iBiome - BGP User Guide

RAPTOR™

Intelligent Cyber Secure Platform

Version: 1.12.04-1-EN, Date: Apr 2022

iS5 COMMUNICATIONS
SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

Copyright Notice

Trademarks

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

Regulatory Compliance Statement

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

Warranty

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

Disclaimer

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

Contact Information

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

End User License Agreement (EULA)

TERMS AND CONDITIONS FOR SOFTWARE PROGRAMS AND EMBEDDED SOFTWARE IN PRODUCTS

1) **EULA**

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

2) **INTELLECTUAL PROPERTY**

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

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

3) **EXPORT CONTROLS AND SANCTIONS**

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

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

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

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

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

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

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

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

Exhibit A: End User License Agreement

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

1) **DEFINITIONS**

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

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

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

2) **LICENSE**

- **2.1 License Grant**

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

- **2.2 License Restrictions**

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

– **2.3 Updates and Upgrades**

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

– **2.4 Versions**

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

– **2.5 Third Party Software**

Customer shall comply with any Third Party License Terms.

3) **OWNERSHIP**

– **3.1 Intellectual Property**

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

– **3.2 Firmware**

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

– **3.3 Third Party Software**

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

4) **CONFIDENTIALITY**

– **4.1 Confidentiality**

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

– **4.2 Irreparable Harm**

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

– **4.3 Security**

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

5) **LIMITATION OF LIABILITY**

– **5.1 Disclaimer**

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

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

– **5.2 Limitation of Liability**

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

6) **TERM**

– **6.1 Term**

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

– **6.2 Survival**

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

7) **MISCELLANEOUS**

– **7.1 Miscellaneous**

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

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

– **7.2 Subject to Change**

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

GLOSSARY ENTRIES

802.1D

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

802.1Q

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

802.1X

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

802.1W

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

AAA

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

AARP

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

ABR

Area Border Router (ABR)

ACK

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

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

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

ACL

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

AES

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

AO

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

ARAP

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

ARP

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

AS

Autonomous System (AS)

ASBR

Autonomous Border System Router (ASBR)

Asdot

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

- 5
- 25
- 196
- 65000
- 65535

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

- 0.65536
- 15.418
- 65535.8520
- 65535.65535

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

ASN

Autonomous System Number (ASN)

BDR

BDR stands for Backup Designated Router.

BFD

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

BGP

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

BGP

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

BIDIR-PIM

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

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

BMS

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

BOOTP

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

BPDU

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

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

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

BPS

BPS (Bits-per-second)

BR

Border Router (BR)

BSD

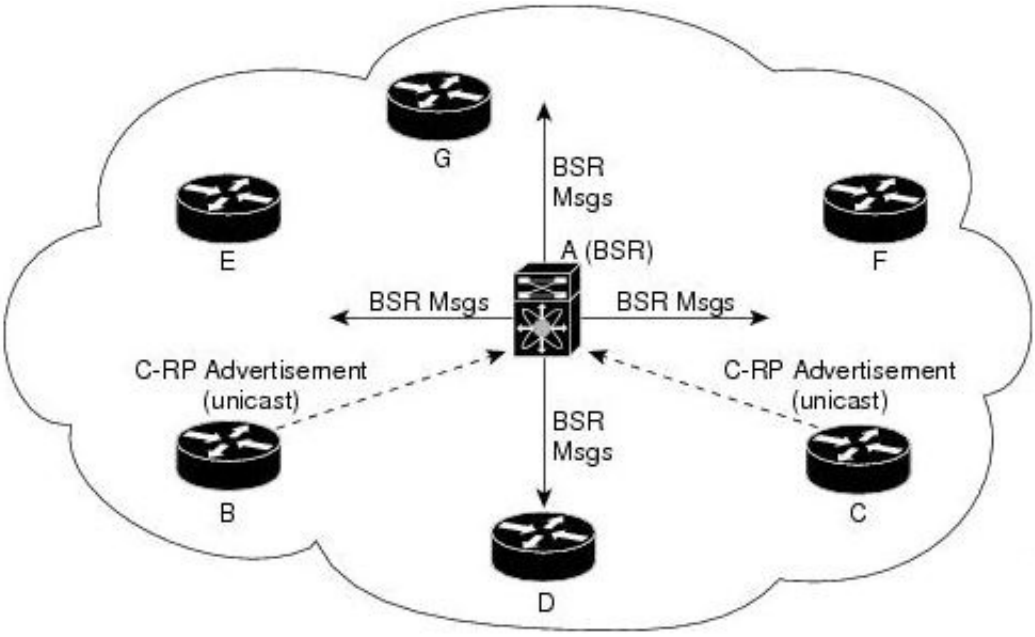
Berkeley Software Distribution (BSD)

BSR

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

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

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



CA

Certificate Authorization (CA)

CBP

Customer Backbone Port (CBP)

CBS

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

CEP

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

CFI

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

MS-CHAP

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

CIDR

Classless Inter Domain Routing (CIDR).

CIR

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

CIST

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

CLI

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

CLKIWF

CLKIWF is short for Clock InterWorking Function.

CoS

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

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

CPLD

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

CPU

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

CRT

CRT stands for "Internet security certificate.

CSR

Certificate Signing Request (CSR)

CST

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

CTS

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

CVID

The C-VID registration table is as follows:

Table 1: C-VID registration table

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

CVLAN

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

DB9

DB9 refers to a common connector type from the D-Subminiatures (D-Sub) connector family, which when introduced, was among the smallest connectors used on computer systems. DB9 houses 9 pins (for the male connector) or 9 holes (for the female connector). DB9 connectors were once very common on PCs and servers. Today, the DB9 has mostly been replaced by more modern interfaces such as USB, PS/2, Firewire, and others.

DB25

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

DCD

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

DEC

Digital Equipment Corporation (DEC)

DEI

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

DES

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

DF

Designated Forwarder (DF).

DHCP

Dynamic Host Configuration Protocol (DHCP)

DITA

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

D-LAG

Distributed Link Aggregation (D-LAG or DLAG)

DLF

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

DM

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

DNAT

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

DNS

Domain Name System

DOT1Q

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

Dot1x

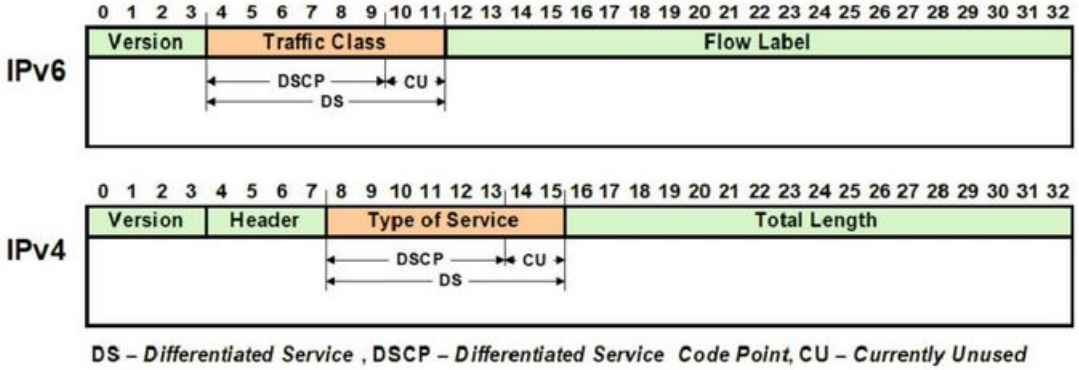
Dot1x Authentication is enabled when dot1x system-auth-control is enabled, and aaa authentication dot1x default is local. If you enable authentication on a port by using the default setting of dot1x port-control, which is force-authorized, it disables 802.1X authentication and causes the port to transition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

DR

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

DS

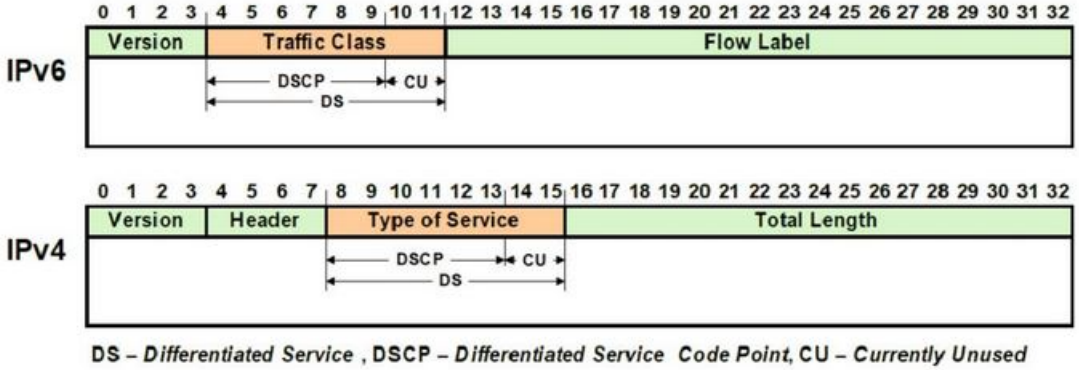
Differentiated Services (DS).



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

DSCP

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



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

DSR

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

DST

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

DTR

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

DUT

Device under Test (DUT)

DVMRP

Distance Vector Multicast Routing Protocol (DVMRP)

E2E

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

EAP

Extensible Authentication Protocol (EAP) is an authentication framework frequently used in network and Internet connections. EAP is usually tunnelled over RADIUS between the Authenticator and the Authentication Server. 802.1x uses EAP.
EAP is an authentication framework, not a specific authentication mechanism. Commonly used modern methods capable of operating in wireless networks include EAP-TLS, EAP-SIM, EAP-AKA, LEAP and EAP-TTLS. Requirements for EAP methods used in wireless LAN authentication are described in RFC 4017.
The Lightweight Extensible Authentication Protocol (LEAP) method was developed by Cisco Systems prior to the IEEE ratification of the 802.11i security standard.

EAPOL

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

EBGP

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

EBS

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

ECN

Explicit Congestion Notification (ECN)

EGP

Exterior Gateway Protocol (EGP) is a defunct routing protocol used in autonomous systems to exchange data between surrounding gateway sites. Border Gateway Protocol (BGP) supplanted EGP, widely utilized by research institutes, universities, government agencies, and commercial companies (BGP). EGP is built on poll instructions to request update answers and periodic message exchange polling for neighbor reachability.

EIR

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

ESD

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

EXEC

exec: Protocol
Commands that are invoked using the exec: protocol must be executable as standalone commands. Commands that are built into a command interpreter or other program cannot be executed directly, but must be executed (if possible) within the context of the application that provides them.

For example, the following seed URL would not work on Microsoft Windows systems because the dir command is built into the Windows command interpreter (cmd.exe):
exec: dir e:\data
To use the exec protocol with commands that are built into the Windows command interpreter, you must do something as the following:
exec: cmd /c dir 'e:\data'

EVB

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

EVC

Ethernet Virtual Connection (EVC).

FCS

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

FDB

Forwarding Database (FDB)

FID

Filtering ID (FID)

FHRP

First Hop Redundancy Protocol (FHRP)

FPGA

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

FTP

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

GARP

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

GGP

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

GMRP

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

GND

Ground

GPS

Global Positioning System

GR

Graceful Restart (GR)

GRE

Generic routing encapsulation (GRE) is an IP encapsulation protocol which is used to transport IP packets over a network. In GRE, an IP datagram is tunnelled (encapsulated) within another IP datagram.One great advantage of GRE is that it allows routing of IP packets between private IPv4 networks which are separated over public IPv4 Internet. GRE also supports encapsulating IPv4 broadcast and multicast traffic.

GVRP

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

HA

High Availability (HA)

HDMI

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

HOL

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

HSR

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

HTTP

Hyper Text Transfer Protocol (HTTP)

HTTPS

Hyper Text Transfer Protocol Secure (HTTPS)

IANA

Internet Assigned Numbers Authority (IANA)

IBGP

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

ICMP

Internet Control Message Protocol

IDPR

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

IETF

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

IGMP

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

IGP

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

IGRP

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

IGS

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

IKE

Internet Key Exchange (IKE)

IP

Internet Protocol (IP).

IPSec

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

IPv4

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

- IPv4 has a 32-bit address length
- IPv4 binary bits are separated by a dot(.) whereas IPv6 binary bits are separated by a colon(:).
- IPv4 is a numeric addressing method whereas IPv6 is an alphanumeric addressing method
- It Supports Manual and DHCP address configuration
- In IPv4 end to end, connection integrity is Unachievable
- It can generate 4.29×109 address space
- Fragmentation performed by Sender and forwarding routers
- In IPv4 Packet flow identification is not available
- In IPv4 checksum field is available
- It has broadcast Message Transmission Scheme
- In IPv4 Encryption and Authentication facility not provided
- IPv4 has a header of 20-60 bytes.

IPv6

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

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

IRTP

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

ISAKMP

Internet Security Association and Key Management Protocol (ISAKMP)

ISDN

Integrated Services Digital Network (ISDN)

ISL

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

ISP

Internet service provider (ISP)

ISS

Intelligent Switch Solution (ISS).

IST

The Internal Spanning Tree (IST) instance receives and sends BPDUs to the CST. The IST can 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

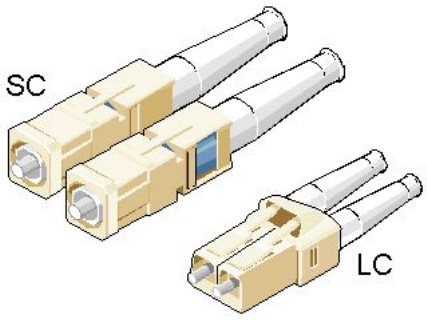
Link Aggregation Group

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, adevice examines MLD messages between hosts and multicast routers and learns which hosts are interested in receiving traffic for a multicast group. On the basis of what it learns, the device then forwards multicast traffic only to those interfaces in the VLAN that are connected to interested receivers instead of flooding the traffic to all interfaces.

MKT

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

MM

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

MIC

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

MPLS

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

MRA

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

MRC

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

MRM

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

MRP

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

MSR

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

MST

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

MSTI

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

MSTP

Multiple Spanning-Tree Protocol

MTU

Maximum Transmission Unit (MTU)

MVLAN

Multicast VLANs (MVLAN)

NAP

Network Access Protection (NAP)

NAPT

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

NAS

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

NAT

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

NBMA

NBMA (Non Broadcast Multi Access)

NBNS

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

NC

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

ND

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

NETBIOS

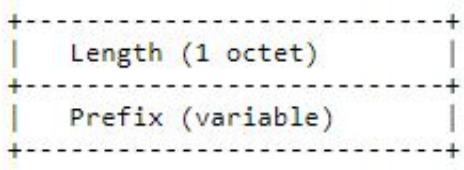
Network Basic Input / Output System (NETBIOS)

NIP

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

NLRI

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



NMS

Network Management System (NMS)

NO

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

NPS

Network Policy Server (NPS)

NSSA

Not-so-stubby Area (NSSA)

NTP

Network Time Protocol (NTP)

NVP

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

NVRAM

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

OID

Object IDentifier

ORF

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

OSPF

Open Shortest Path First routing protocol

OUI

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

P2P

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

PAE

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

PAP

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

PC

Personal Computer

PCB

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

PDU

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

P/E

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

PEB

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

PEM

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

PEP

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

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.

PPVID

Port and Protocol *VLAN* ID (PPVID)

PRP

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

PS

Power Supply

PTP

Precision Timing Protocol

PVID

Port *VLAN* ID (PVID)

PVLAN

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

PVRST

Per VLAN Rapid Spanning-Tree

PVRSTP

Per VLAN Rapid Spanning-Tree Protocol

PW

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

Q-in-Q

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

QoS

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

QRV

Querier’s Robustness Variable (QRV).

RADIUS

Remote Authentication Dial-In User Service

RAM

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

RARP

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

RBAC

Role Based Authentication (RBAC)

RED

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

RFD

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

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

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

RFL

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

RIB

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

RIP

RIP (Routing Information Protocol) sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers about the

change. These updates are sent independently of the regularly scheduled updates that RIP routers send. RIP uses a hop count as a way to determine network distance. Each host with a router in the network uses the routing table information to determine the next host to route a packet for a specified destination.

RMON

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

RP

Rendezvous point (RP)

RPF

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

RPT

Root Part Tree (RPT)

RRD

Route Redistribution (RRD)

RSVP

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

RS-232

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

RS-422

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

RS-485

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

RST

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

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

RSTP

Rapid Spanning-Tree Protocol

RT

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

RTM

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

RTS

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

RX

Receive

SA

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

SAN

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

SEM

State Event Machines (SEM)

SFP

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

SFTP

SSH File Transfer Protocol (SFTP)

SHA

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

SIP

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

SISP

Switch Instance Shared Port (SISP)

SLA

Service-level agreements (SLA).

SLIP

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

SM

State Machine

SNAT

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

SNMP

Simple Network Management Protocol

SNTP

Simple Network Time Protocol (SNTP)

SPT

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

SR

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

SRM

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

SSD

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

SSH

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

SSL

Secure Sockets Layer

SSM

Source-Specific Multicast (SSM)

SST

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

- A switch running STP or RSTP belongs to only one spanning tree.
- An MST region has only one switch.

STP

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

SVL

Shared VLAN Learning (SVL)

S-VLAN

Stacked VLAN (S-VLAN)

TAC

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

TACACS

Terminal Access Controller Access-Control System

TAI

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

TB

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

TC

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

TCN

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

TCP

Transmission Control Protocol

TCP-AO

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

TCP-AO MKT

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

TLS

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

TLV

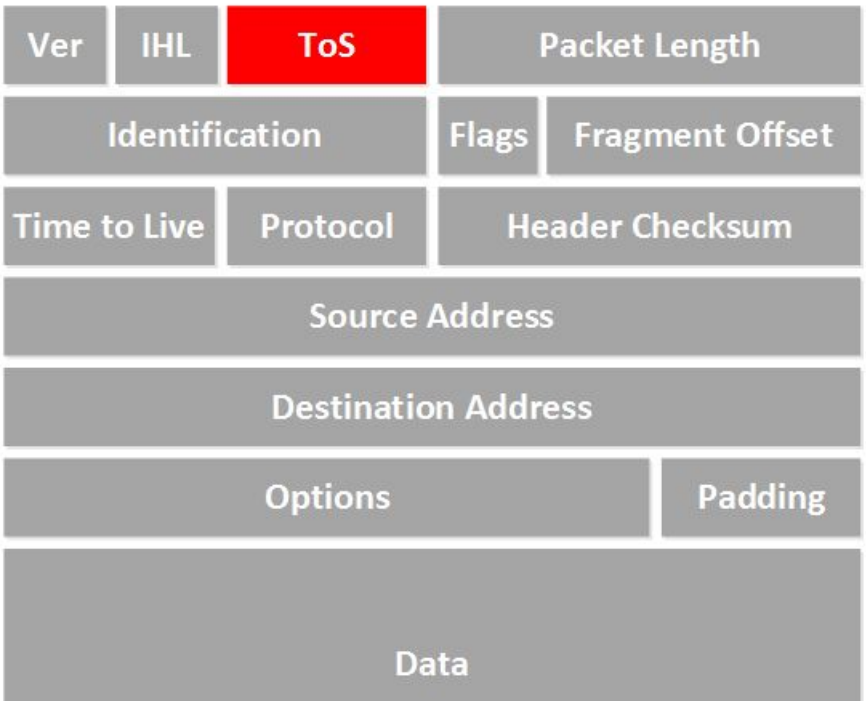
type, length, and value (TLV) traces

TN

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

TOS

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



TPID

Tag Protocol Identifier (TPID)

TTL

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

TX

Transmit

UAP

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

UART

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

UDP

User Datagram Protocol

UFD

Uplink failure detection (UFD)

URM

Unified Route Map (URM)

USM

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

UTC

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

UTP

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

UUID

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

VACM

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

Varbind

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

VFI

Virtual Forwarding Interface (VFI)

VID

Management VLAN ID (VID)

VINES

Virtual Integrated Network Service (VINES)

VLAN

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

VPN

Virtual Private Network (*VPN*)

VRF

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

VRRP

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

VSA

Vendor Specific Attribute (VSA)

WAN

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

Web UI

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

WRED

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

WRR

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

XNS

Xerox Network Systems (XNS)

Contents

INTRODUCTION

1. Introduction

The Border Gateway Protocol version 4 (*BGP4*) implements the Border Gateway Protocol version 4 described in RFC 4271. BGP4 is an inter-Autonomous System routing protocol. The primary function of a BGP speaking system is to exchange network reachability information with other *BGP* systems. This network reachability information includes information on the list of Autonomous Systems (*AS*) that reachability information reverses. This information is sufficient for constructing a graph of *AS* connectivity for this reachability from which routing loops may be pruned, and, at the *AS* level, some policy decisions may be enforced.

