>) to deliver a faster stream of information without error-checking.
Buttons	• Add—adds and saves new configuration. • Reset—resets the configuration. • Delete—delete the selected entry.

All NAT Configurations

Figure 6: All NAT Configurations

All NAT Configurations

Static SNAT Configurations

Interface	Source IP	Translated IP

Dynamic SNAT Configurations

Interface	Network IP	Network Mask	Translated IP Start	Translated IP End
Gi0/4	192.168.10.0	255.255.	80.0.0.10	80.0.0.20

NAPT Configurations

Interface	Source IP	Source Mask	Source Port	Protocol	Translated IP	Translated Port

Destination NAT Configurations

Interface	Destination IP	Destination Port	Translated IP	Translated Port	Protocol

Screen Objective	This screen displays information about all parameters in Static <i>SNAT</i> Configuration, Dynamic <i>SNAT</i> Configuration, <i>NAPT</i> Configuration, and DNAT Configuration.
Navigation	Layer 3 Management > Security > NAT > All NAT Configuration

Active Connections

Figure 7: Active Connections

Active Connections

IP Version	Protocol	Timeout	Request Source IP	Request Source Port	Request Destination IP	Request Destination Port	Request Packets	Response Source IP	Response Source Port	Response Destination IP	Response Destination Port	Response Packets

Screen Objective	This screen displays information about all active connections.
Navigation	Layer 3 Management > Security > NAT > Active Connections

26.2. VPN

Internet Protocol Security (*IPSec*) is described in this section.

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.

IPSec VPN is designated for simple Point-to-Point Protocol (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)**

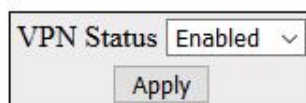
This mode is referred to as Policy-based. The interesting traffic is defined at the IPsec policy. Since there is no additional IP interface created specifically for the tunnel source, the IPsec policy must define both the interesting traffic source/ destination and the network interfaces source/ destination.

To access **VPN** screens, go to **Layer 3 Management > Security > VPN**.

VPN Global Configuration

Figure 8: VPN Global Configuration

VPN Global Configuration



The screenshot shows a configuration window titled "VPN Global Configuration". Inside, there is a dropdown menu labeled "VPN Status" with "Enabled" selected. Below the dropdown is an "Apply" button.

Screen Objective	This screen allows the user to configure the <i>VPN</i> Global Configuration.
Navigation	Layer 3 Management > Security > VPN > Global Configuration
Fields	• VPN Status—the options are (with a default option Disabled): – Enabled—select to activate <i>VPN</i>. – Disabled—select to discontinue the <i>VPN</i>.
Buttons	• Apply—modifies attributes and saves the changes.

How IPSec Works

IPSec involves many component technologies and encryption methods. Yet *IPSec*'s operation can be broken down into five main steps:

- 1) "Interesting traffic" or *IPSec* Policy Configuration initiates the *IPSec* process. Traffic is deemed interesting when the *IPSec* security policy configured in the *IPSec* peers starts the IKE process.
- 2) IKE phase 1— *IKE* authenticates *IPSec* peers and negotiates IKE SAs during this phase, setting up a secure channel for negotiating *IPSec* SAs in phase 2.

- 3) IKE phase 2— *IKE* negotiates *IPSec SA* parameters and sets up matching *IPSec SAs* 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 SAs* terminate through deletion or by timing out.

IKE phase 1 occurs in two modes: main mode and aggressive mode.

IPSec Policy Configuration

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. An *IPSec* policy determines the 'interesting traffic' i.e. the type or subset of the customer traffic to be encrypted.

Internet Security Association and Key Management 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. In endpoint-to-endpoint Transport Mode, both end points of the IP connection implement *IPSec*.

IKE Phase 1 Configuration

Internet Key Exchange (*IKE*) protocol is a component of *IPSec* used for performing mutual authentication and establishing and maintaining Security Associations (*SAs*) (RFC 7296)

Once an *IKE* negotiation is successfully completed, the peers have established two pairs of one-way (inbound and outbound) *SAs*. Since *IKE* always negotiates pairs of *SAs*, the term "*SA*" is generally used to refer to a pair of *SAs* (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*.

IKE Phase 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 data-gram as clear text 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.
- 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 x_a (her private key) and then calculates $y_a = g^{x_a} \bmod p$ (which is her public key). Party B chooses a private key x_b , and calculates his public key in the same way as $y_b = g^{x_b} \bmod p$.

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:

$ZZ = g^{(x_b * x_a)} \bmod p = (y_b^{x_a}) \bmod p = (y_a^{x_b}) \bmod p$, where ZZ is their shared secret as defined by X9.42. For more details, refer to RFC 2631 [8].

Any eavesdropper who was listening in on the communication knows p , g , and both parties public keys y_a and y_b . 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 (KM). The KM 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 Modes

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. The session flow is as follows:

- 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's a secure channel.