BGP4 provides a set of mechanisms for supporting Classless Inter-Domain Routing (*CIDR*). These mechanisms included support for advertising a set of destinations as an IP prefix, and eliminating the concept of network “class” within *BGP*. *BGP4* also introduces mechanisms that allow aggregation of routes, including aggregation of *AS* paths.

Routing information exchanged via *BGP* supports only the destination based forwarding paradigm, which assumes that a router forwards a packet based solely on the destination address carried in the IP Header of the packet. This, in turn, reflects the set of policy decisions that can (and cannot) be enforced using *BGP*. *BGP* can support only those policies conforming to the destination-based forwarding paradigm.

BGP uses TCP [RFC793] as its transport protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgment, and sequencing.

BGP listens on *TCP* port 179. The error notification mechanism used in *BGP* assumes that *TCP* supports a "graceful" close (i.e., that all outstanding data will be delivered before the connection is closed).

1.1. Purpose and Scope

This document describes the different application program interfaces (APIs) supported by *BGP* protocol.

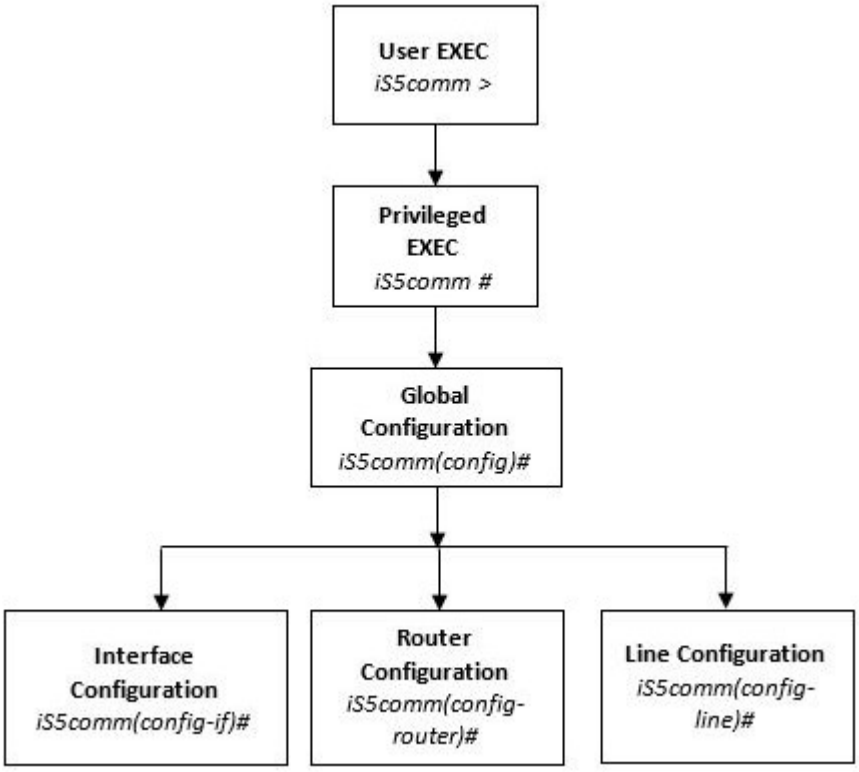
To add *BGP* functionality, some understanding of the concept and its possible configurations is needed as a prerequisite.

1.2. CLI Command Modes

The *CLI* Modes are as follows.

The hierarchical structure of the command modes is as shown on the figure below.

Figure 1: CLI Command Modes



User Exec Mode

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

Privileged Exec Mode

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

Global Configuration Mode

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

Interface Configuration Mode

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

Port Channel Interface Configuration

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

VLAN Interface Configuration Mode

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

MRP Interface Configuration Mode

Prompt	Access method	Exit Method
`iS5comm(config-mrp)#`	The Global Configuration mode command `mrp ringid 1`s used to enter the MRP Interface Configuration Mode.	To return from the MRP Interface Configuration mode to Global Configuration Mode, the command `exit` is used. To exit from the MRP Interface Configuration mode to Privileged EXEC Mode, the command `end` is used.

UFD Configuration Mode

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

DHCP Pool Configuration Mode

Prompt	Access method	Exit Method
`iS5comm(dhcp-config)#`	The Global Configuration mode command **`(config)# ip dhcp pool`***`<pool number (1-2147483647)>`* is used to enter the UFD Interface Configuration Mode.	To return from the DHCP Pool Configuration Mode to Global Configuration Mode, the command `exit` is used. To exit from the DHCP Pool Configuration Mode to Privileged EXEC Mode, the command `end` is used.

Privilege Levels and Command Access

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

Command	First Param	Guest	Tech	Admin	Description
archive	download-sw		x	x	Downloads software image
clear					Clears the specified parameters
	alarm	x	x	x	Alarm related information
	au-message	x	x	x	Address update messages related information
	cfa	x	x	x	CFA module related information
	interfaces	x	x	x	Protocol specific configuration of the interface
	meter-stats	x	x	x	Specific configuration for meter
	poe	x	x	x	PoE related configuration

Command	First Param	Guest	Tech	Admin	Description
	screen	x	x	x	Screen information
	ip		x	x	IP related configuration
	line		x	x	Configures line information
	logs		x	x	Log information
	protocol		x	x	Clears the specified protocol counters
	spanning-tree		x	x	Spanning tree related configuration
	tcp		x	x	TCP related configuration
clock	set		x	x	Sets the system clock value
config-restore					Configures the restore option
	flash		x	x	File in flash to be used for restoration
	norestore		x	x	No configuration restore
	remote		x	x	Remote location configuration
configure	terminal		x	x	Configures the terminal
copy			x	x	Various copy options
debug					Configures trace for the protocol
	ip	x	x	x	IP related configuration
	show	x	x	x	Show mempool status
	sntp	x	x	x	SNTP related configuration
	crypto		x	x	Crypto related information
	cybsec		x	x	Cybsec related information
	dot1x		x	x	PNAC related configuration
	etherchannel		x	x	Etherchannel related information
	firewall		x	x	Firewall related configuration
	garp		x	x	GARP related configuration
	interface		x	x	Configures trace for the interface management
	lacp		x	x	LACP related configuration
	lldp		x	x	LLDP related configuration

Command	First Param	Guest	Tech	Admin	Description
	lns		x	x	LCD notification server
	nat		x	x	Network Address Translation related configuration
	np		x	x	NPAPI configuration
	ptp		x	x	Precision time protocol related configuration
	qos		x	x	QOS related configuration
	security		x	x	Security related configuration
	spanning-tree		x	x	Spanning tree related protocol configuration
	ssh		x	x	SSH related configuration
	tacm		x	x	Transmission and admission control related configuration
	vlan		x	x	VLAN related configuration
display firewall rules				x	Display firewall rules
dot1x	clear	x	x	x	Clear dot1x configuration
	initialize		x	x	State machine and fresh authentication configuration
	re-authenticate		x	x	Re-authentication
dump					Display memory content from the given memory location
	mem		x	x	Dump memory
	que		x	x	Show the queue related information
	sem		x	x	Show the semaphore related information
	task		x	x	Show the task related information
egress bridge			x	x	
end			x	x	Exit to the privileged Exec (#) mode

Command	First Param	Guest	Tech	Admin	Description
erase			x	x	Clears the contents of the startup configuration
exit		x	x	x	Logout
factory reset				x	Reset to factory default configuration
factory reset	users			x	Reset all users on switch
firmware			x	x	Upgrades firmware
generate	tech		x	x	Generate the tech report of various system resources and protocol states for debugging
help		x	x	x	Displays help for commands
ip	igmp snooping clear counters	x	x	x	Clears the IGMP snooping statistics
	clear counters		x	x	Clear operation
	dhcp		x	x	DHCP related configuration
	pim		x	x	PIM related configuration
	ssh		x	x	SSH related information
listuser			x	x	List the user, mode and groups
lock			x	x	Lock the console
logout		x	x	x	Logout
memtrace			x	x	Configures memtrace
no ip					IP related information
	dhcp		x	x	DHCP related configuration
	ssh		x	x	SSH related information
no debug					Configures trace for the module
	ip	x	x	x	Stops debugging on IGMP or PIM
	sntp	x	x	x	Stops debugging on SNTP related configurations
	additional options...		x	x	Stops debugging for other options
ping					

Command	First Param	Guest	Tech	Admin	Description
	A.B.C.D	x	x	x	Ping host
	ip dns host name	x	x	x	Ping host
	ip A.B.C.D	x	x	x	Ping host
	vrf	x	x	x	Ping vrf instance
readarpfromHardware ip	A.B.C.D		x	x	Reads the arp for the given IP
readregister			x	x	Reads the value of the register from the hardware
release dhcp			x	x	Performs release operation
reload			x	x	Restarts the switch
renew dhcp			x	x	Performs renew operation
run script			x	x	Runs CLI commands
shell				x	Shell to Linux prompt
show		x	x	x	Shows configuration or information
sleep		x	x	x	Puts the command prompt to sleep
ssl				x	Configures secure sockets layer related parameters
snmpwalk mib					Allows the user to view Management Information Base related configuration.
	name	x	x	x	
	oid	x	x	x	
traceroute					Traces route to the destination IP
	A.B.C.D		x	x	
write			x	x	Writes the running-config to a flash file
writeregister			x	x	writes in the specified register

Configuration Terminal Access

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

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

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

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

1.3. CLI Document Convention

To provide a consistent user experience, this *CLI* document convention adhere to the Industry Standard *CLI* syntax.

In addition, the font and format are updated to show *DITA* / Structured Framemaker 2019 layout.

Convention	Usage	DESCRIPTION
Italics	User inputs for *CLI* command	`configure terminal`
Font as shown	Syntax of the *CLI* command	`configure terminal`
< >	Parameter inside the brackets < > indicate the Input fields of syntax	`<integer (100-1000)>`
[ ]	Parameter inside [ ] indicate optional fields of syntax	`show split-horizon [all]`
{ }	Grouping parameters in the syntax	`ip address <ip-address> [secondary {node0 | node1}]`
|	Separating grouped parameters in the syntax	`set http authentication-scheme {default| basic| digest}`

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

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

1.4. Default Configurations

CONTEXT:

The table below lists the default values assigned to several *BGP* parameters during start-up of the router.

Parameter	Default Setting
BGP IPv4 global status	Disabled
BGP IPv6 global status	Disabled
BGP Max Peers	50
BGP Max Routes	5000
BGP Listener Port	179
BGP Originator ID	0.0.0.0 (Disabled)
BGP Max Q_MSGS	500
BGP Hold Interval	90 Seconds
BGP Initial Hold Time	240 Seconds
BGP Keepalive Timeout	30 Seconds (BGP Hold Interval/ 3)
BGP Connect-retry Timer	30 Seconds
BGP MinAs Origin Interval	15 Seconds
BGP DelayOpen Interval	0 Seconds
BGP Connect Retry Count	5
BGP Peer Prefix Limit	100
BGP Redistribution	Disabled
BGP Peer-filter	Accept-all
Debug level	None (0)

Preliminary Configurations

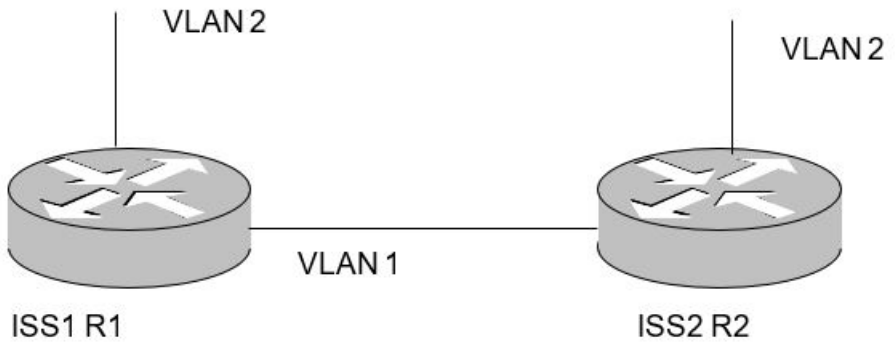
This section describes the preliminary configurations and the configurations for the topologies of Is5Com BGP. Configuration of Is5Com BGP features is done by accessing the Global Configuration or Interface Configuration modes. The configuration steps described in this document begin with accessing one or both modes. Refer to Global Configuration Mode or Interface Configuration Mode for the access and exit method of these modes through CLI. The following points are part of the preliminary configurations

Configuring ISS1 in Topology for Testing BGP

CONTEXT:

The figure shown below depicts the topology setup used for this configuration as follows.

Figure 2: BGP Configuration and Testing Topology



1. To configure ISS2 in Topology for testing BGP:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

2. To enable BGP in Router R2:

   FOR EXAMPLE: Execute the following commands:

```
iS5comm# configure terminal
iS5comm(config)# interface vlan 1
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 12.0.0.1 255.0.0.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# end

iS5comm# configure terminal
iS5comm(config)# interface gigabitethernet 0/1
iS5comm(config-if)# no shutdown
iS5comm(config-if)# end

iS5comm# configure terminal
iS5comm(config)# interface gigabitethernet 0/1
iS5comm(config-if)# switchport pvid 1
iS5comm(config-if)# endiS5comm# configure terminal
iS5comm(config)# interface vlan 2
```

```
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 20.0.0.1 255.0.0.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# end

iS5comm# configure terminal
iS5comm(config)# interface gigabitethernet 0/2
iS5comm(config-if)# no shutdown
iS5comm(config-if)# end

iS5comm# configure terminal
iS5comm(config)# interface gigabitethernet 0/2
iS5comm(config-if)# switchport pvid 2
iS5comm(config-if)# end
```

3. Verify the VLAN configurations using the following command.

   FOR EXAMPLE: Type the following:

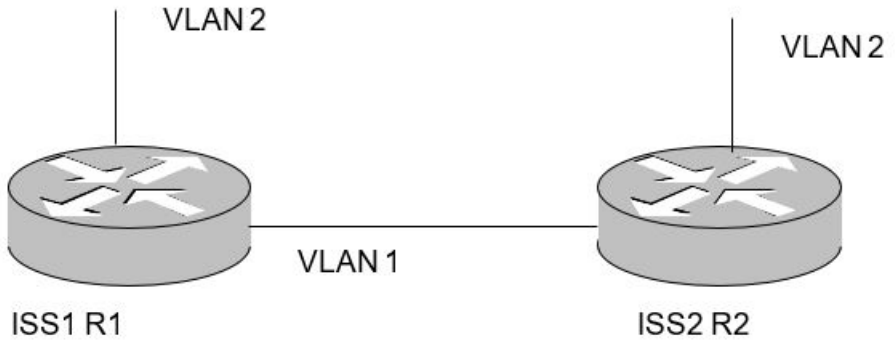
```
iS5comm# show ip interface
Vlan1 is up, line protocol is up
Internet Address is 12.0.0.1/8
Broadcast Address 12.255.255.255

Vlan2 is up, line protocol is up
Internet Address is 20.0.0.1/8
Broadcast Address 20.255.255.255
```

Configuring ISS2 in Topology for Testing BGP

CONTEXT:

The figure shown below depicts the topology setup used for this configuration as follows.

Figure 3: BGP Configuration and Testing topology



1. To configure ISS1 in Topology for testing BGP:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

2. To enable BGP in Router R2:

   FOR EXAMPLE: Execute the following commands:

```
iS5comm# configure terminal
iS5comm(config)# interface vlan 1
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 12.0.0.2 255.0.0.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# end

iS5comm# configure terminal
iS5comm(config)# interface gigabitethernet 0/1
iS5comm(config-if)# no shutdown
iS5comm(config-if)# end

iS5comm# configure terminal
iS5comm(config)# interface gigabitethernet 0/1
iS5comm(config-if)# switchport pvid 1
iS5comm(config-if)# end

iS5comm# configure terminal
iS5comm(config)# interface vlan 2
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 90.0.0.2255.0.0.0
```

```
iS5comm(config-if)# no shutdown
iS5comm(config-if)# end

iS5comm# configure terminal
iS5comm(config)# interface gigabitethernet 0/2
iS5comm(config-if)# no shutdown
iS5comm(config-if)# end

iS5comm# configure terminal
iS5comm(config)# interface gigabitethernet 0/2
iS5comm(config-if)# switchport pvid 2
iS5comm(config-if)# end
```

3. Verify the VLAN configurations using the following command.

   FOR EXAMPLE: Type the following:

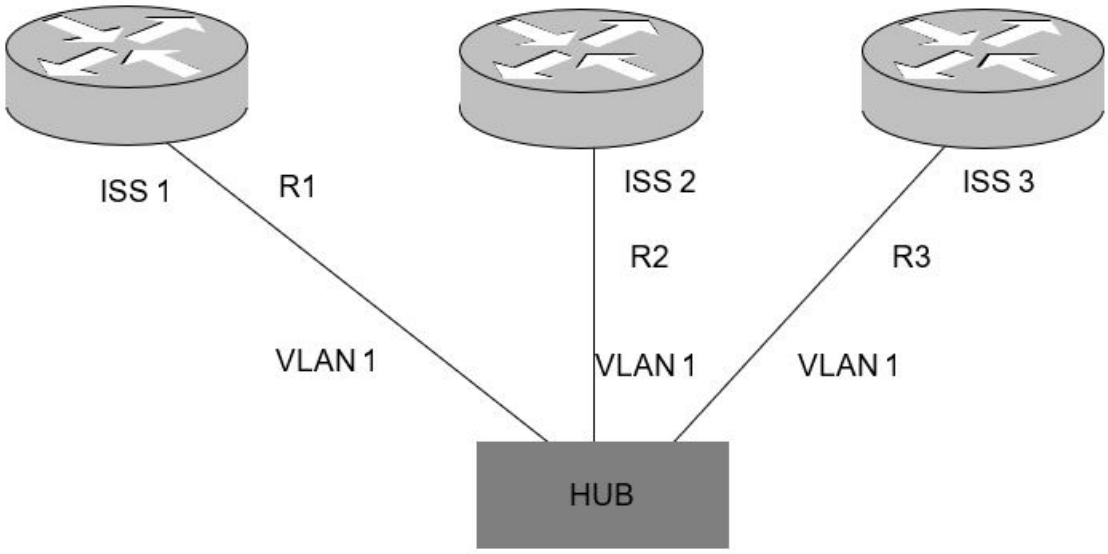
```
iS5comm# show ip interface
Vlan1 is up, line protocol is up
Internet Address is 12.0.0.2/8
Broadcast Address 12.255.255.255

Vlan2 is up, line protocol is up
Internet Address is 90.0.0.2/8
Broadcast Address 90.255.255.255
```

Configuring ISS3 in Topology for Testing BGP

CONTEXT:

The figure shown below depicts the topology setup used for this configuration as follows.

Figure 4: Configuration and Testing BGP Local Preference Value



1. To configure ISS3 in Topology for testing BGP:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

2. To enable BGP in Router R2:

   FOR EXAMPLE: Execute the following commands:

```
iS5comm# configure terminal
iS5comm(config)# interface vlan 1
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 12.0.0.3 255.0.0.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# end

iS5comm# configure terminal
iS5comm(config)# interface gigabitethernet 0/1
iS5comm(config-if)# no shutdown
iS5comm(config-if)# end

iS5comm# configure terminal
iS5comm(config)# interface gigabitethernet 0/1
iS5comm(config-if)# switchport pvid 1
iS5comm(config-if)# end
```

3. Verify the VLAN configurations using the following command.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip interface
Vlan1 is up, line protocol is up
Internet Address is 12.0.0.3/8
Broadcast Address 12.255.255.255
```

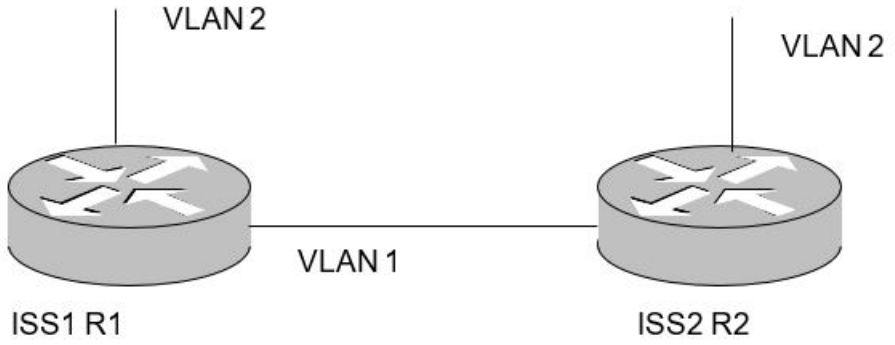
2. Configuration and Testing Topologies

This chapter provides sample deployment scenarios used for the configuration steps given in this document. The following sub sections depict sample topologies that can be used for configuring and testing the basic features of the *BGP* protocol.

2.1. Topology Scenarios for Configuring & Testing General BGP

The shown below topology depicts the sample topology used for configuring and testing *BGP*.

Figure 1: BGP Configuration and Testing Topology



The figure shown above depicts the components used in the topology. The description is as follows:

- ISS1 and ISS2 represent routers in which *ISS* is installed.
- VLAN1 and VLAN2 represent the *VLAN* interfaces of the *ISS* routers.
- Each *ISS* switch has a router ID.

Refer to the table below for the list of the IPv4 and IPv6 addresses of the interfaces and hosts shown.

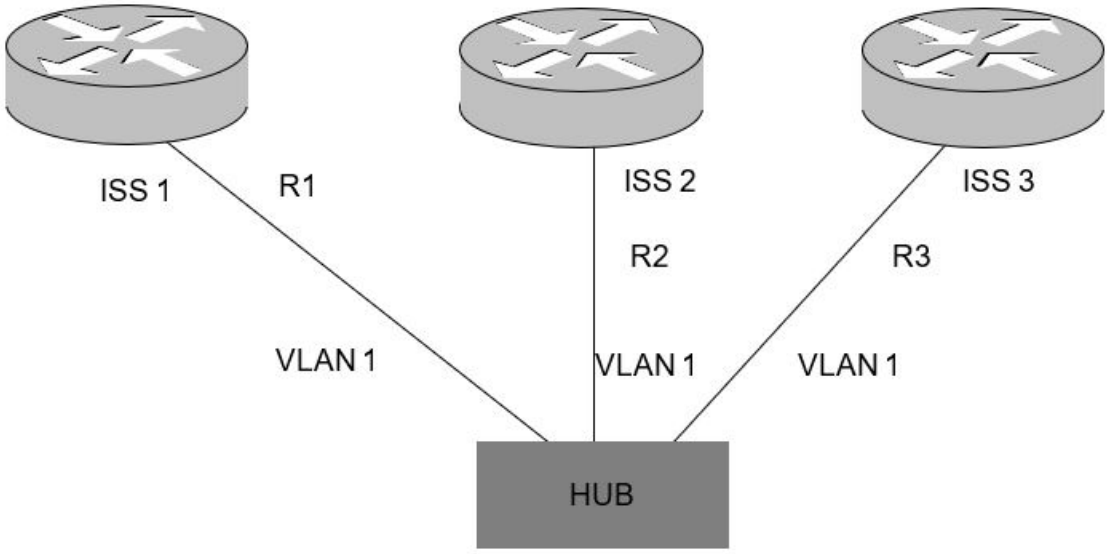
Table 1: IPv4 and IPv6 Addresses of Interfaces in the Routers and Hosts

Router/Host	Interface	Slot	IPv4 Address / Mask	IPv6 Address / Prefix Length
ISS1	VLAN1	0/1	12.0.0.1 / 255.0.0.0	fec0::1111:0:1 / 96, 1111::1/96
	VLAN2	0/2	20.0.0.1 / 255.0.0.0	fec0::2222:0:1 / 96, 2222::1/96
IS2	VLAN1	0/1	12.0.0.2 / 255.0.0.0	fec0::1111:0:2 / 96, 1111::2/96
	VLAN2	0/2	90.0.0.2 / 255.0.0.0	fec0::2222:0:2 / 96, 2222::2/96

2.2. Topology for Configuring and Testing BGP Local Preference

The shown below figure depicts the sample topology used for configuring and testing *BGP* Local Preference value.

Figure 2: Configuration and Testing BGP Local Preference Value



The figure shown above depicts the components used in the topology. The description is as follows:

- R1, R2 and R3 represent the *ISS* switches over which *BGP4* is enabled.
- ISS1, ISS2 and ISS3 represent *ISS* switches.
- Hub to connect all three routers.

The table below lists the IPv4 and IPv6 addresses of the interfaces and hosts shown.

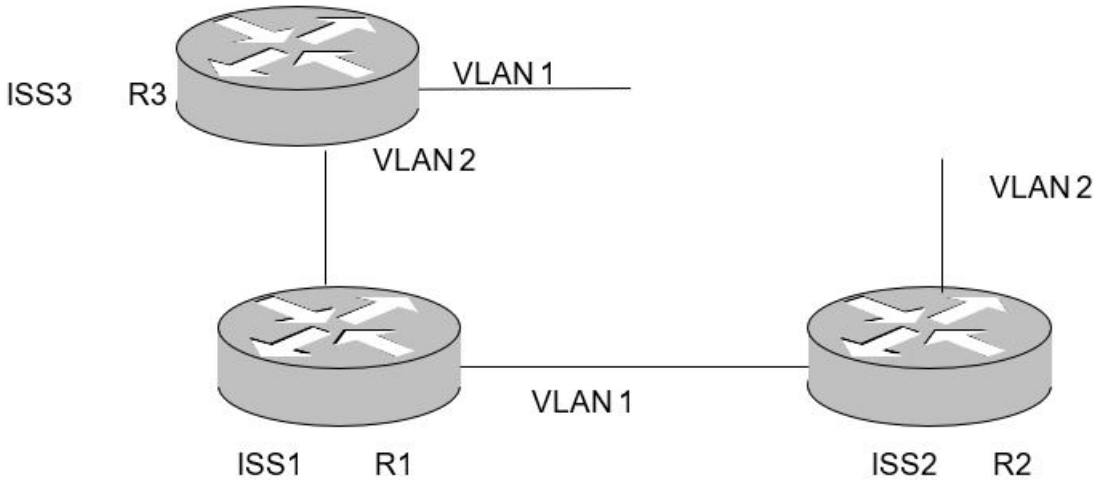
Table 2: IPv4 and IPv6 Addresses of Interfaces in the Routers and

Router/Host	Interface	Slot	IPv4 Address / Mask	IPv6 Address / Prefix Length
ISS1	VLAN1	0/1	10.0.0.1 / 255.0.0.0	fec0::1111:0:1 / 96, 1111::1/96
ISS2	VLAN1	0/1	10.0.0.2 / 255.0.0.0	fec0::1111:0:2 / 96, 2222::2/96
ISS3	VLAN1	0/1	10.0.0.3 / 255.0.0.0	fec0::1111:0:3 / 96, 3333::3/96

2.3. Topology for Configuring & Testing General BGP Internal Route Redistribution

The shown below figure depicts the sample topology used for configuring and testing *BGP* Internal route redistribution.

Figure 3: BGP Configuration and Testing Topology for BGP Internal route redistribution



The figure shown above depicts the components used in the topology. The description is as follows:

- ISS1, ISS2 and ISS3 represent routers in *ISS* switches.
- VLAN1 and VLAN2 represent the *VLAN* interfaces of the *ISS* routers.
- Each *ISS* switch has a router ID.

Refer to the table below for the list of the IPv4 and IPv6 addresses of the interfaces and hosts shown.

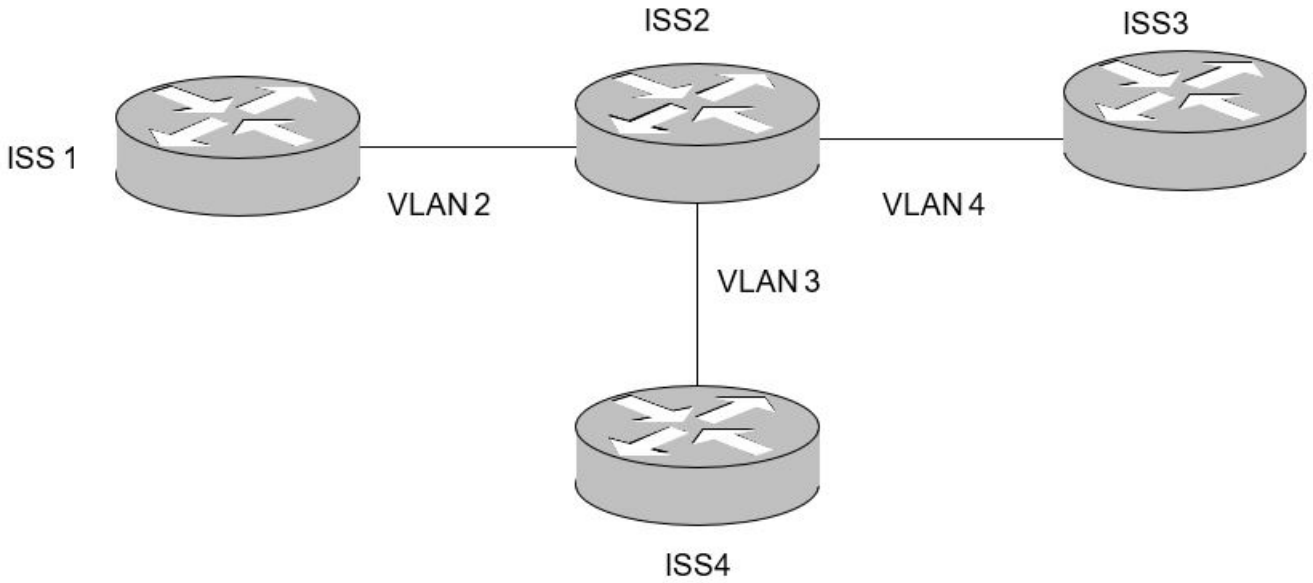
Table 3: IPv4 and IPv6 Addresses of Interfaces in the Routers and Hosts

Router/Host	Interface	Slot	IPv4 Address / Mask	IPv6 Address / Prefix Length
ISS1	VLAN1	0/1	12.0.0.1 / 255.0.0.0	fec0::1111:0:1 / 96, 1111::1/96
	VLAN2	0/2	20.0.0.1 / 255.0.0.0	fec0::2222:0:1 / 96, 2222::1/96
ISS2	VLAN1	0/1	12.0.0.2 / 255.0.0.0	fec0::1111:0:2 / 96, 1111::2/96
	VLAN2	0/2	90.0.0.2 / 255.0.0.0	fec0::2222:0:2 / 96, 2222::2/96
ISS3	VLAN1	0/1	12.0.0.3 / 255.0.0.0	fec0::1111:0:3 / 96, 1111::3/96
	VLAN2	0/2	90.0.0.3 / 255.0.0.0	fec0::2222:0:3 / 96, 2222::3/96

2.4. Topology for Configuring & Testing BGP Peer Groups

The shown below figure depicts the sample topology used for configuring and testing *BGP* Peer Groups.

Figure 4: Configuration and Testing BGP Peer Groups



The figure shown above depicts the components used in the topology. The description is as follows:

- ISS1, ISS2, ISS3, and ISS 4 are BGP4 enabled routers.

Refer to the table below for the list of the IPv4 and IPv6 addresses of the interfaces and hosts shown.

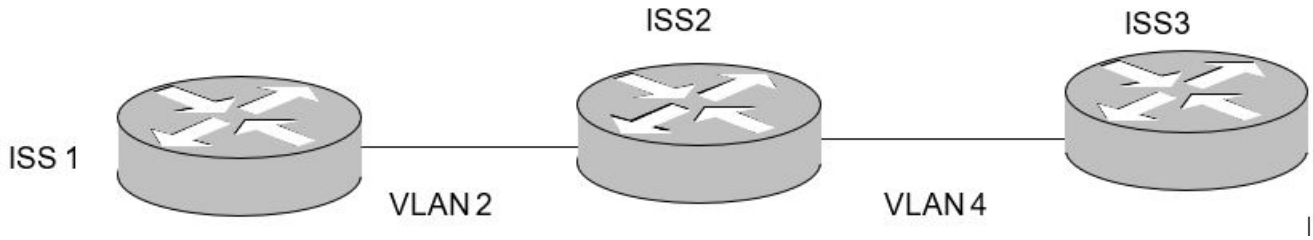
Table 4: IPv4 and IPv6 Addresses of Interfaces in the Routers and Hosts

Router/Host	Interface	Slot	IPv4 Address / Mask	IPv6 Address / Prefix Length
ISS1	VLAN2	0/2	14.0.0.1 / 255.0.0.0	fec0::1111:0:1 / 96, 1111::1/96
ISS2	VLAN2	0/2	14.0.0.2 / 255.0.0.0	fec0::1111:0:2 / 96, 1111::2/96
	VLAN3	0/3	15.0.0.1 / 255.0.0.0	fec0::1112:0:1 / 96, 2222::1 / 96
	VLAN4	0/4	16.0.0.1 / 255.0.0.0	fec0::1113:0:1 / 96, 4444::1 / 96
ISS3	VLAN4	0/3	15.0.0.2 / 255.0.0.0	fec0::1112:0:2 / 96, 2222::2 / 96
ISS4	VLAN3	0/4	16.0.0.2 / 255.0.0.0	fec0::1113:0:2 / 96, 4444::2 / 96

2.5. Topology for Configuring & Testing Cost Community Attribute

The shown below figure depicts the sample topology used for configuring and testing *BGP* Cost Community Attribute.

Figure 5: BGP Configuration and Testing Topology for BGP Cost Community Attribute



The figure shown above depicts the components used in the topology. The description is as follows:

- ISS1, ISS2, and ISS3 are *BGP4*-enabled routers.

Refer to the table below for the list of the IPv4 and IPv6 addresses of the interfaces and hosts shown.

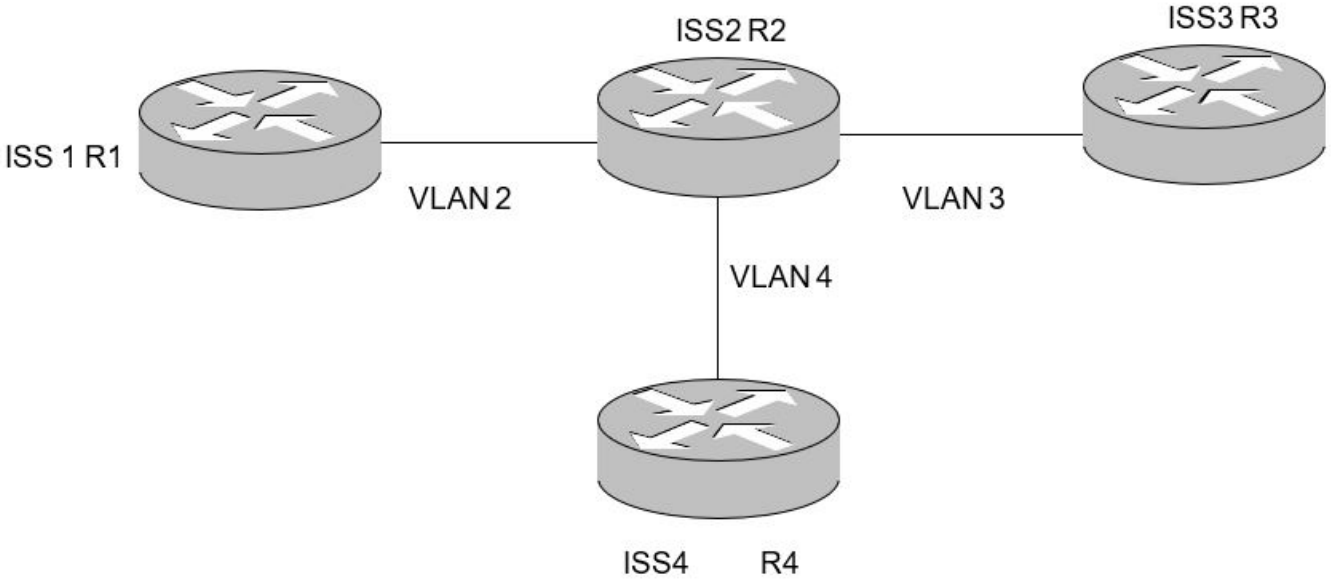
Table 5: IPv4 and IPv6 Addresses of Interfaces in the Routers and Hosts

Router/Host	Interface	Slot	IPv4 Address / Mask	IPv6 Address / Prefix Length
ISS1	VLAN2	0/2	14.0.0.1 / 255.0.0.0	fec0::1111:0:1 / 96, 1111::1/96
ISS2	VLAN2	0/2	14.0.0.2 / 255.0.0.0	fec0::1111:0:2 / 96, 1111::2/96
	VLAN4	0/4	15.0.0.1 / 255.0.0.0	fec0::1112:0:1 / 96, 2222::1 / 96
ISS3	VLAN4	0/3	15.0.0.2 / 255.0.0.0	fec0::1112:0:2 / 96, 2222::2 / 96

2.6. Topology for Configuring BGP Aggregation

The shown below figure depicts the sample topology used for configuring and testing *BGP* aggregation.

Figure 6: BGP Configuration for BGP aggregation



The figure shown above depicts the components used in the topology. The description is as follows:

- ISS1, ISS2, ISS3, and ISS 4 are *BGP4*-enabled routers.
- VLAN2, VLAN3, and VLAN4 represent the *VLAN* interfaces of the *ISS* routers.
- Each *ISS* switch has a router ID.

Refer to the table below for the list of the IPv4 and IPv6 addresses of the interfaces and hosts shown.

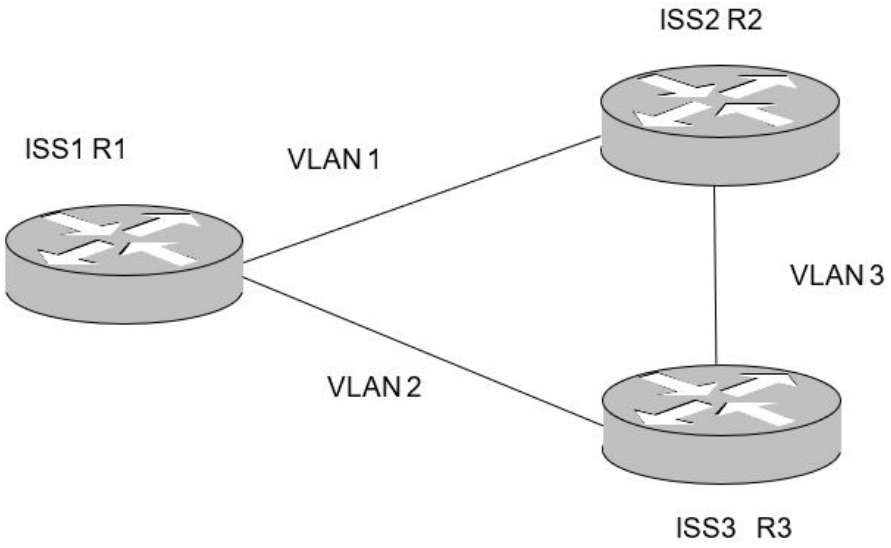
Table 6: IPv4 and IPv6 Addresses of Interfaces in the Routers and Hosts

Router/Host	Interface	Slot	IPv4 Address / Mask	IPv6 Address / Prefix Length
ISS1	VLAN1	0/1	14.0.0.1 / 255.0.0.0	fec0::1111:0:1 / 96, 1111::1/96
	VLAN2	0/2	13.0.0.1 / 255.0.0.0	fec0::2222:0:1 / 96, 2222::1/96
ISS2	VLAN1	0/1	14.0.0.2 / 255.0.0.0	fec0::1111:0:2 / 96, 1111::2/96
	VLAN2	0/2	13.0.0.2 / 255.0.0.0	fec0::2222:0:2 / 96, 2222::2/96
	VLAN3	0/3	16.0.0.1 / 255.0.0.0	fec0::3333:0:2 / 96, 3333::2/96
	VLAN4	0/4	15.0.0.1 / 255.0.0.0	fec0::4444:0:2 / 96, 4444::2/96
ISS3	VLAN3	0/3	16.0.0.2 / 255.0.0.0	fec0::3333:0:3 / 96, 3333::3/96
ISS4	VLAN4	0/4	15.0.0.2 / 255.0.0.0	fec0::4444:0:3 / 96, 4444::4/96

2.7. Topology for Configuring BGP Multipath

The shown below figure depicts the sample topology used for configuring and testing *BGP* multipath.

Figure 7: BGP Configuration for BGP Multipath



The figure shown above depicts the components used in the topology. The description is as follows:

- ISS1, ISS2 and ISS3 are BGP4 enabled routers.

- VLAN1 and VLAN2 represent the *VLAN* interfaces of the *ISS* routers.
- Each BGP router has a router ID.

Refer to the table below for the list of the IPv4 and IPv6 addresses of the interfaces and hosts shown.

Table 7: IPv4 and IPv6 Addresses of Interfaces in the Routers and Hosts

Router/Host	Interface	Slot	IPv4 Address / Mask	IPv6 Address / Prefix Length
ISS1	VLAN1	0/1	14.0.0.1 / 255.0.0.0	fec0::1111:0:1 / 96, 1111::1/96
	VLAN2	0/2	13.0.0.1 / 255.0.0.0	fec0::2222:0:1 / 96, 2222::1/96
ISS2	VLAN1	0/1	14.0.0.2 / 255.0.0.0	fec0::1111:0:2 / 96, 1111::2/96
	VLAN3	0/2	16.0.0.1 / 255.0.0.0	fec0::3333:0:1 / 96, 3333::1/96
ISS3	VLAN2	0/1	13.0.0.2 / 255.0.0.0	fec0::2222:0:2 / 96, 2222::2/96
	VLAN3	0/2	16.0.0.2 / 255.0.0.0	fec0::3333:0:2 / 96, 3333::2/96

Table 8: BGP ASN and Router Ids for the Routers

Router / Host	BGP ASN	BGP RouterID
ISS1	100	13.0.0.1
ISS2	200	14.0.0.2
ISS3	200	13.0.0.2

BGP Configuration

3. BGP Configuration

The Border Gateway Protocol version 4 (*BGP4*) has been designed in accordance with the FSAP2 (Flexible Software Architecture for Portability) to ensure a high level of portability.

This chapter describes the configuration of the following BGP features using CLI interface.

- Configuring BGP4 Global Router Information
- Configuring BGP Peer Extension Information
- Configuring BGP Neighbor Connected Information
- Configuring BGP MED (Multi Exit Discriminator) Policy Information
- Configuring BGP LocalPref Policy Information
- Configuring BGP Update Filter Policy Information
- Configuring BGP Aggregate Policy information
- BGP Route Redistribution
- BGP Route Reflector Information
- BGP Route Flap Dampening Information
- Configuring BGP Community Global Information
- Configuring BGP Community Policies
- Configuring BGP Extended Community Policies
- Configuring BGP Peer Link Bandwidth Entry
- Configuring BGP Supported Capabilities
- Configuring AS Confederation Peers
- Route-Refresh / SoftReconfig Inbound Configuration
- Configuring Peer TCP-MD5 Authentication Information
- Automatic Start Feature for BGP Peer
- Automatic Stop Feature for BGP Peer
- Delaying sending of OPEN messages
- Configuring the Maximum Peer Prefixes Limit for a Peer
- Configuring BGP Keep Alive Interval and Peer Hold Time
- Configuring BGP Idle Hold Time and Delay Open Time
- Configuring BGP Originator ID
- Configuring BGP Connect Retry Count value for a peer
- Configuring BGP Connect Retry Timeout Value

- Shutdown of BGP Peer

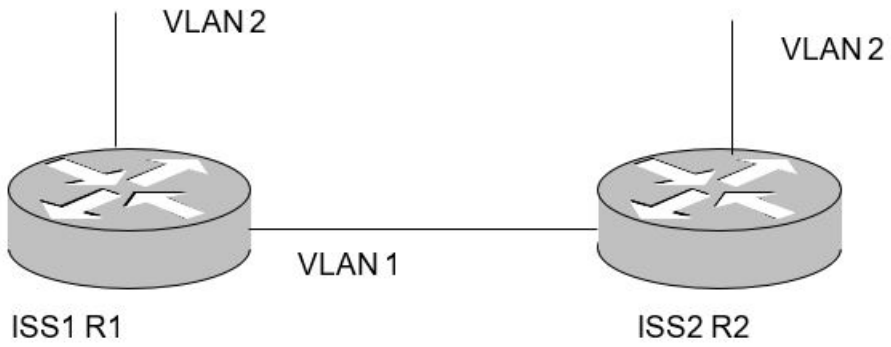
3.1. Configuring BGP Global Status

The global status configuration for a BGP Peer is given in the below steps.

CONTEXT:

The figure shown below depicts the topology setup used for this configuration.

Figure 1: BGP Configuration and Testing Topology



Use the following commands for global status configuration for a *BGP* Peer.

1. To globally enable *BGP* in the router:

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number.

   ```
   iS5comm(config)# as-num 100
   ```

   – Enter the Router Id value.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Set the *AS* number of the BGP Speaker.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Exit the Global Configuration mode.

   ```
   iS5comm(config)# end
   ```

   – View *BGP* statistics related to the peer.

   ```
   iS5comm# show ip bgp summary
   BGP router identifier is 12.0.0.1, local AS number 100
   Forwarding State is enabled
   BGP router identifier is 12.0.0.1, local AS number 100
   BGP table version is 0
   ```