IKE Phase 2

The purpose of *IKE* Phase 2 is to negotiate IPsec SAs. *IKE* phase 2 performs the following functions:

- Negotiates IPsec SA parameters protected by an existing *IKE SA*
- Establishes IPsec security associations
- Periodically renegotiates IPsec SAs 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 Protocol (ESP) or Authentication Header (AH)). To select a transform set, consider the following:
 - For data confidentiality, include an ESP.
 - 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—options are tunnel and transport modes
- Perfect Forward Secrecy— Perfect forward secrecy (PFS) means that 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 perfect forward secrecy (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.

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. It is an attempt to subvert security by someone who records legitimate communications and repeats them in order to impersonate a valid user, and to disrupt or cause negative impact for legitimate connections.

IPsec provides anti-replay protection against an attacker who duplicates encrypted packets with the assignment of a monotonically increasing sequence number to each encrypted packet. The receiving IPsec endpoint keeps track of which packets it has already processed on the basis of these numbers with the use of a sliding window of all acceptable sequence numbers.

ACK Packets

This section lists off some details of how 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.

VPN Policy Configuration

Figure 9: VPN Policy Configuration

VPN Policy Configuration

Policy Action	☐ Create
Policy Name	cybsec *
Existing Policies	cybsec ▾
Policy Status	Inactive ▾ *
Local ID Type	IPv4 ▾
Local ID	1
Local Endpoint IP Address	255.255.255.255
Peer ID Type	IPv4 ▾
Peer ID	1
Peer Endpoint IP Address	255.255.255.255
Traffic Selector	
Local Subnets	192.168.0.0/16 ...
Remote Subnets	10.10.3.0/24 ...
IKE (Phase 1) Proposal	
IKE Version	IKEv2 ▾
IPSec Encryption	▾ *
IPSec Authentication	HMAC-SHA1 ▾ *
DH Group	Group 1 ▾ *
Exchange	Main ▾
Life Time	Minutes ▾ *
Life Time Value	20 ... *
PreShared Key	
IKE (Phase 2) Proposal	
Protocol	ESP ▾ *
Encryption	AES-128 ▾
Authentication	HMAC-SHA-256 ▾
IPSec Mode	Tunnel ▾ *
Preferred Forward Secrecy	Group 15 ▾ *
Life Time	Minutes ▾
Life Time Value	2 ...
Anti Replay	ENABLE ▾
Apply Delete	

Note: ACTIVE Policies cannot be modified.
In order to modify a policy, please set the Policy Status to INACTIVE.

**Screen
Objective**

This screen allows the user to configure the VPN Policy Configuration.

Navigation	Layer 3 Management > Security > VPN > Policy Configuration
Fields	• Policy Action—add a check mark to create a new <i>VPN IPSec</i> policy. • Policy Name—enter a name for the new <i>VPN IPSec</i> policy. NOTE: This field is grayed out and cannot be configured if the Policy Action is not checked. • Existing Policies—select from the drop-down list and choose a policy from the list. NOTE: This field is grayed out and cannot be configured if the Policy Action is checked. • Policy Status—select status for the selected <i>VPN IPSec</i> policy. The default option is Inactive. – Active—select to activate the selected policy (i.e. the <i>IPSec</i> processing has started) – Inactive—select to deactivate the selected policy (i.e. the <i>IPSec</i> processing has stopped). • Local ID Type—select address type of network address which represents the local protected network. IPv4 shown. • Local ID—specify the identity of the local endpoint configuration to be used by the router when participating in the Internet Key Exchange (<i>IKE</i>) protocol. It configures local identity type and its value to be used in <i>IKE</i> Phase 1. It can be a format for email, fqdn, dn, or key id. The options are: – dn <string>—specify domain name for local identity value. As shown in VPN Policy Configuration dialog box, to dn is assigned a value of 1. – email <string>— specify email address for local identity value. – fqdn <string>—fully Qualified Domain Name for local identity value. – keyId <string>—key Identifier related information for local identity value. • Local Endpoint IP Address—enter IPv4 address related information for local identity value. • Peer ID Type—Select address type of network address which represents the remote endpoint configuration. IPv4 shown. • Peer ID—specify the identity of the remote endpoint configuration to be used by the router when participating in the <i>IKE</i> protocol. It can be a format for email, fqdn, dn, or key id. The options are: – dn <string>—specify domain name for local identity value. As shown in VPN Policy Configuration dialog box, to dn is assigned a value of 1. – email <string>— specify email address for local identity value. – fqdn <string>—fully qualified domain name for local identity value. – keyId <string>—key Identifier related information for local identity value.

Fields (cont)	• Peer Endpoint IP Address—enter IPv4 address related information for the remote endpoint. • Traffic Selector – Local Subnets—enter information for the remote endpoint. The format is A.B.C.D/E or <ip/subnet>. – Remote Subnets—enter information for the remote endpoint. The format is A.B.C.D/E or <ip/subnet>. • IKE (Phase 1) Proposal – IKE Version—select <i>IKE</i> version. • IKEv1 —select <i>IKEv1</i> if you don't need NAT traversal (not supported) • IKEv2—select it 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. – IPSec Encryption—selects encryption algorithm: • 3DES—sets the ESP algorithm type as 3DES • AES-128—sets the <i>AES</i> to 128 bits key-length for encrypting / decrypting a block of message • AES-192—sets the <i>AES</i> to 192 bits key-length for encrypting / decrypting a block of message • AES-256—sets the <i>AES</i> to 256 bits key-length for encrypting / decrypting a block of message. – IPSec Authentication—select authentication hash algorithm. • HMAC-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. • HMAC-SHA1—sets the hash to Secure Hash Algorithm <i>SHA-1</i> (160 bit) • HMAC-SHA256—sets the hash to Secure Hash Algorithm <i>SHA-2</i> (256 bit) • HMAC-SHA384—sets the hash to Secure Hash Algorithm <i>SHA-2</i> (384 bit) • HMAC-SHA512—sets the hash to Secure Hash Algorithm <i>SHA-1</i> (512 bit) – DH Group—select a Diffie-Hellman (DH) group for the IKE policy. DH key exchange is the method of securely exchanging cryptographic keys over a public channel. The options are: • Group1—specifies use of 768-bit DH Group 1 cryptography • Group2—specifies use of 1024-bit DH Group 2 cryptography • Group5—specifies use of 1536-bit DH Group 5 cryptography

Fields (cont)	• IKE (Phase 1) Proposal (cont) – DH Group (cont) • Group14—specifies use of 2048-bit DH Group 14 cryptography • Group15—specifies use of 3072-bit DH Group 15 cryptography • Group16—specifies use of 4096-bit DH Group 16 cryptography • Group17—specifies use of 6144-bit DH Group 17 cryptography • Group18—specifies use of 8192-bit DH Group 18 cryptography – Exchange—select IKE exchange mode. The exchange modes are Main and Aggressive. The current version available is Main. Main Mode is a more secure option for Phase1 as it involves the identity protection. – Life Time—specifies the time an SA will live before expiring. Shorter lifetimes can make it harder to mount a successful key recovery attack, since the attacker has less data encrypted under the same key to work with. However, shorter lifetimes require more CPU processing time for establishing new SAs. Its units are secs/mins/hrs as shown below: • Seconds • Minutes • Hours – Life Time Value—enter life time value. – PreShared Key—enter PreShared key value. • IKE (Phase 2) Proposal – Protocol—select an IPSec security protocol. The options are: • AH—specify Authentication header (AH) • ESP—specify encapsulating security payload (ESP) NOTE: if you select AH, the encryption algorithm is preset to None and the Encryption field is dimmed. – Encryption—some of the offered options are for AES Counter Mode (AES-CTR). 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. The following options are available for selection: • None—select it for no encryption. • 3DES—sets the ESP algorithm type as 3DES • AES-128—sets the AES to 128 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.

Fields (cont)	• Encryption (cont) – AES-CTR-128—sets the <i>AES-CTR</i> to 128 bits key-length for encrypting / decrypting a block of message – AES-CTR-192—sets the <i>AES-CTR</i> to 192 bits key-length for encrypting / decrypting a block of message – AES-CTR-256—sets the <i>AES-CTR</i> to 256 bits key-length for encrypting / decrypting a block of message. – blowfish—sets the <i>AES</i> to 256 bits key-length for encrypting / decrypting a block of message. • Authentication—select authentication hash algorithm. – HMAC-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. – HMAC-SHA1—sets the hash to Secure Hash Algorithm SHA-1 (160 bit) – XCBC-MAC—sets the hash to XCBC-MAC – HMAC-SHA256—sets the hash to Secure Hash Algorithm SHA-2 (256 bit) – HMAC-SHA384—sets the hash to Secure Hash Algorithm SHA-2 (384 bit) – HMAC-SHA512—sets the hash to Secure Hash Algorithm SHA-1 (512 bit) • IPSec Mode—select <i>IPSec</i> mode. Options are: – 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. • Preferred Forward Secrecy—enables Perfect Forward Secrecy (PFS) related configuration. • None—select for no PFC. • PFC Group 1—specifies use of 768-bit DH Group 1 cryptography • PFC Group 2—specifies use of 1024-bit DH Group 2 cryptography • PFC Group 5—specifies use of 1536-bit DH Group 5 cryptography • PFC Group 14—specifies use of 2048-bit DH Group 14 cryptography • Group 15—specifies use of 3072-bit DH Group 14 cryptography • Group 16—specifies use of 4096-bit DH Group 16 cryptography • Group 17—specifies use of 6144-bit DH Group 17 cryptography • Group 18—specifies use of 8192-bit DH Group 18 cryptography