```
Neighbor Version AS Msg RcvdMsgSent Up/DownState/PfxRcd
 ------------------------------ ---------------
12.0.0.2 4 2007700:00:3:2 Established
```

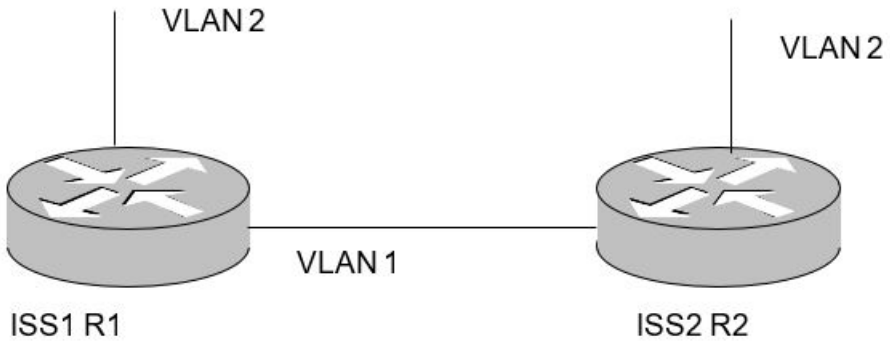
3.2. BGP Session Establishment between External Peers

Peers from two different autonomous systems are external peers. The following steps reveal how *BGP* Session establishment is made between two external peers.

CONTEXT:

The figure shown below depicts the topology setup used for this configuration.

Figure 2: BGP Configuration and Testing Topology



Use the following commands to configure *BGP* routing.

1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Enable BGP in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R2 (with as-num 200) as external peer in R1.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 remote-as 200
   ```

2. To enable *BGP* in Router R2:

   FOR EXAMPLE: Execute the following commands:

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enter the Autonomous System (*AS*) number in R2.

```
iS5comm(config)# as-num 200
```

– Configure the router-id in R2.

```
iS5comm(config)# router-id 12.0.0.2
```

– Enable BGP in R2.

```
iS5comm(config)# router bgp 200
```

– Configure R1 (with as-num 100) as external peer in R2.

```
iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100
```

3. Verify that the *BGP* session between the external peers R1 and R2 is established, using the following show commands in R1 and R2.

FOR EXAMPLE: Type the following:

– R1: View the bgp summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
Forwarding State is enabled
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
 ------------------------------- ----------------
12.0.0.2   4    200   7      7   00:00:3:2 Established

iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 200, external link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 10 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status: NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 2 messages, 0 Updates
Sent 2 messages, 0 Updates
Route refresh: Received 0, sent 0.
```

```
Minimum time between advertisement runs is 30 seconds
Connections established 1 time(s)
Local host: 12.0.0.1, Local port: 179
Foreign host: 12.0.0.2, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

– View the peer details for IPv6 entry.

```
iS5comm# show bgp ipv6 neighbor
BGP neighbor is fec0::1111:0:2, remote AS 200, internal link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 27 minutes 22 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 54 messages, 0 Updates
Sent 55 messages, 0 UpdatesRoute refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 secondsConnections
established 1 time(s)
Local host: 0.0.192.254, Local port: 179
Foreign host: 0.0.192.254, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

– R2: View the BGP summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.2, local AS number 200
BGP table version is 0
Neighbor Version ASMsgRcvd MsgSent Up/DownState/PfxRcd
 -------- ------- ---- -------------- ----------------
12.0.0.1   4    100  13     13   00:00:5:40 Established
```

– View the peer details for IPv6 entry.

```
iS5comm# show ip ipv6 neighbor
BGP neighbor is fec0::1111:0:1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.1
BGP state = Established, up for 24 minutes 57 seconds
```

```
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 50 messages, 0 Updates
Sent 50 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
Connections established 1 time(s)
Local host: 0.0.192.254, Local port: 49152
Foreign host: 0.0.192.254, Foreign port: 179
Last Error: Code 0, SubCode 0.
```

NOTE: BGP can be enabled on pseudowire interface similarly to BGP on router port.

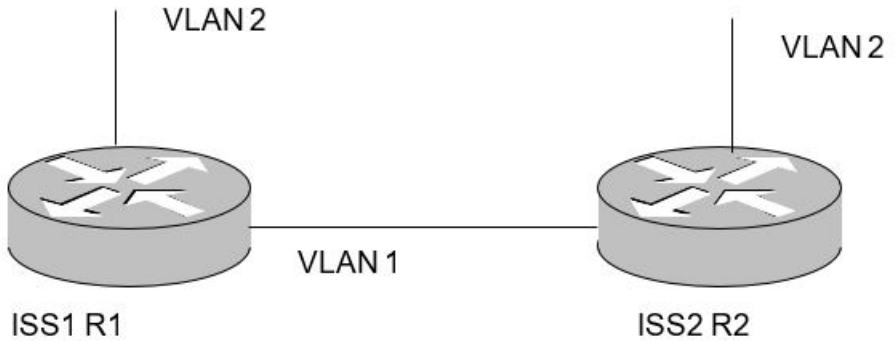
3.3. BGP Session Establishment between Internal Peers

Peers from the same autonomous systems are referred as internal peers. The following steps describe how *BGP* Session establishment is made between two internal peers.

CONTEXT:

The figure shown below depicts the topology setup used for this configuration.

Figure 3: BGP Configuration and Testing Topology



Use the following commands to configure *BGP* routing.

1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enter the Autonomous System (*AS*) number in R1.

```
iS5comm(config)# as-num 100
```

– Configure the router-id in R1.

```
iS5comm(config)# router-id 12.0.0.1
```

– Enable *BGP* in R1.

```
iS5comm(config)# router bgp 100
```

– Configure R2 (with as-num 100) as internal peer in R1.

```
iS5comm(config-router)# neighbor 12.0.0.2 remote-as 100
```

2. To enable *BGP* in Router R2:

FOR EXAMPLE: Execute the following commands:

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enter the Autonomous System (*AS*) number in R2.

```
iS5comm(config)# as-num 100
```

– Configure the router-id in R2.

```
iS5comm(config)# router-id 12.0.0.2
```

– Enable *BGP* in R2.

```
iS5comm(config)# router bgp 200
```

– Configure R1 (with as-num 100) as internal peer in R2.

```
iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100
```

3. Verify that the *BGP* session between the external peers R1 and R2 is established, using the following show commands in R1 and R2.

FOR EXAMPLE: Type the following:

– R1: View the bgp summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
 ------------------------------- ----------------
12.0.0.2   4    100   2     2    00:00:00:23 Established

iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 100, external link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 3 minutes 11 seconds
```

```
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status: NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 8 messages, 0 Updates
Sent 8 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
Connections established 1 time(s)
Local host: 12.0.0.1, Local port: 179
Foreign host: 12.0.0.2, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

– View the peer details for IPv6 entry.

```
iS5comm# show bgp ipv6 neighbor
BGP neighbor is fec0::1111:0:2, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 27 minutes 22 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 50 messages, 0 Updates
Sent 50 messages, 0 UpdatesRoute refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
Connections established 1 time(s)
Local host: 0.0.192.254, Local port: 179
Foreign host: 0.0.192.254, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

– R2: View the bgp summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version ASMsgRcvd MsgSent Up/DownState/PfxRcd
 -------- ------- ---- -------------- ----------------
12.0.0.1 4 1002 200:00:00:6 Established
```

– View the peer details for the neighbor.

```
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.1
BGP state = Established, up for 3 minutes 55 seconds
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 9 messages, 0 Updates
Sent 9 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 12.0.0.2, Local port: 49152
Foreign host: 12.0.0.1, Foreign port: 179
Last Error: Code 0, SubCode 0.
```

– View the peer details for IPv6 entry.

```
iS5comm# show ip ipv6 neighbor
BGP neighbor is fec0::1111:0:1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 27 minutes 22 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 54 messages, 0 Updates
```

```
Sent 55 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 0.0.192.254, Local port: 49152
Foreign host: 0.0.192.254, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

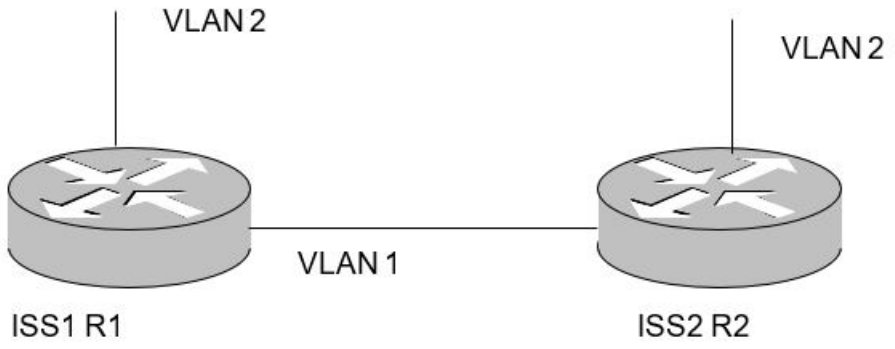
3.4. Verifying the Automatic Start Feature for BGP Peers

Session Establishment for External Peers

CONTEXT:

The figure shown below depicts the topology setup used for this configuration.

Figure 4: BGP Configuration and Testing Topology



Use the following commands to configure *BGP* routing.

1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Enable BGP in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R2 (with as-num 200) as external peer in R1, enabling the autostart feature and setting the value of idle hold timer as 30 seconds. The peer will now wait for 30 seconds before initiating the connection.

```
iS5comm(config-router)# neighbor 12.0.0.2 remote-as 200 allow-autostart
idlehold-time 30
```

2. To enable *BGP* in Router R2:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

   – Enter the Autonomous System (*AS*) number in R2.

```
iS5comm(config)# as-num 200
```

   – Configure the router-id in R2.

```
iS5comm(config)# router-id 12.0.0.2
```

   – Enable *BGP* in R2.

```
iS5comm(config)# router bgp 200
```

   – Configure R1 (with as-num 100) as external peer in R2, enabling the autostart feature and setting the value of idle hold timer as 20 seconds. The peer will now wait for 20 seconds before initiating the connection.

```
iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100 allow-autostart
idlehold-time 20
```

3. Verify that the *BGP* session between the external peers R1 and R2 is established, using the following show commands in R1 and R2.

   FOR EXAMPLE: Type the following:

   – R1: View the bgp summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
 ------------------------------- ----------------
12.0.0.2   4     200 67     66     00:00:00:0 Established

iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 200, external link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 3 minutes 11 seconds
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status: NOT DAMPED
```

```
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 8 messages, 0 Updates
Sent 8 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
Connections established 1 time(s)
Local host: 12.0.0.1, Local port: 179
Foreign host: 12.0.0.2, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

– View the peer details for IPv6 entry.

```
iS5comm# show bgp ipv6 neighbor
BGP neighbor is fec0::1111:0:2, remote AS 200, internal link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 1 hour 5 minutes 39 seconds
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 50 messages, 0 Updates
Sent 50 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
Connections established 1 time(s)
Local host: 0.0.192.254, Local port: 179
Foreign host: 0.0.192.254, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

– R2: View the *BGP* summary information.

```
iS5comm# show ip bgp summary
```

```
BGP router identifier is 12.0.0.2, local AS number 100
BGP table version is 0
Neighbor Version ASMsgRcvd MsgSent Up/DownState/PfxRcd
 -------- ------- ---- -------------- ----------------
12.0.0.1   4    100 78      79     00:00:00:0 Established
```

– View the peer details for the neighbor.

```
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.1
BGP state = Established, up for 39 minutes 44 seconds
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
```

– View the peer details for IPv6 entry.