Fields (cont)	– Life Time—specifies the time an SA will live before expiring. Shorter lifetimes can make it harder to mount a successful key recovery attack, since the attacker has less data encrypted under the same key to work with. However, shorter lifetimes require more CPU processing time for establishing new SAs. Its units are secs / mins / hrs as shown below: • Seconds • Minutes • Hours – Life Time Value—enter life time value. – Anti-Reply—it shows if anti-reply IPsec protection is available. The options are: • ENABLE appears when any authentication is specified • DISABLE appears when None is selected for Authentication.
Buttons	• Apply—modifies attributes and saves the changes. • Delete—deleted the configuration.

VPN Status

Figure 10: VPN Status

VPN Status						
<i>ikeInitRekey</i>	<i>ikeRspRekey</i>	<i>ikeChildSaRekey</i>	<i>ikeInInvalid</i>	<i>ikeInInvalidSpi</i>	<i>ikeInInitReq</i>	<i>ikeInInitRsp</i>
ikeInitRekey_KEY	ikeRspRekey_KEY	ikeChildSaRekey_KEY	ikeInInvalid_KEY	ikeInInvalidSpi_KEY	ikeInInitReq_KEY	ikeInInitRsp_KEY
<i>ikeInAuthReq</i>	<i>ikeInAuthRsp</i>	<i>ikeOutAuthReq</i>	<i>ikeOutAuthRsp</i>	<i>ikeInCrChildReq</i>	<i>ikeInCrChildRsp</i>	
ikeInAuthReq_KEY	ikeInAuthRsp_KEY	ikeOutAuthReq_KEY	ikeOutAuthRsp_KEY	ikeInCrChildReq_KEY	ikeInCrChildRsp_KEY	
<i>ikeOutCrChildReq</i>	<i>ikeOutCrChildRsp</i>	<i>ikeInInfoReq</i>	<i>ikeInInfoRsp</i>	<i>ikeOutInfoReq</i>	<i>ikeOutInfoRsp</i>	
ikeOutCrChildReq_KEY	ikeOutCrChildRsp_KEY	ikeInInfoReq_KEY	ikeInInfoRsp_KEY	ikeOutInfoReq_KEY	ikeOutInfoRsp_KEY	
Screen Objective	This screen allows the user to configure the VPN Global Configuration.					
Navigation	Layer 3 Management > Security > VPN > VPN Status					

Fields	The displayed counters are: 1) ikeInitRekey 2) ikeRspRekey 3) ikeChildSaRekey 4) ikeInInvalid 5) ikeInInvalidSpi 6) ikeInInitReq 7) ikeInInitRsp 8) ikeOutInitReq 9) ikeOutInitRsp 10) ikeInAuthReq 11) ikeInAuthRsp 12) ikeOutAuthReq 13) ikeOutAuthRsp 14) keInCrChildReq 15) ikeInCrChildRsp 16) ikeOutCrChildReq 17) ikeOutCrChildRsp 18) ikeInInfoReq 19) ikeInInfoRsp 20) ikeOutInfoReq 21) ikeOutInfoRsp

26.3. Firewall

This section describes how the Firewall feature on the switch is configured.

An organization can define its fundamental security policy using one of the following firewall techniques:

- Block all packets that are not explicitly configured to allow into the protected network.
- Allow all packets that are not explicitly configured to block into the protected network.

This chapter outlines how to configure a firewall.

To access **Firewall** screens, go to **Layer 3 Management > Security > Firewall**.

Firewall Global Configuration

Figure 11: Firewall Global Configuration

Firewall Global Configuration

Firewall Status	Enabled ▾
Maximum Rules	5000 ▴ ▾
Maximum Access Groups	64 ▴ ▾
Apply	

Screen Objective	This screen allows the user to configure the Firewall Global Configuration.
Navigation	Layer 3 Management > Security > Firewall > Global Configuration
Fields	• Firewall Status—select the status of the firewall. The default option is disabled. The list contains: – Enabled – Disabled • Maximum Rules—select the maximum number of rules • Maximum Access Groups—select a number for maximum access groups.
Buttons	• Apply—select to save the configuration.

Firewall Rule Configuration

Figure 12: Firewall Rule Configuration

Firewall Rule Configuration

Rule Name	
Source Range	Any ▾
Source Address	/
Destination Range	Any ▾
Destination Address	/
Protocol	Any ▾ 255 ▴ ▾
Source Port	> ▾ 1 ▴ ▾
Destination Port	> ▾ 1 ▴ ▾
Action	Permit ▾
Priority	1 ▴ ▾
Add Reset	

Select	Rule Name	Source Address	Destination Address	Protocol	Protocol Number	Source Port	Destination Port	Action	Priority	Status
☐	ac1	80.0.0.0/8	0.0.0.0/0	Any ▾	255 ▴ ▾	>1 ▴ ▾	>1 ▴ ▾	Permit ▾	5000 ▴ ▾	Active ▾

Screen Objective	This screen allows the user to configure a firewall rule. A firewall rule is determined by parameters such as Source Range / Address, Destination Range / Address, Source & Destination Ports, Protocol and Priority.
Navigation	Layer 3 Management > Security > Firewall > Rule Configuration
Fields	• Select—click to select the entry or which Firewall Rules configuration needs to be modified or deleted. • Rule Name—enter a text string for a rule name. • Source Range—select a source range. The options are: – Any NOTE: If Any is selected, the field Source Address is dimmed. – Subnet NOTE: If Subnet is selected, the field Source Address is available for entry. • Source Address—enter the actual IP address / mask. • Destination Range—select a destination range. The options are: – Any NOTE: If Any is selected, the field Destination Address is dimmed. – Subnet NOTE: If Subnet is selected, the field Destination Address is available for entry.

Fields (cont)	• Destination Address—enter the destination IP address / mask. • Protocol—select a protocol from the drop-down list. The options are as follows: – Any—choose this option for any protocol. NOTE: When this option is selected, the field Source port number and Destination Port number are dimmed. – ICMP—choose this option for Internet Control Message Protocol (<i>ICMP</i>). NOTE: When this option is selected, the field Source port number and Destination Port number are dimmed. – IGMP—choose this option for Internet Group Management Protocol (<i>IGMP</i>). NOTE: When this option is selected, the Source port number and Destination Port number are dimmed. – GGP—choose this option for Gateway-to-Gateway Protocol (<i>GGP</i>). NOTE: When this option is selected, the Source port number and Destination Port number are dimmed. – IP—choose this option for IP. NOTE: When this option is selected, the Source port number and Destination Port number are dimmed. – TCP—choose Transmission Control Protocol (<i>TCP</i>) to deliver and receive an ordered and error-checked stream of information packets over the network NOTE: If <i>TCP</i> is selected, the field Source port number and Destination Port number are available. – EGP—choose this option for Exterior Gateway Protocol (<i>EGP</i>). NOTE: When this option is selected, the Source port number and Destination Port number are dimmed. – IGP—choose this option for Interior Gateway Protocol (<i>IGP</i>). NOTE: When this option is selected, the Source port number and Destination Port number are dimmed. – NVP—choose this option for Network Voice Protocol (<i>NVP</i>). NOTE: When this option is selected, the Source port number and Destination Port number are dimmed. – UDP—choose User Datagram Protocol (<i>UDP</i>) to deliver a faster stream of information without error-checking. NOTE: If <i>UDP</i> is selected, the field Source port number and Destination Port number are available. – IRTP—choose this option for Internet Reliable Transaction Protocol (<i>IRTP</i>). NOTE: When this option is selected, the Source port number and Destination Port number are dimmed. – IDPR—choose this option for Inter-domain Routing Protocol (<i>IDPR</i>). NOTE: When this option is selected, the Source port number and Destination Port number are dimmed.

Fields (cont)	• Protocol—(cont). The options are as follows: – RSVP—choose this option for Resource Reservation Protocol (<i>RSVP</i>). NOTE: When this option is selected, the Source port number and Destination Port number are dimmed. – MHRP—choose this option for Multipath Hybrid Routing Protocol (<i>MHRP</i>). NOTE: When this option is selected, the Source port number and Destination Port number are dimmed. – IGRP—choose this option for Interior Gateway Routing Protocol (<i>IGRP</i>). NOTE: When this option is selected, the Source port number and Destination Port number are dimmed. – OSPF—choose this option for Open Shortest Path First protocol (<i>OSPF</i>). NOTE: When this option is selected, the Source port number and Destination Port number are dimmed. – Other—choose this option for other protocols. NOTE: When you select Other, the field next to this field is also available for information to be added. NOTE: When this option is selected, the Source port number and Destination Port number are dimmed. • Source Port—enter the number of source port. • Destination Port—enter the number of the destination port. • Action— Every packet that attempts to enter or leave must be tested against each rule in the ACL until a match is found. If no match is found, then access will be denied. Select an action for the selected rule. – Deny – Permit • Priority—select a rule priority.
Buttons	• Add—adds and saves new configuration. • Reset—resets the configuration. • Delete—delete the selected entry.

Access Group Configuration

Figure 13: Access Group Configuration

Access Group Configuration

Interface
vlan55 ▾ *

Group Name
 *

Rule Name
ac1 ▴ ▾ *

Packet Direction
-Select- ▾ *

Add
Reset

Note: Press CTRL+Left-mouse click to select multiple Rule Names.