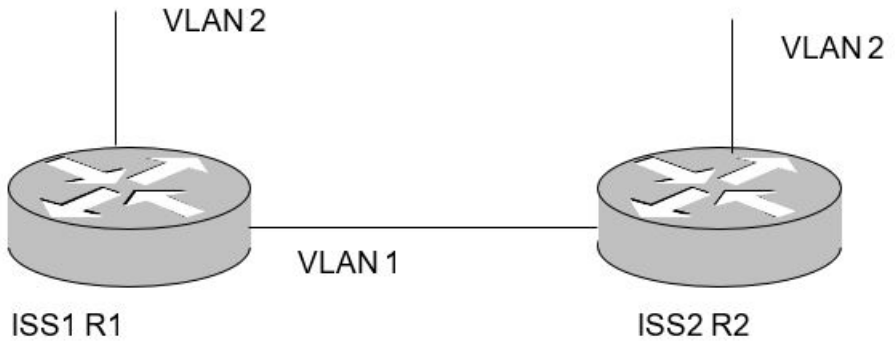
```
iS5comm# show ip ipv6 neighbor
BGP neighbor is fec0::1111:0:1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 27 minutes 22 seconds
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Idlehold time is 20
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 78 messages, 0 Updates
Sent 79 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
Connections established 1 time(s)
Local host: 12.0.0.2, Local port: 49152
Foreign host: 12.0.0.1, Foreign port: 179
Last Error: Code 0, SubCode 0.
```

Session Establishment for Internal Peers

CONTEXT:

The figure shown below depicts the topology setup used for this configuration.

Figure 5: BGP Configuration and Testing Topology



Use the following commands to configure *BGP* routing.

1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R2 (with as-num 100) as internal peer in R1, enabling the autostart feature and setting the value of idle hold timer as 30 seconds. The peer will now wait for 30 seconds before initiating the connection.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 remote-as 100 allow-autostart
   idlehold-time 30
   ```

2. To enable *BGP* in Router R2:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R2.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R2.

```
iS5comm(config)# router-id 12.0.0.2
```

– Enable *BGP* in R2.

```
iS5comm(config)# router bgp 100
```

– Configure R1 (with as-num 100) as internal peer in R2, enabling the autostart feature and setting the value of idle hold timer as 20 seconds. The peer will now wait for 20 seconds before initiating the connection.

```
iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100 allow-autostart
idlehold-time 20
```

3. Verify that the *BGP* session between the internal peers R1 and R2 is established, using the following show commands in R1 and R2.

FOR EXAMPLE: Type the following:

– R1: View the bgp summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
 ------------------------------- ----------------
12.0.0.2    4   100   12     13   00:00:00:0 Established

iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 100, external link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up 5 minutes 57 seconds
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status: NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 12 messages, 0 Updates
Sent 13 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 12.0.0.1, Local port: 179
```

```
Foreign host: 12.0.0.2, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

– View the peer details for IPv6 entry.

```
iS5comm# show bgp ipv6 neighbor
BGP neighbor is fec0::1111:0:2, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 1 hour 5 minutes 39 seconds
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 129 messages, 0 Updates
Sent 129 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 0.0.192.254, Local port: 179
Foreign host: 0.0.192.254, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

– R2: View the *BGP* summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.2, local AS number 100
BGP table version is 0
Neighbor Version ASMsgRcvd MsgSent Up/DownState/PfxRcd
 -------- ------- ---- -------------- ----------------
12.0.0.1  4     100  4        4    00:00:00:0 Established
```

– View the peer details for the neighbor.

```
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.1
BGP state = Established, up for 7 minute 18 seconds
```

```
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Idlehold time is 20
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 4 messages, 0 Updates
Sent 4 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 12.0.0.2, Local port: 49152
Foreign host: 12.0.0.1, Foreign port: 179
Last Error: Code 0, SubCode 0.
```

– View the peer details for IPv6 entry.

```
iS5comm# show ip ipv6 neighbor
BGP neighbor is fec0::1111:0:1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.1
BGP state = Established, up for 24 minutes 57 seconds
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Idlehold time is 20
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 50 messages, 0 Updates
Sent 50 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
```

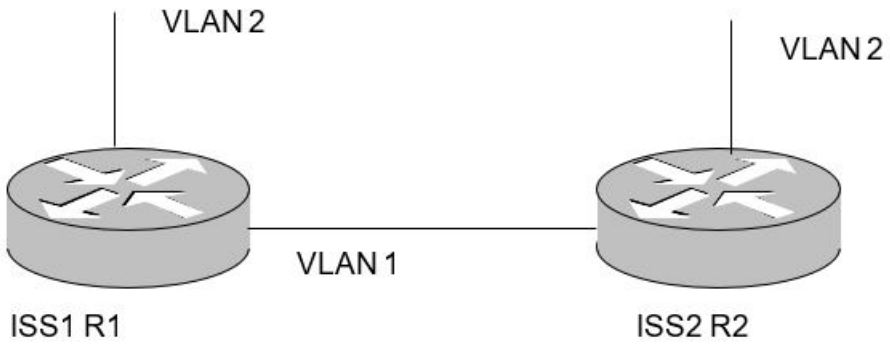
```
Connections established 1 time(s)
Local host: 0.0.192.254, Local port: 4915
Foreign host: 0.0.192.254, Foreign port: 179
Last Error: Code 0, SubCode 0.
```

3.5. BGP Delay OPEN feature – Internal Peers

CONTEXT:

The figure shown below depicts the topology setup used for this configuration.

Figure 6: BGP Configuration and Testing Topology



Use the following commands to configure *BGP* routing.

1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R2 (with as-num 100) as internal peer in R1, enabling the autostart feature and setting the value of idle hold timer as 20 seconds. The peer will now wait for 20 seconds before initiating the connection.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 remote-as 100 allow-autostart
   idlehold-time 20
   ```

   – Enable Delay OPEN flag in R1.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 delay-open
   ```

– Configure the Delay Open Timer to 50 seconds in R1. So the router R1 will wait for a period of 50 seconds before sending the OPEN message.

```
iS5comm(config-router)# neighbor 12.0.0.2 timers delayopentime 50
```

2. To enable *BGP* in Router R2:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R2.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R2.

   ```
   iS5comm(config)# router-id 12.0.0.2
   ```

   – Enable *BGP* in R2.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R1 (with as-num 100) as internal peer in R2, enabling the autostart feature and setting the value of idle hold timer as 20 seconds. The peer will now wait for 20 seconds before initiating the connection.

   ```
   iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100 allow-autostart
   idlehold-time 20
   ```

   – Enable Delay OPEN flag in R2.

   ```
   iS5comm(config-router)# neighbor 12.0.0.1 delay-open
   ```

   – Configure the Delay Open Timer to 60 seconds in R2. So, the router R2 will wait for a period of 60 seconds before sending the OPEN message.

   ```
   iS5comm(config-router)# neighbor 12.0.0.1 timers delayopentime 60
   ```

   Both internal peers R1 and R2 move to Connect state after the idle hold timer expires. They remain in the Connect state till the Delay Open Timer expires. After the Delay Open timer expires, the Peer sends its OPEN message to its neighbor and moves from the Connect State.

3. Verify that the *BGP* session between the external peers R1 and R2 is established, using the following show commands in R1 and R2.

   FOR EXAMPLE: Type the following:

   – R1: View the bgp summary information.

   ```
   iS5comm# show ip bgp summary
   BGP router identifier is 12.0.0.1, local AS number 100
   BGP table version is 0
   Neighbor Version AS MsgRcvdMsgSent Up/DownState/PfxRcd
    ------------------------------ ---------------
   12.0.0.2  4     100  0      0        -Connect
   ```

```
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 100, external link
BGP version 4, remote router ID 0.0.0.0
BGP state = Connect
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
DelayOpen ENABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Idlehold time is 20 DelayOpen interval is 50 secs
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Received 0 messages, 0 Updates
Sent 0 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 0 time(s)
Local host: 12.0.0.1, Local port: 49152
Foreign host: 12.0.0.2, Foreign port: 179
Last Error: Code 0, SubCode 0.
```

– R2: View the BGP summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.2, local AS number 100
BGP table version is 0
Neighbor Version ASMsgRcvd MsgSent Up/DownState/PfxRcd
 -------- ------- ---- -------------- ----------------
12.0.0.1  4     100  0      0        -Connect
```

– View the peer details for the neighbor.

```
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.1, remote AS 100, internal link
BGP version 4, remote router ID 0.0.0.0
BGP state = Connect
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
DelayOpen ENABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
```

```
Peer Status : NOT DAMPED
Idlehold time is 20 DelayOpen interval is 60 secs
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Received 0 messages, 0 Updates
Sent 0 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 0 time(s)
Local host: 12.0.0.2, Local port: 179
Foreign host: 12.0.0.1, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

Verify that the BGP session between the internal peers R1 and R2 is established finally after the Delay Open timer expires at both the ends by using the following show commands in R1 and R2.

– R1: View the BGP summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvd MsgSent Up/Down State/PfxRcd
---------------------------------------- ------------
12.0.0.2 4      100  13     9      14000:00:00:0 Established

iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 1 hour 11 minutes 14 seconds
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
DelayOpen ENABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Idlehold time is 20 DelayOpen interval is 50 secs
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 139 messages, 0 Updates
```

```
Sent 140 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 12.0.0.1, Local port: 49152
Foreign host: 12.0.0.2, Foreign port: 179
Last Error: Code 0, SubCode 0
```

– View the peer details for IPv6 entry.

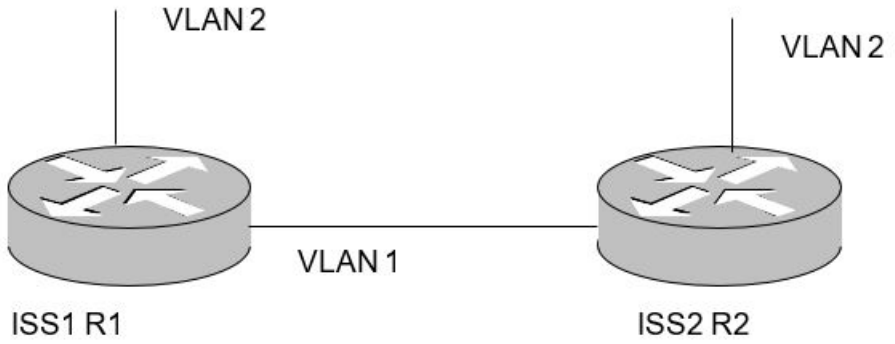
```
iS5comm# show ip bgp neighbor
BGP neighbor is fec0::1111:0:2, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 29 seconds
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
DelayOpen ENABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Idlehold time is 20 DelayOpen interval is 50 secs
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 2 messages, 0 Updates
Sent 2 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 0.0.192.254, Local port: 179
Foreign host: 0.0.192.254, Foreign port: 49153
Last Error: Code 0, SubCode 0.
```

3.6. BGP Automatic Stop feature – Internal Peers

CONTEXT:

The figure shown below depicts the topology setup used for this configuration.

Figure 7: BGP Configuration and Testing Topology



Use the following commands to configure *BGP* routing.

1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R2 (with as-num 100) as internal peer in R1, enabling the autostart feature, and setting the value of idle hold timer as 20 seconds. The peer will now wait for 30 seconds before initiating the connection.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 remote-as 100 allow-autostart
   idlehold-time 20
   ```

   – Enable Automatic Stop flag in R1.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 allow-autostop
   ```

   – Connect-retry-count as 2 for R1. It denotes the Maximum number of times the *BGP* Peer can issue a TCP-Connect with its neighboring peers.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 connect-retry-count 2
   ```

2. To enable *BGP* in Router R2:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R2.

   ```
   iS5comm(config)# as-num 100
   ```

– Configure the router-id in R2.

```
iS5comm(config)# router-id 12.0.0.2
```

– Enable BGP in R2.

```
iS5comm(config)# router bgp 100
```

– Configure R1 (with as-num 100) as internal peer in R2.

```
iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100
```

3. Verify that the *BGP* session between the internal peers R1 and R2 is established, after the idle hold timer expires in R1, using the following show commands in R1 and R2.

FOR EXAMPLE: Type the following:

– R1: View the bgp summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvdMsgSent Up/DownState/PfxRcd
 ------------------------------- ----------------
12.0.0.2  4     100  3      3        00:00:00:0 Established

iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 100, external link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 1 minute 27 seconds
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
DelayOpen ENABLED
Configured Connect Retry Count 2
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Idlehold time is 20 DelayOpen interval is 50 secs
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Received 0 messages, 0 Updates
Sent 4 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 0 time(s)
Local host: 12.0.0.1, Local port: 49152
Foreign host: 12.0.0.2, Foreign port: 179
Last Error: Code 0, SubCode 0.
```

– R2: View the *BGP* summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.2, local AS number 100
BGP table version is 0
Neighbor Version ASMsgRcvd MsgSent Up/DownState/PfxRcd
 -------- ------- ---- -------------- ----------------
12.0.0.1  4     100  6      3        6300:00:00:0 Established
```

– View the peer details for the neighbor.

```
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.1
BGP state = Established, up for 31 minutes 38 seconds
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
DelayOpen ENABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Idlehold time is 20 DelayOpen interval is 60 secs
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Received 63 messages, 0 Updates
Sent 63 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 12.0.0.2, Local port: 179
Foreign host: 12.0.0.1, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

Whenever a CEASE message is received from a peer, Automatic Stop event takes place. In response to this event, the Current Connect Retry Count is incremented, and the peer moves to its Idle State. It remains in the Idle State until the Idle Hold timer expires. After the timer expires, the peer begins to initiate the connection with its neighboring peer. Whenever a CEASE message is received, the Error Code becomes 6.

To generate and check this scenario, we need to manually issue the following commands:

At R2,

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enable BGP in R2.

```
iS5comm(config)# router bgp 100
```

– Shutdown the neighbor R1 from R2.

```
iS5comm(config-router)# no neighbor 12.0.0.1 remote-as 100
```

– Configure the neighbor R1 from R2.

```
iS5comm(config)# neighbor 12.0.0.1 remote-as 100
```

R1: View the bgp summary information immediately at R1 using 'show ip bgp summary'

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
------------------------------- -------------------
12.0.0.2  4     100  0      0        - Idle
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 100, internal link
BGP version 0, remote router ID 0.0.0.0
BGP state = Idle
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
AutomaticStop ENABLED
Configured Connect Retry Count 2
Current Connect Retry Count 1
Peer Status : NOT DAMPED
Idlehold time is 20 Rcvd update before 0 secs, hold time is 90,
keepalive interval is 30 secs
Received 0 messages, 0 Updates
Sent 0 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 0.0.0.0, Local port: 0
Foreign host: 12.0.0.2, Foreign port: 0
Last Error: Code 6, SubCode 0.
```

R2: View the bgp summary information using 'show ip bgp summary'

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
```

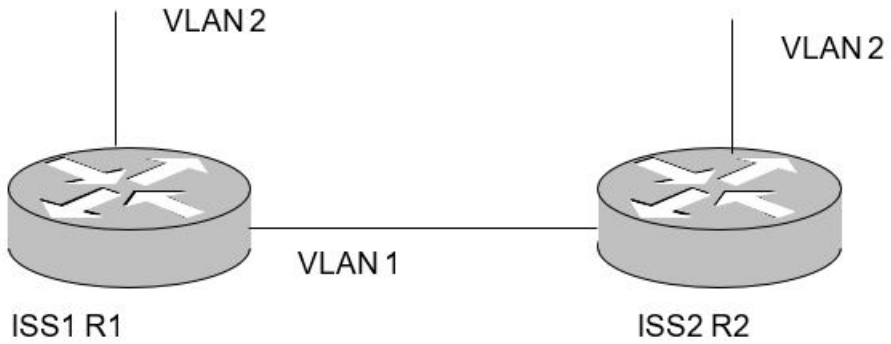
```
-------------------------------- -------------------
12.0.0.1  4     100  119   119      00:00:00:0 Established
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.1, remote AS 100, internal link
BGP version 0, remote router ID 12.0.0.1
BGP state = Established, up for 1 hour 1 minute 16 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 120 messages, 0 Updates
Sent 120 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 12.0.0.2, Local port: 179
Foreign host: 12.0.0.1, Foreign port: 49152
Last Error: Code 0, SubCode 0
```

3.7. BGP Damp Peer Oscillations Feature – Internal Peers

CONTEXT:

The figure shown below depicts the topology setup used for this configuration.

Figure 8: BGP Configuration and Testing Topology



Use the following commands to configure *BGP* routing.

1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R2 (with as-num 100) as internal peer in R1 with automatic start feature enabled. Set the Idle Hold Timer value as 20 seconds.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 remote-as 100 allow-autostart
   idlehold-time 20
   ```

   – Enable Automatic Stop Flag for R1.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 allow-autostop
   ```

   – Configure the Connect-retry-count as 1 for R1. It denotes the Maximum number of times the *BGP* Peer can issue a TCP-Connect with its neighboring peers.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 connect-retry-count 1
   ```

   – Enable Damp Peer Oscillations Flag for R1.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 damp-peer-oscillations
   ```

2. To enable *BGP* in Router R2:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R2.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R2.

   ```
   iS5comm(config)# router-id 12.0.0.2
   ```

   – Enable BGP in R2.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R1 (with as-num 100) as internal peer in R2.

   ```
   iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100
   ```

3. Verify that the *BGP* session between the internal peers R1 and R2 is established, after the idle hold timer expires in R2, using the following show commands in R1 and R2.

   FOR EXAMPLE: Type the following:

– R1: View the bgp summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvdMsgSent Up/DownState/PfxRcd
 ------------------------------ ----------------
12.0.0.2  4     100  3      3        00:00:00:0 Established

iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 100, external link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 36 seconds
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
AutomaticStop ENABLED
DampPeer Oscillations ENABLED
Configured Connect Retry Count 1
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Idlehold time is 20
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 3 messages, 0 Updates
Sent 3 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 12.0.0.1, Local port: 49152
Foreign host: 12.0.0.2, Foreign port: 179
Last Error: Code 0, SubCode 0.
```

Whenever a CEASE message is received from a peer, Automatic Stop event takes place. In response to this event, the Current Connect Retry Count is incremented, and the peer moves to its Idle State. It remains in the Idle State till the Idle Hold timer expires. After the timer expires, the peer begins to initiate the connection with its neighboring peer. Whenever a CEASE message is received, the Error Code becomes 6.

To simulate and verify this scenario, we need to enter manually the following commands:

4. At R2:

FOR EXAMPLE: Execute the following commands:

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enable BGP in R2.

```
iS5comm(config)# router bgp 100
```

– Shutdown the neighbor R1 from R2

```
iS5comm(config)# no neighbor 12.0.0.1 remote-as 100
```

– Configure the neighbor R1 from R2

```
iS5comm(config)#neighbor 12.0.0.1 remote-as 100
```

– At R1, view the bgp summary information immediately at R1 using 'show ip bgp summary'

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor VersionAS MsgRcvd MsgSent Up/DownState/PfxRcd
-------- --------- -------------------------------
12.0.0.2 4      100  0      0        -Idle

iS5comm# show ip bgp neighbor
BGP router identifier is 12.0.0.1, local AS number 100
BGP neighbor is 12.0.0.2, remote AS 100, internal link
BGP version 0, remote router ID 0.0.0.0
BGP state = Idle
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
AutomaticStop ENABLED
DampPeer Oscillations ENABLED
Configured Connect Retry Count 1
Current Connect Retry Count 1
Peer Status : NOT DAMPED
Idlehold time is 20 Rcvd update before 0 secs, hold time is 90,
keepalive interval is 30 secs
Received 0 messages, 0 Updates
Sent 0 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 0.0.0.0, Local port: 0
Foreign host: 12.0.0.2, Foreign port: 0
```

```
Last Error: Code 6, SubCode 0.
```

Now after the Idle Hold Timer expires for the peer R1, it begins to initiate the connection again with its neighbor R2.

– Verify that the BGP session between the internal peers R1 and R2 is established, after the idle hold timer expires in peer R1, using the following show commands in R1 and R2.