Select	Interface	ACL Name	Rule Name	Direction	Status
☐	vlan555	ag1	ac1	Inbound ▾	Active ▾
Delete					

Screen Objective	This screen allows the user to configure the access group.
Navigation	Layer 3 Management > Security > Firewall > Access Group Configuration
Fields	Select—select a configuration to be deleted. Interface—select an interface from the drop-down list. VLAN55 shown selected on the figure above. Group Name—enter a group name. Rule Name—select a rule name if the drop-down list is available for selection. NOTE: Use CTRL+left mouse click to select multiple rule names. Packet Direction—select packet direction. The options for selection are: – Inbound – Outbound Status—displays the status of the access group configuration.
Buttons	Add—adds and saves new configuration. Reset—resets the configuration. Delete—delete the selected entry.

Firewall Status

Figure 14: Firewall Status

Firewall Status							
Rule Name	Hit Count	Protocol	Source IP Address	Destination IP Address	Source Port	Destination Port	Access-Group Name
ac1	0	Any ▾	80.0.0.0/8	0.0.0.0/0	>1	>1	ag1

Screen Objective	This screen displays the firewall status. the only field which accepts user input is Protocol .
Navigation	Layer 3 Management > Security > Firewall > Status
Fields	• Rule Name—displays the rule name. • Hit Count—this is the number of times this flow was permitted or denied by this ACL entry in the configured time interval. The value becomes 1 when the security generates the first syslog message for this flow. • Protocol—choose a protocol from the drop-down list. The options are Any, ICMP, IGMP, GGP, IP, TCP, EGP, IGP, NVP, UDP, IRTP, RSVP, MHRP, IGRP, OSPF, and Other. The default option is Any. • Source IP Address—displays the source IP address of the packets. • Destination IP Address—displays the destination IP address of the packets. • Source Port—displays the source port number for the packets. • Destination Port—displays the destination port number for the packets. • Access Group Name—displays the access-group name.

26.4. Security IPv4 Interface Settings

This section describes the IPv4 interface security settings on the switch.

To access **Security IPv4 Interface Settings** screen, go to **Layer 3 Management > Security > IPv4 Address Config**.

Figure 15: Security IPv4 Interface Settings

Security IPv4 Interface Settings

Interface ID vlan55 ▾ *

IP Address *

Subnet Mask *

Proxy ARP Disabled ▾

Add
Reset

Select	Interface	IP Address	Subnet Mask	Proxy ARP
☐	Gi0/1	51.0.0.2	255.0.0.0	Disabled ▾
☐	vlan50	192.168.51.2	255.255.255.0	Enabled ▾
☐	vlan555	51.0.0.2	255.0.0.0	Disabled ▾

Delete

Screen Objective	This screen allows the user to configure the Security IPv4 Interface Settings.
Navigation	Layer 3 Management > Security > IPv4 Address Config
Fields	Interface ID—select an interface from the drop-down list. Ip Address—enter an IP address for the host. The format is A.B.C.D. Subnet Mask—enter an subnet mask for the host. The format is 4 bytes. As shown in the figure above, vlan50 has subnet mask 255.255.255.0 which is Class C network. vlan 555 has a subnet mask of 255.0.0.0 which corresponds to Class A network. Proxy ARP—IPv4 Proxy ARP allows a system to send responses to ARP requests on one interface on behalf of hosts connected to another interface. To prevent information unauthorized information sharing, Pv4 Proxy ARP must be disabled. Disabled is the default option for this field. The other option available from the drop-down list is Enabled.
Buttons	Add—adds and saves new configuration. Reset—resets the configuration. Delete—delete the selected entry.

26.5. Security IP Route Configuration

This section describes the Security IP Route Configuration on the switch.

To access **Security IP Route Configuration** screen, go to **Layer 3 Management > Security > IP Route Config**.

Figure 16: Security IP Route Configuration

Security IP Route Configuration

Destination Subnet *

Gateway *

Add

Reset

Select	Destination Subnet	Gateway
☐	51.0.0.0/8	
☐	51.0.0.0/8	
☐	51.0.0.0/8	
☐	51.0.0.0/8	
☐	51.0.0.0/8	
☐	51.0.0.0/8	
☐	51.0.0.0/8	
☐	51.0.0.0/8	

Delete

Screen Objective	This screen allows the user to configure the Security IP Route Configuration.
Navigation	Layer 3 Management > Security > IP Route Config
Fields	Select—select a configuration to be deleted or modified. Destination Subnet—enter destination subnet value. The format is A.B.C.D/M.
Buttons	Add—adds and saves new configuration. Reset—resets the configuration. Delete—delete the selected entry.