R1: View the bgp summary information using 'show ip bgp summary'

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version ASMsgRcvd MsgSent Up/DownState/PfxRcd
-------- ---------------------- ------------------
12.0.0.2 4      100  6      6       00:00:00:0 Established

iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 2 minutes 12 seconds
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
AutomaticStop ENABLED
DampPeer Oscillations ENABLED
Configured Connect Retry Count 1
Current Connect Retry Count 1
Peer Status : NOT DAMPED
Idlehold time is 20 Rcvd update before 0 secs, hold time is 90,
keepalive interval is 30 secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 6 messages, 0 Updates
Sent 6 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 2 time(s)
Local host: 12.0.0.1, Local port: 49152
Foreign host: 12.0.0.2, Foreign port: 179
Last Error: Code 6, SubCode 0.
```

R2: View the bgp summary information using 'show ip bgp summary'

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.2, local AS number 100
```

```
BGP table version is 0
Neighbor Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
-------------------------------- -------------------
12.0.0.1  4     100  8      8       00:00:00:0 Established

iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.1
BGP state = Established, up for 3 minutes 34 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 8 messages, 0 Updates
Sent 8 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 12.0.0.2, Local port: 179
Foreign host: 12.0.0.1, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

Whenever a CEASE message is received from a peer, Automatic Stop event takes place. In response to this event, the Current Connect Retry Count is incremented, and the peer moves to its Idle State. If the 'Current Connect Retry Count' is greater than the 'Configured Connect Retry Count', the peer status moves to 'DAMPED' state (if the Damp Peer Oscillations Flag is Enabled) and the Idle Hold Timer value is doubled internally.

The peer remains in the DAMPED state till the Idle Hold Timer value expires. Once this Idle Hold Timer expires, the peer status changes to 'NOT DAMPED' and proceeds to initiate the connection.

So after the 'Current Connect Retry Count ' exceeds the 'Configured Connect Retry Count', for each alternative Automatic Stop and Automatic Start events, the Idle Hold Timer value is doubled internally, and it keeps on increasing.

Whenever the Idle Hold Time value exceeds its maximum Threshold limit (32768), the peer moves to the Idle State and remains in the same, or until a manual start is issued by the administrator.

To simulate and verify the above-mentioned scenario, enter the following commands.

At R2,

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enable BGP in R2.

```
iS5comm(config)# router bgp 100
```

– Shutdown the neighbor R1 from R2.

```
iS5comm(config)# no neighbor 12.0.0.1 remote-as 100
```

– Configure the neighbor R1 from R2.

```
iS5comm(config)#neighbor 12.0.0.1 remote-as 100
```

R1: view the bgp summary information immediately at R1 using 'show ip bgp summary'

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
------------------------------ ------------------
12.0.0.2  4     100  0      0        - Idle
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 100, internal link
BGP version 0, remote router ID 0.0.0.0
BGP state = Idle
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
AutomaticStop ENABLED
DampPeer Oscillations ENABLED
Configured Connect Retry Count 1
Current Connect Retry Count 2
Peer Status : DAMPED
Idlehold time is 20 Rcvd update before 0 secs, hold time is 90,
keepalive interval is 30 secs
Received 0 messages, 0 Updates
Sent 0 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 2 time(s)
Local host: 0.0.0.0, Local port: 0
Foreign host: 12.0.0.2, Foreign port: 0
Last Error: Code 6, SubCode 0.
```

We can see that the peer status is changed to DAMPED. The Idle Hold Timer value is increased from 20 seconds to 40 seconds internally (not displayed in the neighbor information) and the peer remains in the Idle State till this timer expires. On the expiry of the Idle Hold Timer, the peer status is changed to NOT DAMPED and the peer begins to initiate the connection with its neighbor.

R1: After the Idle Hold Timer expires, view the bgp summary information at R1 using 'show ip bgp summary'

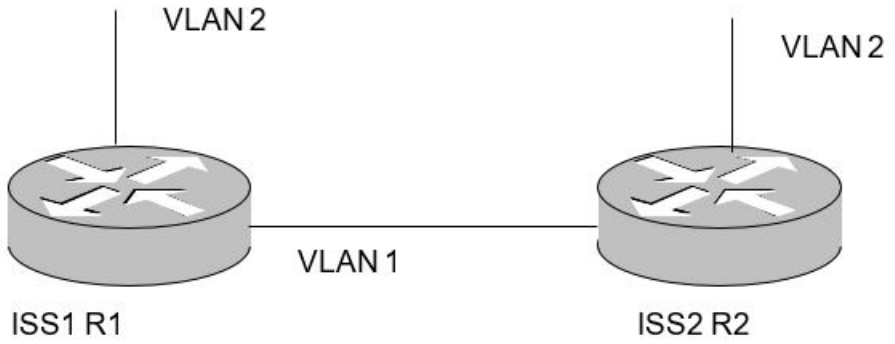
```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
------------------------------- -------------------
12.0.0.1   4    100  10      8   00:00:00:0 Established
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 5 minutes 20 seconds
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
AutomaticStop ENABLED
DampPeer Oscillations ENABLED
Configured Connect Retry Count 1
Current Connect Retry Count 2
Peer Status : NOT DAMPED
Idlehold time is 20
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 12 messages, 0 Updates
Sent 12 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 3 time(s)
Local host: 12.0.0.1, Local port: 49152
Foreign host: 12.0.0.2, Foreign port: 179
Last Error: Code 6, SubCode 0.
```

3.8. BGP Route Redistribution – Internal Peers

CONTEXT:

The figure shown below depicts the topology setup used for this configuration.

Figure 9: BGP Configuration and Testing Topology



Use the following commands to configure *BGP* routing.

1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R2 (with as-num 100) as internal peer in R1.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 remote-as 100
   ```

2. To enable *BGP* in Router R2:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R2.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R2.

   ```
   iS5comm(config)# router-id 12.0.0.2
   ```

   – Enable *BGP* in R2.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R1 (with as-num 100) as internal peer in R2.

   ```
   iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100
   ```

3. Verify that the *BGP* session between the internal peers R1 and R2 is established, using the following show commands in R1 and R2.

   FOR EXAMPLE: Type the following:

   – R1: View the bgp summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
 ------------------------------ ----------------
12.0.0.2  4     100  2      2        00:00:00:23 Established

iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 100, external link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 3 minutes 11 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Idlehold time is 20 DelayOpen interval is 50 secs
Rcvd update before 0 secs, hold time is 120, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 8 messages, 0 Updates
Sent 8 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
Connections established 1 time(s)
Local host: 12.0.0.1, Local port: 179
Foreign host: 12.0.0.2, Foreign port: 49152
Last Error: Code 0, SubCode 0
```

   – R2: View the BGP summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.2, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
-------- ------- ---- -------------- ----------------
```

```
12.0.0.1    4    100   2      2   00:00:00:6 Established
```

– View the peer details for the neighbor.

```
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.1
BGP state = Established, up for 31 minutes 38 seconds
Configured BGP Maximum Prefix Limit 100
AutomaticStart ENABLED
DelayOpen ENABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Idlehold time is 20 DelayOpen interval is 60 secs
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Received 63 messages, 0 Updates
Sent 63 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 12.0.0.2, Local port: 179
Foreign host: 12.0.0.1, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

– Add static route in R1:

```
iS5comm# configure terminal
iS5comm(config)# ip route 91.0.0.0 255.0.0.0 20.0.0.2
iS5comm(config)# exit
iS5comm# show ip route
C 12.0.0.0/8 is directly connected, vlan1
C 20.0.0.0/8 is directly connected, vlan2
S 91.0.0.0/8 [-1] via 20.0.0.2
```

– In R1, redistribute the static route into *BGP*.

```
iS5comm# configure terminal
iS5comm(config)# router bgp 100
iS5comm(config-router)# redistribute static
iS5comm(config-router)# end
```

– Verify the *BGP* route in R2.

```
iS5comm# show ip bgp rib
BGP table version is 1,local router ID is 12.0.0.2
Status codes: d damped* valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Path
------- ---- --- ------------ ----
*>i   91.0.0.0/8 12.0.0.1 100   ?
```

– iS5comm# show ip route

```
C 12.0.0.0/8 is directly connected, vlan1B 91.0.0.0/8 [-1] via 12.0.0.1
```

– Delete the static route in R1.

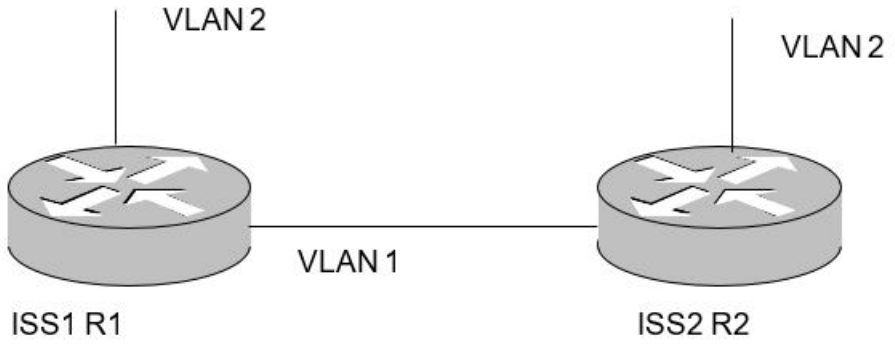
```
iS5comm# configure terminal
iS5comm(config)# no ip route 91.0.0.0 255.0.0.0 20.0.0.2
iS5comm(config)# end

iS5comm# show ip route
C 12.0.0.0/8 is directly connected, vlan1
C 20.0.0.0/8 is directly connected, vlan2
In R2 verify that BGP route is not present after deletion of the static
route in R1

iS5comm# show ip bgp rib
BGP table version is 0, local router ID is 0.0.0.0
Status codes: d damped * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
 Network Next Hop Metric LocPrf Path
------- ---- --- ------ ------ ----

iS5comm# show ip route
C 12.0.0.0/8 is directly connected, vlan1
```

3.9. BGP Route Redistribution feature – External Peers

CONTEXT:

The figure shown below depicts the topology setup used for this configuration.

Figure 10: BGP Configuration and Testing Topology



Use the following commands to configure *BGP* routing.

1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R2 (with as-num 200) as external peer in R1.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 remote-as 200
   ```

2. To enable *BGP* in Router R2:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R2.

   ```
   iS5comm(config)# as-num 200
   ```

   – Configure the router-id in R2.

   ```
   iS5comm(config)# router-id 12.0.0.2
   ```

   – Enable *BGP* in R2.

   ```
   iS5comm(config)# router bgp 200
   ```

   – Configure R1 (with as-num 100) as external peer in R2.

   ```
   iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100
   ```

3. Verify that the *BGP* session between the internal peers R1 and R2 is established, using the following show commands in R1 and R2.

   FOR EXAMPLE: Type the following:

   – R1: View the *BGP* summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvdMsgSent Up/DownState/PfxRcd
 ------------------------------- ----------------
12.0.0.2  4     200  2      2        00:00:00:13 Established
```

   – R2: View the BGP summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.2, local AS number 200
BGP table version is 0
Neighbor Version AS MsgRcvdMsgSent Up/DownState/PfxRcd
 ------------------------------- ----------------
12.0.0.1  4     100  2      2        00:00:00:1 Established
```

   – Add static route in R1:

```
iS5comm# configure terminal
iS5comm(config)# ip route 92.0.0.0 255.0.0.0 20.0.0.1
iS5comm(config)# exit
iS5comm# show ip route
C 12.0.0.0/8 is directly connected, vlan1
C 20.0.0.0/8 is directly connected, vlan2
S 91.0.0.0/8 [-1] via 20.0.0.1
```

   – In R1, redistribute the static route into *BGP*:

```
iS5comm# configure terminal
iS5comm(config)# router bgp 100
iS5comm(config-router)# redistribute static
iS5comm(config-router)# end
```

   – Verify the BGP route in R2

```
iS5comm# show ip bgp rib
BGP table version is 1,local router ID is 12.0.0.2
Status codes: d damped* valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Network Next Hop Metric LocPrf Path
------- ---- --- ------------ ----
*>i  91.0.0.0/8 12.0.0.1 100 ?
```

– iS5comm# show ip route

```
C 12.0.0.0/8 is directly connected, vlan1B 91.0.0.0/8 [-1] via 12.0.0.1
```

– Delete the static route in R1.

```
iS5comm# configure terminal
iS5comm(config)# no ip route 92.0.0.0 255.0.0.0 20.0.0.1
iS5comm(config)# end

iS5comm# show ip route
C 12.0.0.0/8 is directly connected, vlan1
C 20.0.0.0/8 is directly connected, vlan2
```

In R2 verify that BGP route is not present after deletion of the static route in R1.

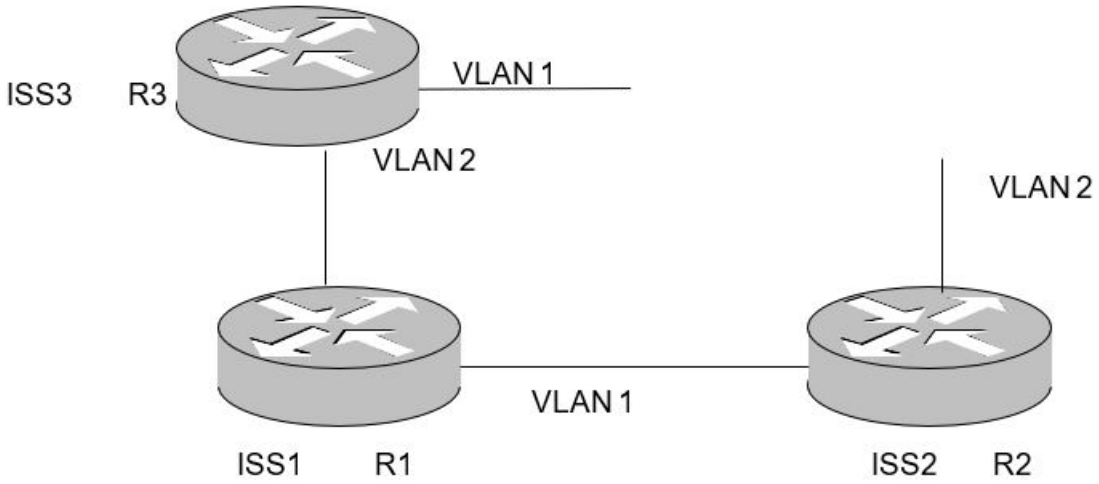
```
iS5comm# show ip bgp rib
BGP table version is 0, local router ID is 0.0.0.0
Status codes: d damped * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
 Network Next Hop Metric LocPrf Path
------- ---- --- ------ ------ ----

iS5comm# show ip route
C 12.0.0.0/8 is directly connected, vlan1
```

3.10. BGP Internal Route Redistribution to other IGPs

CONTEXT:

The figure shown below depicts the topology setup used for this configuration.

Figure 11: BGP Configuration and Testing Topology for BGP Internal route redistribution



Use the following commands to configure *BGP* routing.

1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R2 (with as-num 200) as external peer in R1.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 remote-as 100
   ```

2. To enable *BGP* in Router R2:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R2.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R2.

   ```
   iS5comm(config)# router-id 12.0.0.2
   ```

   – Enable *BGP* in R2.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R1 (with as-num 100) as internal peer in R2.

   ```
   iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100
   ```

3. Verify that the *BGP* session between the internal peers R1 and R2 is established, using the following show commands in R1 and R2.

   FOR EXAMPLE: Type the following:

   – R1: View the *BGP* summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvdMsgSent Up/DownState/PfxRcd
 ------------------------------- ----------------
12.0.0.2  4     200  2      2        00:00:00:23 Established

iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 3 minutes 11 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 120, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 8 messages, 0 Updates
Sent 8 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
Connections established 1 time(s)
Local host: 12.0.0.1, Local port: 179
Foreign host: 12.0.0.2, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

   – R2: View the BGP summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.2, local AS number 200
BGP table version is 0
Neighbor Version AS MsgRcvdMsgSent Up/DownState/PfxRcd
 ------------------------------- ----------------
```

```
12.0.0.1  4     100  2      2        00:00:00:6 Established

iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.1
BGP state = Established, up for 3 minutes 55 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 120, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 9 messages, 0 Updates
Sent 9 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
Connections established 1 time(s)
Local host: 12.0.0.2, Local port: 49152
Foreign host: 12.0.0.1, Foreign port: 179
Last Error: Code 0, SubCode 0.
```

– Add static route in R2:

```
iS5comm# configure terminal
iS5comm(config)# ip route 91.0.0.0 255.0.0.0 90.0.0.3
iS5comm(config)# exit
iS5comm# show ip route
C 12.0.0.0/8 is directly connected, vlan1
C 90.0.0.0/8 is directly connected, vlan2
S 91.0.0.0/8 [-1] via 90.0.0.3
```

– In R2, redistribute the static route into *BGP*:

```
iS5comm# configure terminal
iS5comm(config)# router bgp 100
iS5comm(config-router)# redistribute static
iS5comm(config-router)# end
```

– Verify the *BGP* route in R2

```
iS5comm# show ip bgp rib
BGP table version is 1,local router ID is 12.0.0.1
Status codes: d damped* valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Path
------- ---- --- ------------ ----
*>i   91.0.0.0/8 12.0.0.1 100   ?
```

– iS5comm# show ip route

```
C 12.0.0.0/8 is directly connected, vlan1B 91.0.0.0/8 [-1] via 12.0.0.1
```

4. Execute the following commands to configure *RIP* routing:

FOR EXAMPLE: Execute the following commands:

To enable *RIP* in Router R1, perform the following.

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enable *RIP* globally in R1.

```
iS5comm(config)# router rip
```

– Enable *RIP* over the interface vlan 2 (IP address 20.0.0.1).

```
iS5comm(config-router)# neighbor 12.0.0.2 remote-as 100
```

To enable *RIP* in Router R3, perform the following:

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enable *RIP* globally in R3.

```
iS5comm(config)# router rip
```

– Enable *RIP* over the interface vlan 2 (IP address 20.0.0.3).

```
iS5comm(config-router)# network 20.0.0.3
```

5. Verify the ip route in R3.

FOR EXAMPLE: Execute the following commands:

```
iS5comm# show ip route
Codes: C - connected, S - static, R - rip, B - bgp, O - ospf
Vrf Name:          default
---------
C 12.0.0.0/8  is directly connected, vlan1
C 20.0.0.0/8  is directly connected, vlan2
```

6. Configure to redistribute internal *BGP* routes to other *IGP* protocols such as *RIP* in R1.

   FOR EXAMPLE: Execute the following commands:

```
iS5comm# configure terminal
iS5comm(config)# router bgp 100
iS5comm(config-router)# bgp redistribute-internal
iS5comm(config-router)# end
```

   – In R1, redistribute the static route into *BGP*:

```
iS5comm# configure terminal
iS5comm(config)# router bgp 100
iS5comm(config-router)# redistribute bgp
iS5comm(config-router)# end
```

7. Verify the ip route in R3.

   FOR EXAMPLE: Execute the following commands:

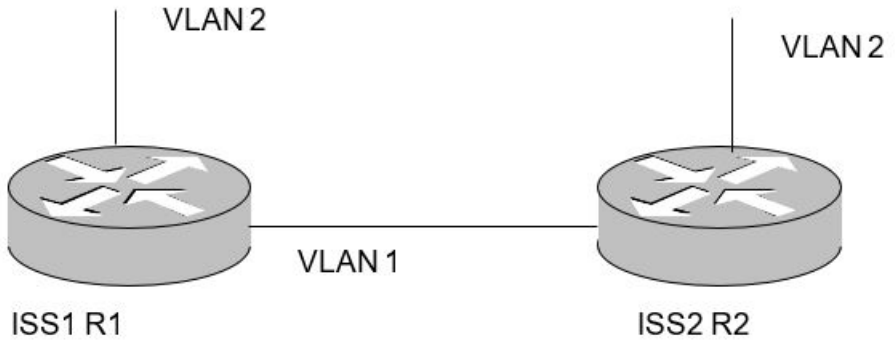
```
iS5comm# show ip route
Codes: C - connected, S - static, R - rip, B - bgp, O - ospf
Vrf Name:          default
---------
C 12.0.0.0/8  is directly connected, vlan1
C 20.0.0.0/8  is directly connected, vlan2
R 91.0.0.0/8  [4] via 20.0.0.1
```

3.11. BGP Prefix Upper Limit Feature – Internal Peers

CONTEXT:

The figure shown below depicts the topology setup used for this configuration.

Figure 12: BGP Configuration and Testing Topology



Use the following commands to configure *BGP* routing.

1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R2 (with as-num 100) as internal peer in R1.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 remote-as 100
   ```

   – Configure the prefix upper limit as 4 for the peer R1. It denotes the number of address prefixes the speaker is willing to accept from its neighbor.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 maximum-prefix 4
   ```

2. To enable *BGP* in Router R2:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R2.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R2.

   ```
   iS5comm(config)# router-id 12.0.0.2
   ```

   – Enable *BGP* in R2.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R1 (with as-num 100) as internal peer in R2.