Index

Numerics

802.1x

- Basic Settings 116
- MAC Session Statistics 555
- Port Settings 121
- Session Statistics 553
- Supplicant Statistics Information 555
- Timer Configuration 126

A

- ACK Packets 587
- Agent 163
- Agent Control Settings 162
- Audit Log 52
- Authentication 128

B

BGP

- Basic Settings 417
- Clear BGP 458
- Community Filter Confederation 467
- Community Routes 470
- Confederation Settings 464
- Creation 416
- Extended Community Filter Configuration 471
- Extended Community Set Status Table 473
- Filter Preference Configuration 437
- Filters 463
- GR Settings 444
- Local Preference Configuration 434
- MED Configuration 431
- Neighbor Configuration 424

- Neighbor Configuration 452
- Orf Filters Config 462
- Peer Addition 456
- Peer Group Configuration 448
- Peer Orf Config 461
- Route Aggregation Configuration 440
- Route Map Settings 460
- Routes Community Set Status Table 469
- Routes Extended Community Table 474
- Settings 422
- TCP-AO MKT Configuration 446
- Timer Configuration 442

C

- Clock
 - Interworking Settings 143
- Community Settings 164

D

- DHCP 344, 352, 355, 358
 - Basic Settings 344
 - Bootfile Configuration 351
 - Client Identifier 358
 - Host IP Settings 349
 - Host Options Settings 350
 - Option Type 355
 - Pool Option Settings 347
 - Pool Settings 345
 - Relay Configuration 352
 - Relay Interface 353
 - Server IP Exclude Settings 348
- Document Conventions 5

Dynamic VLAN	Interface 488
GARP Clear Statistics 240	Static 491
GARP Timers Configuration 238	Timer 483
Global Configuration 234	VLAN 485
Introduction 234	VLAN Router Port 489
Port Configuration 236	MAC Based Multicast Forwarding Table 492
E	Multicast Receiver Table 492
Ethernet	V1/V2 Statistics 558
Statistics 529	V3 Statistics 559
F	VLAN Router Ports 491
Firewall	IKE Phase 1 584
Access Group Configuration 598	Diffie and Hellman Key Exchange 585
Global Configuration 594	Encryption Algorithms 584
Rule Configuration 595	Exchange Mode 585
Status 600	Generation of ZZ 585
G	IKE Phase 1 Configuration 584
GARP	IKE Phase 2 586
Configuration 231	Interface
Introduction 231	Clear 528
Traces 232	Statistics 528
H	IP
How IPSec Works 583	ARP Cache 559
HTTP 160	ICMP Statistics 560
Settings 160	IPv4 Interface Specific Statistics 561
I	IPv4 System Specific Statistics 561
IGMP	IPSec Policy Configuration 584
Configuration 494	IPv4 Multicasting
Group 497	Basic Settings 516
Group List 498	Interface Settings 517
Interface 495	Next Hop Statistics 567
Membership 498	Route Statistics 566
Proxy 566	L
Configuration 499	Link Aggregation
MRoute Configuration 501	Neighbour Statistics Information 548
Next Hop Configuration 502	Port Statistics 547
Statistics 565	LLDP
Upstream Interface Configuration 500	Error Information 553
IGMP Snooping	Statistics Information 552
Clear Statistics 558	Traffic Information 550
Configuration	Local 128
Basic Settings 478	M
	MAC 132
	Session 132
	MRP

-
- Configuration 281
 - Statistics 547
 - Status 283
 - MSTP
 - Bridge Priority 270
 - CIST Port Statistics 540
 - CIST Port Status 268
 - Global Information 255
 - Information 540
 - MSTI Port Statistics 541
 - Port Configuration - CIST Settings 262
 - Port Settings 267
 - Timers 261
 - Traces 259
 - VLAN Mapping 266
 - N**
 - NAT
 - Active Connections 582
 - All Configurations 581
 - Destination Configuration 580
 - Dynamic SNAT Configuration 577
 - Global Configuration 576
 - NAPT Configuration 578
 - O**
 - OSPF
 - Area Aggregation 395
 - Area Configuration 386
 - AS External Area Aggregation 396
 - Basic Settings 383
 - Debug Trace Settings 381
 - Graceful Restart Settings 398
 - Interface Configuration 388
 - Link State Database 563
 - Redundancy Information 564
 - Route Information 563
 - RRD Route Configuration 394
 - Virtual Interface Configuration 391
 - Virtual Neighbor Configuration 393
 - VRF Creation 380
 - P**
 - PIM
 - Basic Settings 503
 - Candidate RP Configuration 507
 - Component Configuration 505
 - DF Information 515
 - DM Global Configuration 511
 - Elected RP Information 515
 - Global Configuration 510
 - High Availability 514
 - Interface Configuration 506
 - Route Configuration 512
 - Static RP Configuration 509
 - PNAC
 - Traces 119
 - PoE
 - Global Configuration 572
 - Port Settings 573
 - PTP
 - Clock Settings 140
 - Global Configurations 139
 - Interfaces 142
 - Introduction 138
 - PTP Port Statistics 568
 - PVRST
 - Basic Information 544
 - Global Configuration 271
 - Instance Bridge Configuration 276
 - Instance Information 545
 - Instance Port Configuration 277
 - Instance Port Statistics 546
 - Instance Port Status 278
 - Port Configuration 273
 - Port Statistics 545
 - Q**
 - QoS
 - CoS Statistics 557
 - Policer Statistics 556
 - QoS Egress
 - Max Rate 108
 - Min Rate 106
 - Queue 114
 - Queue Map Settings 110
 - Queue Table Settings 105
 - Queue Template Settings 95
 - Red Conf Settings 99
 - Scheduler 112
 - Scheduler Table Settings 103
 - QoS Ingress
-