```
iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100
```

3. Verify that the *BGP* session between the internal peers R1 and R2 is established, using the following show commands in R1 and R2.

   FOR EXAMPLE: Type the following:

   – R1: View the bgp summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 4
Neighbor Version AS MsgRcvdMsgSent Up/DownState/PfxRcd
 ------------------------------- ----------------
12.0.0.2  4     100 29     28        00:00:10:30 Established

iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 14 minutes 7 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 4
Current Connect Retry Count 5
Peer Status : NOT DAMPED
Idlehold time is 20 DelayOpen interval is 50 secs
Rcvd update before 0 secs, hold time is 120, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 30 messages, 4 Updates
Sent 29 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
Connections established 1 time(s)
Local host: 12.0.0.1, Local port: 179
Foreign host: 12.0.0.2, Foreign port: 49152
Last Error: Code 0, SubCode 0
```

   – **R2:** View the *BGP* summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.2, local AS number 100
BGP table version is 0
```

```
Neighbor Version ASMsgRcvd MsgSent Up/DownState/PfxRcd
 -------- ------- ---- -------------- ----------------
12.0.0.1  4     100  31    32        00:00:00:6 Established

iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.1
BGP state = Established, up for 15 minutes 53 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 31 messages, 0 Updates
Sent 32 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 12.0.0.2, Local port: 49152
Foreign host: 12.0.0.1, Foreign port: 179
Last Error: Code 0, SubCode 0.
```

– Add static route in R2.

```
iS5comm# configure terminal
iS5comm(config)# ip route 15.0.0.0255.0.0.0 90.0.0.0
iS5comm(config)# ip route 16.0.0.0255.0.0.0 90.0.0.0
iS5comm(config)# ip route 17.0.0.0255.0.0.0 90.0.0.0
iS5comm(config)# ip route 18.0.0.0255.0.0.0 90.0.0.0
iS5comm(config)# ip route 19.0.0.0255.0.0.0 90.0.0.0
iS5comm(config)# ip route 29.0.0.0255.0.0.0 90.0.0.0
iS5comm(config)# exit
iS5comm# show ip route
C 12.0.0.0/8 is directly connected, vlan1
C 90.0.0.0/8 is directly connected, vlan2
S 15.0.0.0/8 [-1] via 90.0.0.0
S 16.0.0.0/8[-1] via 90.0.0.0
```

```
S 17.0.0.0/8[-1] via 90.0.0.0
S 18.0.0.0/8[-1] via 90.0.0.0
S 19.0.0.0/8[-1] via 90.0.0.0
S 29.0.0.0/8[-1] via 90.0.0.0
```

– In R2, redistribute the static route into *BGP*.

```
iS5comm# configure terminal
iS5comm(config)# router bgp 100
iS5comm(config-router)# redistribute static
iS5comm(config-router)# end
```

– Verify the *BGP* route in R2.

```
iS5comm# show ip bgp rib
BGP table version is 4,local router ID is 12.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete
 Type Network NextHop Metric LocPrf Path Origin
------------------------ ------ ---- ------
* i 15.0.0.0/890.0.0.0/4100-?
* i 16.0.0.0/890.0.0.0/4100-?
* i 17.0.0.0/890.0.0.0/4100-?
* i 18.0.0.0/890.0.0.0/4100-?
```

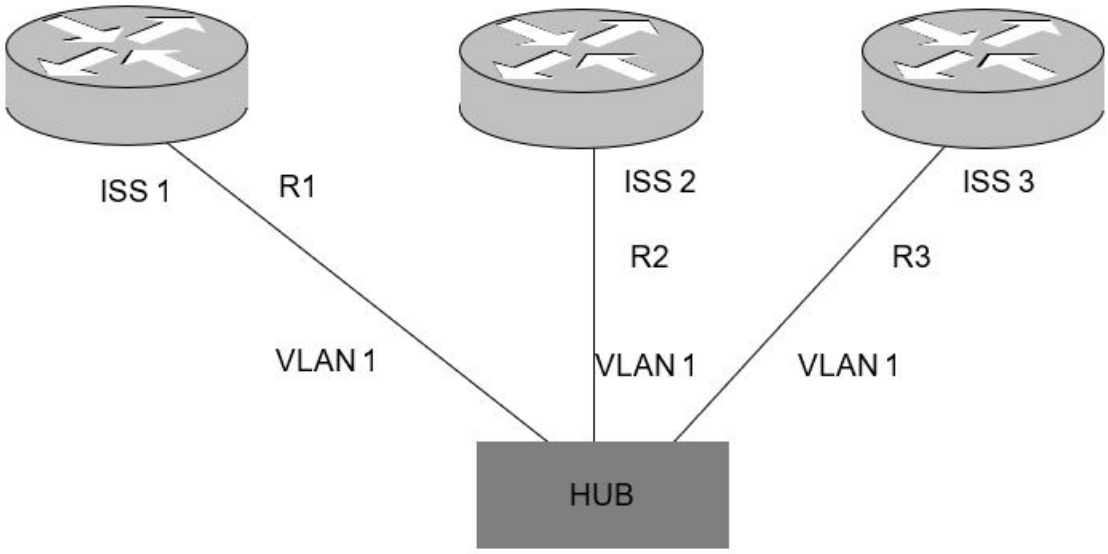
Since the Maximum Prefix Limit is configured as 4 in R1, it can take up to only 4 routes in its RIB. The remaining routes are discarded as expected.

3.12. BGP Local Preference

CONTEXT:

The figure shown below depicts the topology setup used for this configuration.

Figure 13: Configuration and Testing BGP Local Preference Value



Use the following commands to configure *BGP* routing.

1. To test the decision process using the LOCAL_PREF value when received from internal peers.

   FOR EXAMPLE: Type the following:

   – Configuration in R1.

```
iS5comm# configure terminal
iS5comm(config)# shutdown spanning-tree
iS5comm(config)# as-num 100
iS5comm(config)# router-id 10.0.0.1
iS5comm(config)# router bgp 100
iS5comm(config-router)# neigh 10.0.0.2 remote-as 100
iS5comm(config-router)# neigh 10.0.0.3 remote-as 100
iS5comm(config-router)# end
```

   – Configuration in R2.

```
iS5comm# configure terminal
iS5comm(config)# as-num 100
iS5comm(config)# router-id 10.0.0.2
iS5comm(config)# router bgp 100
iS5comm(config-router)# neighbor 10.0.0.1 remote-as 100
iS5comm(config-router)# neighbor 10.0.0.3 remote-as 100
iS5comm(config-router)# end
```

   – Configuration in R3.

```
iS5comm# configure terminal
```

```
iS5comm(config)# interface gigabit 0/2
iS5comm(config-if)# no shutdwon
iS5comm(config-if)# exit
iS5comm(config)# interface vlan 2
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 12.0.0.3 255.0.0.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 2
iS5comm(config-vlan)# ports gigabit 0/2
iS5comm(config-vlan)# exit
iS5comm(config)# sh sp
S5comm(config)# end
iS5comm# configure terminal
iS5comm(config)# as-num 100
iS5comm(config)# router-id 10.0.0.3
iS5comm(config)# router bgp 100
iS5comm(config-router)# neighbor 10.0.0.1 remote-as 100
iS5comm(config-router)# neighbor 10.0.0.2 remote-as 100
iS5comm(config-router)# end
```

2. R1: View the *BGP* summary information using 'show ip bgp summary'.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp summary
BGP router identifier is 10.0.0.1, local AS number 100B
GP table version is 0
Neighbor Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
------------------------------- ----------------
10.0.0.2 4      100 2       2      00:00:00:22 Established
10.0.0.3 4      100 2       2      00:00:00:5 Established
```

3. R2: View the *BGP* summary information using 'show ip bgp summary'.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp summary
BGP router identifier is 10.0.0.2, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
------------------------------- ----------------
10.0.0.1  4     100  2      2       00:00:00:29 Established
10.0.0.3  4     100  2      2       00:00:00:12 Established
```

4. R3: View the *BGP* summary information using 'show ip bgp summary'.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp summary
BGP router identifier is 10.0.0.3, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
-------------------------------- ----------------
10.0.0.1  4     100  2      2       00:00:00:16 Established
10.0.0.2  4     100  2      2       00:00:00:16 Established
```

5. R2 Configuration:

   FOR EXAMPLE: Type the following:

   – Add static route in R2.

```
iS5comm# configure terminal
iS5comm(config)# ip route 90.0.0.0 255.0.0.0 12.0.0.4
iS5comm# end
```

   – Configure the *BGP* local-preference for the static route 90.0.0.0 with next hop 12.0.0.4 as 150 and redistribute all routes into BGP.

```
iS5comm# configure terminal
iS5comm(config)# router bgp 100
iS5comm(config-router)# bgp local-preference 1 remote-as 100 90.0.0.0 8
value 150 direction out 0
```

   – View the BGP Local preference using 'show ip bgp local-perf' command.

```
iS5comm# show ip bgp local-pref
Index AdminRemote -ASPrefixPrefixLen Inter-AS Direction Value Preference
Status
----------- -------------- --------- ------- ----------- ----------
1     up          100 90.0.0.0 8            - out      150   false
```

   – Enable redistribution of all routes in R2.

```
iS5comm# configure terminal
iS5comm(config)# router bgp 100
iS5comm(config-router)# redistribute all
iS5comm(config-router)#end
```

6. R3 Configuration.

   FOR EXAMPLE: Type the following:

– Add static route in R3.

```
iS5comm# configure terminal
iS5comm(config)# ip route 90.0.0.0 255.0.0.0 12.0.0.4
iS5comm# end
```

– Configure the BGP local-preference for the static route 90.0.0.0 with next hop 12.0.0.4 as 250 and redistribute all routes into BGP.

```
iS5comm# configure terminal
iS5comm(config)# router bgp 100
iS5comm(config-router)# bgp local-preference 1 remote-as 100 90.0.0.0 8
value 250 direction out
```

– View the BGP Local preference using 'show ip bgp local-perf' command.

```
iS5comm# show ip bgp local-pref
Index AdminRemote -AS PrefixPrefixLen Inter-AS Direction Value
Preference Status
----------- --------------- --------- ------- ----------- ----------
1      up          100 0.0.0.0 8              - out      250    false
```

– Enable redistribution of all routes in R2.

```
iS5comm# configure terminal
iS5comm(config)# router bgp 100
iS5comm(config-router)# redistribute all
iS5comm(config-router)#end
```

7. Verify that route learned from R3 is selected as the best route in R1. Verify that route learned from R2 is not the best route in R1.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp rib
BGP table version is 6,local router ID is 10.0.0.1
Status codes: d damped* valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
NetworkNext Hop Metric LocPrf Path
------- ---- --- ------ ------ ----
*>i 10.0.0.0/8 10.0.0.20 100  i
* i 10.0.0.0/8 10.0.0.30 100 i
*>i 12.0.0.0/8 10.0.0.20 100 i
* i 12.0.0.0/8 10.0.0.30 100 i
```

```
*>i 90.0.0.0/8 10.0.0.3  250 ?
* i 90.0.0.0/8 10.0.0.2  150 ?
```

3.13. Configuring Peer TCP-MD5 Authentication Information

CONTEXT:

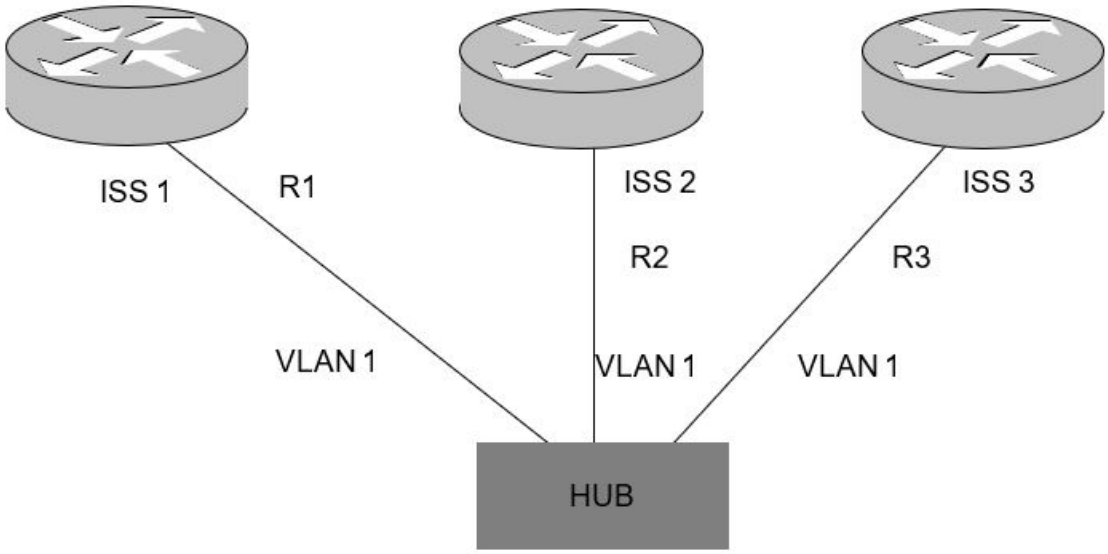
Configuration of *TCP MD5* authenticated *BGP* peering sessions is supported. With this configuration, it is possible to configure a unique password for a peer. The same password needs to be configured in the peer router before session establishment is initiated. Configuration of password for a peer causes ISS-TCP to generate a *MD5* signature of the outgoing segments and verify the signature in the incoming segments. Thus, the *BGP* peering session is protected with MD5 authentication using the configured password at the transport layer.

The password can be a string of alpha-numeric and special characters with the exception of the following special characters - ! , |, ? and ;.

The following steps explain how *TCP MD5* authenticated session can be configured between *BGP* peers.

The figure shown below depicts the topology setup used for this configuration.

Figure 14: Configuration and Testing BGP Local Preference Value



Use the following commands to configure *BGP* routing.

1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

```
iS5comm(config)# router-id 10.0.0.1
```

– Enable *BGP* in R1.

```
iS5comm(config)# router bgp 100
```

– Configure R2 (with as-num 100) as internal peer in R1.

```
iS5comm(config-router)# neighbor 10.0.0.2 remote-as 100
```

– Configure *TCP MD5* password for peer R2 in R1.

```
iS5comm(config-router)# neighbor 10.0.0.2 password secret123&*()
```

– Configure R3 (with as-num 100) as internal peer in R1.

```
iS5comm(config-router)# neighbor fec0::1111:0:3 remote-as 100
```

– Configure *TCP MD5* password for peer R3 in R1.

```
iS5comm(config-router)# neighbor fec0::1111:0:3 password
test98^%*+_675#{}
```

2. To enable *BGP* in Router R2:

FOR EXAMPLE: Execute the following commands:

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enter the Autonomous System (*AS*) number in R2.

```
iS5comm(config)# as-num 100
```

– Configure the router-id in R2.

```
iS5comm(config)# router-id 10.0.0.2
```

– Enable *BGP* in R2.

```
iS5comm(config)# router bgp 100
```

– Configure R1 (with as-num 100) as internal peer in R2.

```
iS5comm(config-router)# neighbor 10.0.0.1 remote-as 100
```

– Configure *TCP MD5* password for peer R1 in R2.

```
iS5comm(config-router)# neighbor 10.0.0.1 password secret123&*()
```

3. To enable *BGP* in Router R3:

FOR EXAMPLE: Execute the following commands:

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enter the Autonomous System (*AS*) number in R3.

```
iS5comm(config)# as-num 100
```

– Configure the router-id in R3.

```
iS5comm(config)# router-id 10.0.0.3
```

– Enable *BGP* in R3.

```
iS5comm(config)# router bgp 100
```

– Configure R1 (with as-num 100) as internal peer for R3.

```
iS5comm(config-router)# neighbor fec0::1111:0:1 remote-as 100
```

– Configure *TCP MD5* password for peer R1 in R3.

```
iS5comm(config-router)# neighbor fec0::1111:0:1 password
test98^%*+_675#{}
```

4. Verify that the *BGP* sessions between the peers R1, R2 and R1, R3 are established, using the following show commands in R1, R2, and R3.

FOR EXAMPLE: Type the following:

– R1: View the BGP session information using 'show ip bgp summary', 'show ip bgp neighbor' and 'show ip bgp info' commands.