-
- Action 83
 - Basic Settings 71
 - Class Map Settings 87
 - Class to Priority Settings 89
 - Classifier 75
 - Classifier Element 76
 - Data Path 72
 - Def UserPri Settings 94
 - Meter 78
 - Policy Map Settings 90
 - Priority Map Settings 85
 - Token Bucket Meter 80
- R**
- RADIUS 129, 131
 - Radius Server Statistics 556
 - Server 129
 - Configuration 129
 - Global Configuration 129
 - Traces 131
 - Redistribution BGP Configuration 401
 - RIP
 - Basic Settings 360
 - Interface 363
 - Interface Specific Address Summarization 368
 - Interface Statistics 562
 - Neighbour List 365
 - Security Settings 366
 - VRF Creation 359
 - RMON
 - Ethernet Statistics 567
 - Route Map
 - Creation 369
 - IP Prefix List 378
 - Match 371
 - Set 375
 - Route Redistribution
 - OSPF Configuration 405
 - RIP Configuration 403
 - RSTP
 - Configuration 247
 - Global Information 242, 280
 - Information 542
 - Port Statistics 542
 - Port Status 253
 - Status Configuration 248
 - Traces 245
- S**
- Serial
 - Serial Port Statistics 570
 - Serial Communication
 - Comparison of Serial Communication Standards 311
 - RS-232
 - 3-wire Mode 312
 - 5-wire Mode 313
 - Simple Null Modem Cable Route 312
 - RS-422 313
 - Direct Connect Mode 314
 - Multi Listener Mode 314
 - RS-485 315, 316
 - 2-Wire Half-duplex Mode 316
 - 4-Wire Full-duplex Mode 315
 - SNAT
 - SNAT Configuration 576
 - SNMP 162, 164, 166, 167, 169, 170, 171, 173, 174, 176, 177, 179, 181
 - Agent 569
 - Filter Profile 173
 - Filter Settings 177
 - Group Access 167
 - Group Settings 166
 - Proxy Settings 179
 - Security Settings 174
 - Settings 181
 - Target Address 170
 - Target Parameter 171
 - Trap Manager 176
 - View Tree 169
 - SNTF
 - Broadcast Configuration 150
 - Manycast Configuration 152
 - Multicast Configuration 151
 - Settings 145
 - Unicast Table 148
 - SSH 154
 - Global Settings 154
 - SSL 156, 158
 - Digital Certificate 158
 - Global Settings 156
 - System
-

- ACL Introduction 54
- Clear Counters 25
- File Transfer
 - Diagnostic File Transfer 52
 - File Download 51
 - File Upload 49
- IP Authorized Manager 65
- IP Extended ACL Configuration 61
- IP Standard ACL Configuration 58
- Line Cards Information 22
- MAC ACL Configuration 54
- Port Isolation 68
- Power Supply Information 24
- Protecting Against CPU Overloading Settings 38
- Reboot 47
- Save and Restore 42
 - Factory Reset 46
 - Restore Configuration 45
 - Save Configuration 43
- SFP Information 23
- Syslog Transfer 47
- System Alarms 26
- System Alarms History 27
- System Alarms Supported 29
- System Information 16
- System Logging Information 40
- System Resources 29
- System Settings 18
- System Upgrade 41
- User Manager 37

T

- TAC Profile Configuration 518
- TACACS 134, 136, 137
 - Server 137
 - Active Server Configuration 137
 - Configuration 134
- Traces 136

TCP

- Connections 532
- Listeners 531
- Statistics 531

U

- UDP

- Connections 533
- Statistics 533

V

VLAN

- Basic Settings 213
- Capabilities 538
- Counter Statistics 537
- Current DB 535
- FDB Entries 538
- FDB Flush 230
- Introduction 212
- Multicast Table 537
- Port Mac Map 229
- Port Settings 219
- Port VLAN Protocol Settings 228
- Protocol Group Settings 225
- Static VLAN Configuration 223

VPN

- Global Configuration 583
- Policy Configuration 587
- Status 593

VRRP

- Associated IP Table 414
- Global Settings 407
- IF Track Settings 408
- IP Track Settings 410
- Virtual Router Settings 411

- VRRPv3 Statistics 564

W

Web Interface

- Browser Settings 3
- Conventions 1
- System Acknowledgment 8

- Web Session 161