```
iS5comm# show ip bgp summary
BGP router identifier is 10.0.0.1, local AS number 100
BGP table version is 0
Neighbor       Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
 ------------------------------- ----------------
10.0.0.2       4      100  4      4       00:00:00:0 Established
fec0::1111:0:3 4      100  2      2       00:00:00:0 Established

iS5comm# show ip bgp neighbor
BGP neighbor is 10.0.0.2, remote AS 100, external link
BGP version 4, remote router ID 10.0.0.2
BGP state = Established, up for 1 minute 49 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 2
Current Connect Retry Count 0
Peer Passive : DISABLED
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 5 messages, 0 Updates
Sent 5 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 10.0.0.1, Local port: 49152
Foreign host: 10.0.0.2, Foreign port: 179
Last Error: Code 0, SubCode 0.
```

```
iS5comm# show bgp ipv6 neighbor
BGP neighbor is fec0::1111:0:3, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.3
BGP state = Established, up for 2 minutes 6 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Passive : DISABLED
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 6 messages, 0 Updates
Sent 6 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 0.0.192.254, Local port: 49153
Foreign host: 0.0.192.254, Foreign port: 179
Last Error: Code 0, SubCode 0.

iS5comm# show ip bgp info
Routing Protocol is "bgp 100"
IGP synchronization is disabled
Both more-specific and less-specificoverlap route policy is set
Local Preference is 100
Non-bgp routes are advertised to bothexternal and internal peers
MED Comparision is disabled
Metric is 0
Default Originate Disable
Redistributing:
 BGP GR admin status is disabled

Peer Table
Peer Address RemoteAS NextHop MultiHop  send-community
------------ -------- ------- --------   --------------
10.0.0.2       100   automatic disablestandard,extended
```

```
fec0::1111:0:3 100   automatic disablestandard,extended
```

5. R2: View the *BGP* session information using 'show ip bgp summary', 'show ip bgp neighbor' and 'show ip bgp info' commands.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp summary
BGP router identifier is 10.0.0.2, local AS number 100
BGP table version is 0
Neighbor  Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
 ------------------------------- ----------------
10.0.0.1  4      100  6      6       00:00:00:0  Established

iS5comm# show ip bgp summary
BGP neighbor is 10.0.0.1, remote AS 100, internal link
BGP version 4, remote router ID 10.0.0.1
BGP state = Established, up for 2 minutes 27 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Passive : DISABLED
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 6 messages, 0 Updates
Sent 6 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 10.0.0.2, Local port: 179
Foreign host: 10.0.0.1, Foreign port: 49152
Last Error: Code 0, SubCode 0.

iS5comm# show ip bgp info
Routing Protocol is "bgp 100"
IGP synchronization is disabled
Both more-specific and less-specificoverlap route policy is set
Local Preference is 100
Non-bgp routes are advertised to bothexternal and internal peers
```

```
MED Comparision is disabled
Metric is 0
Default Originate Disable
Redistributing:
BGP GR admin status is disabled
Peer Table
Peer Address RemoteAS NextHopMultiHop send-community
---- ------- -------- ------- -------- --------------
10.0.0.1 100 automatic disablestandard,extended
```

6. R3: View the *BGP* session information using 'show ip bgp summary', 'show ip bgp neighbor' and 'show ip bgp info' commands.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp summary
BGP router identifier is 10.0.0.3, local AS number 100
BGP table version is 0
Neighbor       Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
 ------------------------------- ----------------
fec0::1111:0:1 4      100 10      10     00:00:00:0 Established


iS5comm# show ip bgp summary
BGP neighbor is fec0::1111:0:1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.1
BGP state = Established, up for 4 minutes 23 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Passive : DISABLED
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 10 messages, 0 Updates
Sent 10 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 0.0.192.254, Local port: 179
```

```
Foreign host: 0.0.192.254, Foreign port: 49152
Last Error: Code 0, SubCode 0.

iS5comm# show ip bgp info
Routing Protocol is "bgp 100"
IGP synchronization is disabled
Both more-specific and less-specificoverlap route policy is set
Local Preference is 100
Non-bgp routes are advertised to bothexternal and internal peers
MED Comparision is disabled
Metric is 0
Default Originate Disable
Redistributing:
BGP GR admin status is disabled
Peer Table
Peer Address   RemoteAS NextHopMultiHop send-community
---- -------   -------- ------- -------- --------------
fec0::1111:0:1 100      automatic disablestandard,extended
```

7. To remove the configured peer password, perform the following steps in CLI:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Remove *TCP MD5* password configured for peer R2 in R1.

   ```
   iS5comm(config-router)# no neighbor 10.0.0.2 password
   ```

   – Remove *TCP MD5* password configured for peer R3 in R1.

   ```
   iS5comm(config-router)# no neighbor fec0::1111:0:3 password
   ```

3.14. Configuring Route Map for Neighbors

CONTEXT:

Route maps are used to control and modify routing information that is exchanged between routing domains. Route maps consist of a list of match and set configuration commands. The match commands specify match criteria and the set commands specify the action taken if the match criteria are met.

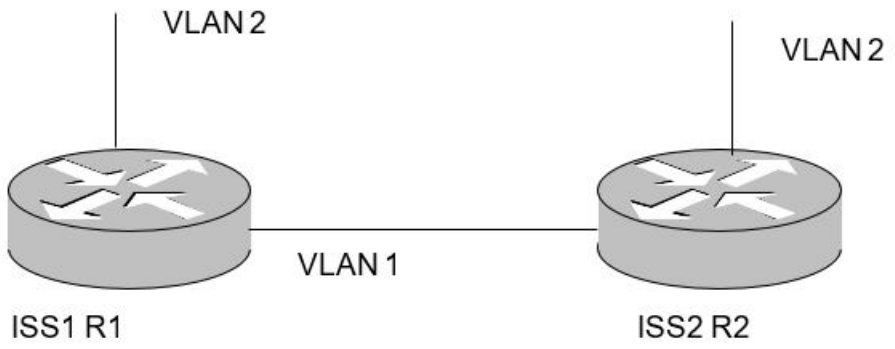
When applied to incoming or outgoing routes, route map provides the control on the distribution of routes between two *BGP* peers.

When configuring “In direction Routemap for the Neighbor”, the route map will be applied on the routes coming from that Neighbor before installing to the local *RIB*.

When configuring “Out direction Routemap for the Neighbor”, the route map will be applied on the routes advertised to that neighbor.

The figure shown below depicts the topology setup used for this configuration.

Figure 15: BGP Configuration and Testing Topology



Use the following commands to configure *BGP* routing.

1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R2 (with as-num 100) as internal peer in R1.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 remote-as 100
   ```

   – Configure Out Direction Route Map for the peer R2.

   ```
   iS5comm(config-router)# neighbor 10.0.0.2 route-map RMAP out
   ```

   – Configure In Direction Route Map for the peer R2.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 route-map INRMAP in
   ```

   – Create Route map RMAP.

   ```
   iS5comm(config)# route-map  RMAP permit 10
   ```

   – Match destination ip 16.0.0.0 /8

   ```
   iS5comm(config-rmap-RMAP)# match destination ip 16.0.0.0 255.0.0.0
   ```

– Set local preference.

```
iS5comm(config-rmap-RMAP)# set local-preference 150
```

– Create Route map INRMAP. local preference.

```
iS5comm(config)# route-map INRMAP permit 10
```

– Match destination IP 17.0.0.0 /8

```
iS5comm(config-rmap-RMAP)# match destination ip 17.0.0.0 255.0.0.0
```

– Set local preference

```
iS5comm(config-rmap-RMAP)# set local-preference 125
```

2. To enable *BGP* in Router R2:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

   – Enter the Autonomous System (*AS*) number in R2.

```
iS5comm(config)# as-num 100
```

   – Configure the router-id in R2.

```
iS5comm(config)# router-id 12.0.0.2
```

   – Enable *BGP* in R2.

```
iS5comm(config)# router bgp 100
```

   – Configure R1 (with as-num 100) as internal peer in R2.

```
iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100
```

3. R1: Add static route 16.0.0.0/8.
4. R2: Add static route 17.0.0.0/8 and verify the results.

   FOR EXAMPLE: Type the following:

   – R1:

```
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 100, external link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 2 minutes 43 seconds, un-authenticated
session
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Passive : DISABLED
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
```

```
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 7 messages, 0 Updates
Sent 7 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 12.0.0.1, Local port: 179
Foreign host: 12.0.0.2, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

5. R2: View the *BGP* session information using 'show ip bgp summary', 'show ip bgp neighbor' and 'show ip bgp info' commands.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp summary
BGP router identifier is 10.0.0.2, local AS number 100
BGP table version is 0
Neighbor  Version AS MsgRcvd MsgSent Up/DownState/PfxRcd
 ------------------------------- ----------------
10.0.0.1  4      100  6      6       00:00:00:0  Established

iS5comm# show ip bgp summary
BGP neighbor is 10.0.0.1, remote AS 100, internal link
BGP version 4, remote router ID 10.0.0.1
BGP state = Established, up for 2 minutes 27 seconds
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Passive : DISABLED
Peer Status : NOT DAMPED
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 6 messages, 0 Updates
Sent 6 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
```

```
Local host: 10.0.0.2, Local port: 179
Foreign host: 10.0.0.1, Foreign port: 49152
Last Error: Code 0, SubCode 0.

iS5comm# show ip bgp bgp
BGP table version is 3,local router ID is 12.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 S Stale
 Origin codes: i - IGP, e - EGP, ? - incomplete

 Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------
 >           12.0.0.0/ 8         0.0.0.0       0       0     -     i
 >           16.0.0.0/ 8         0.0.0.0               0     -     ?
 >i          17.0.0.0/ 8        12.0.0.2             125     -     ?
```

– R2:

```
iS5comm# show ip bgp bgp
BGP table version is 3,local router ID is 12.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Type   Network NextHop   Metric LocPrf Path  Origin
-----  ------ ------  ------  ----  ------
>    12.0.0.0/ 8  0.0.0.0   0      0     -      i
>i   16.0.0.0/ 8  12.0.0.1  150           -     ?
>    17.0.0.0/ 8  0.0.0.0    0            -     ?
```

3.15. Configuring Peer Groups

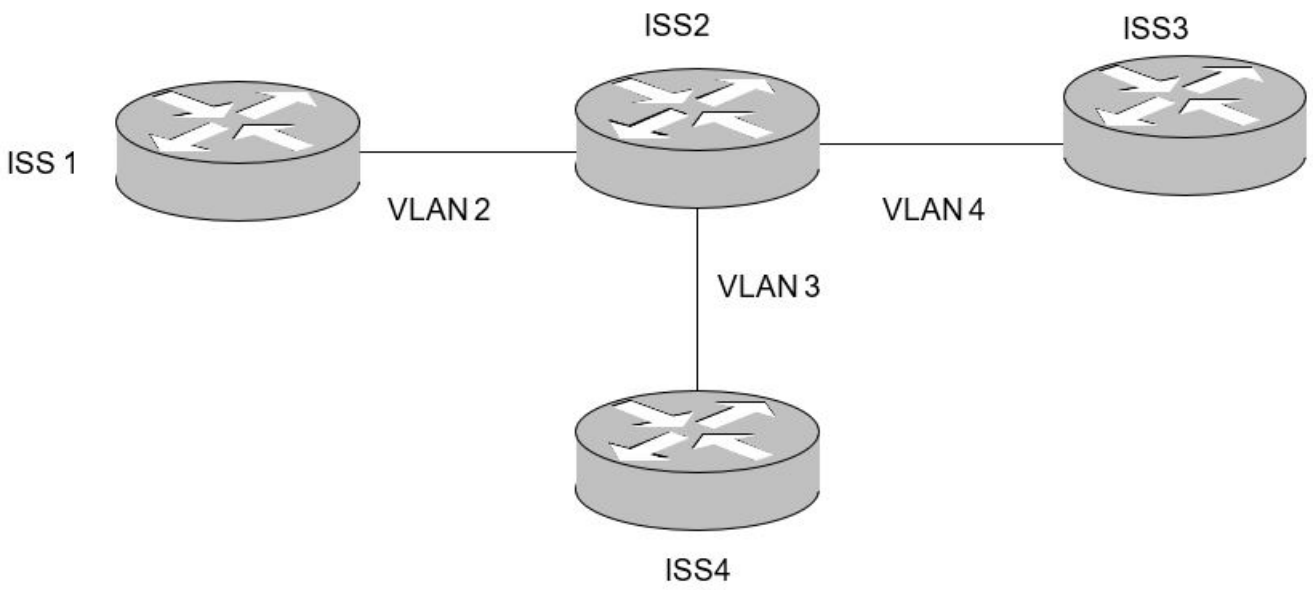
CONTEXT:

BGP peer group reduces the amount of system resources (*CPU* and memory) necessary in an update generation. In addition, a *BGP* peer group also simplifies the *BGP* configuration of peers. It is recommended that administrator group together neighbors with identical outbound announcement policies.

Neighbors configured in different address-families could not belong to the same peer group. Neighbors configured in the same autonomous system and in different autonomous system could not belong to the same peer group.

The figure shown below depicts the topology setup used for this configuration.

Figure 16: Configuration and Testing BGP Peer Groups



Use the following commands to configure *BGP* routing.

1. Execute the following commands to configure *BGP* Peer group.

   FOR EXAMPLE: Perform the following:

   Configure Peer Group in Router ISS

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure an internal peer group pgrp1 in R2.

   ```
   iS5comm(config-router)# neighbor pgrp1 peer-group
   iS5comm(config-router)# neighbor pgrp1 remote-as 100
   ```

   – Configure maximum prefix limit for peer group.

   ```
   iS5comm(config-router)# neighbor pgrp1 maximum-prefix 125
   ```

   – Configure keep alive time for peer group.

   ```
   iS5comm(config-router)# neighbor pgrp1 timers keepalive 35
   ```

   – Configure peer group as passive.

   ```
   iS5comm(config-router)# neighbor pgrp1 transport connection-mode passive
   ```

   – Configure advertisement interval for the peer group.

   ```
   iS5comm(config-router)# neighbor pgrp1 advertisement-interval 15
   ```

   – Configure dampening for the peer group

   ```
   iS5comm(config-router)# neighbor pgrp1damp-peer-oscillations
   ```

   – Configure route reflection for the peer group.

```
iS5comm(config-router)# neighbor pgrp1route-reflector-client
```

– Configure ISS1, ISS3, ISS4 as internal peer of ISS2.

```
iS5comm(config-router)# neighbor 14.0.0.1 peer-group pgrp1
iS5comm(config-router)# neighbor 15.0.0.2 peer-group pgrp1
iS5comm(config-router)# neighbor 16.0.0.2 peer-group pgrp1
```

2. To configure internal *BGP* sessions:

FOR EXAMPLE: Execute the following commands:

Configure internal BGP session inISS1

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enable *BGP* in ISS1.

```
iS5comm(config)# router bgp 100
```

– Configure an internal BGP session with ISS2.

```
iS5comm(config-router)# neighbor 14.0.0.2 remote-as 100
```

Configure internal BGP session in ISS3

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enable *BGP* in ISS3.

```
iS5comm(config)# router bgp 100
```

– Configure an internal *BGP* session with ISS2.

```
iS5comm(config-router)# neighbor 15.0.0.1 remote-as 100
```

Configure internal BGP session in ISS4

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enable *BGP* in ISS4.

```
iS5comm(config)# router bgp 100
```

– Configure an internal BGP session with ISS2.

```
iS5comm(config-router)# neighbor 16.0.0.1 remote-as 100
```

3. ISS2: View the *BGP* peer group configurations.

FOR EXAMPLE: Type the following:

– R1: View the bgp summary information.

```
iS5comm# show ip bgp peer-group
BGP peer-group is pgrp1, Remote AS 100
 BGP Version 0
```

```
 For address family: IPv4 Unicast
 BGP neighbor is pgrp1,peer-group internal, members:
14.0.0.115.0.0.216.0.0.2
BGP Maximum Prefix Limit: 125
Connect Retry Count: 5
 Peer Passive :Enabled
 Damp Peer oscillatios:Enabled
 Rfl Status :Client
 In Route Map: -
 Out Route Map: -
```

4. ISS2: View the *BGP* summary information using 'show ip bgp summary'.

   FOR EXAMPLE: Type the following:

   – R1: View the bgp summary information.

```
iS5comm# show ip bgp summary
BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor Version AS MsgRcvd  MsgSent Up/Down State/PfxRcd
-------- ------- -- -------  ------- ------- ------------
14.0.0.1   4    100   5         5   00:00:1:48 Established
15.0.0.2   4    100   5         5   00:00:1:48 Established
16.0.0.2   4    100   4         4   00:00:1:21 Established
```

5. ISS2: View the BGP neighbor configurations.

   FOR EXAMPLE: Type the following:

   – R1: View the bgp summary information.

```
iS5comm# show ip bgp neighbor
BGP neighbor is 14.0.0.1, remote AS 100, internal link
BGP version 4, remote router ID 14.0.0.1
BGP state = Established, up for 1 minute 56 seconds, un-authenticated
session
 Configured BGP Maximum Prefix Limit 125
 DampPeer Oscillations ENABLED
 Configured Connect Retry Count 5
 Current Connect Retry Count 0
 Peer Passive : ENABLED
 Peer Status : NOT DAMPED
 Idlehold time is 60   Rcvd update before 0 secs, hold time is 90,
keepalive interval is 35 secs
 Neighbors Capability:
```

```
 Route-Refresh: Advertised and received
 Address family IPv4 Unicast: Advertised and received
 Received 5 messages, 0 Updates
 Sent 5 messages, 0 Updates
 Route refresh: Received 0, sent 0.
 Minimum time between advertisement runs is 15 seconds
 Connections established 2 time(s)
 Local host: 14.0.0.2, Local port: 179
 Foreign host: 14.0.0.1, Foreign port: 49153
 Last Error: Code 0, SubCode 0.

BGP neighbor is 15.0.0.2, remote AS 100, internal link
 BGP version 4, remote router ID 15.0.0.2
BGP state = Established, up for 1 minute 56 seconds, un-authenticated
session
 Configured BGP Maximum Prefix Limit 125
 DampPeer Oscillations ENABLED
 Configured Connect Retry Count 5
 Current Connect Retry Count 0
 Peer Passive : ENABLED
 Peer Status : NOT DAMPED
Idlehold time is 60   Rcvd update before 0 secs, hold time is 90,
keepalive interval is 35 secs
 Neighbors Capability:
 Route-Refresh: Advertised and received
 Address family IPv4 Unicast: Advertised and received
 Received 5 messages, 0 Updates
 Sent 5 messages, 0 Updates
 Route refresh: Received 0, sent 0.
 Minimum time between advertisement runs is 15 seconds
 Connections established 2 time(s)
 Local host: 15.0.0.1, Local port: 179
 Foreign host: 15.0.0.2, Foreign port: 49153
 Last Error: Code 0, SubCode 0.

BGP neighbor is 16.0.0.2, remote AS 100, internal link
 BGP version 4, remote router ID 16.0.0.2
 BGP state = Established, up for 1 minute 26 seconds, un-authenticated
session
 Configured BGP Maximum Prefix Limit 125
 DampPeer Oscillations ENABLED
```

```
 Configured Connect Retry Count 5
 Current Connect Retry Count 0
 Peer Passive : ENABLED
 Peer Status : NOT DAMPED
Idlehold time is 60   Rcvd update before 0 secs, hold time is 90,
keepalive interval is 35 secs
 Neighbors Capability:
 Route-Refresh: Advertised and received
 Address family IPv4 Unicast: Advertised and received
 Received 4 messages, 0 Updates
 Sent 4 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 15 seconds
Connections established 2 time(s)
Local host: 16.0.0.1, Local port: 179
Foreign host: 16.0.0.2, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

3.16. BGP Cost Community

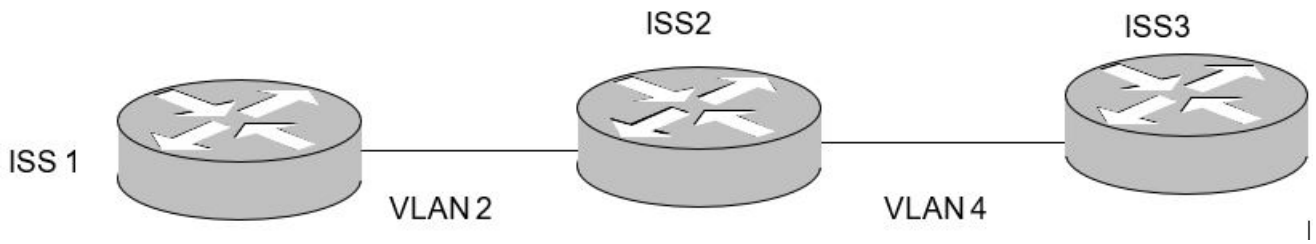
CONTEXT:

The *BGP* specification defines a decision process for installation of routes into the Loc-RIB. This process takes into account extensive series of path attributes, which can be manipulated to indicate preference for specific paths. It is cumbersome (if possible) for the end user to define policies that will select, after partial comparison, a path based on subjective local (domain and/or node) criteria.

The *BGP* Cost Community feature uses the extended cost community attribute. The cost community is a non-transitive extended community attribute that is passed to internal *BGP* (iBGP) and confederation peers but not to external *BGP* (eBGP) peers. The cost community feature allows the end user to customize the local route preference and influence the best path selection process by assigning cost values to specific routes.

The figure shown below depicts the topology setup used for this configuration.

Figure 17: BGP Configuration and Testing Topology for BGP Cost Community Attribute



Use the following commands to configure *BGP* routing.

1. Execute the following commands to configure *BGP* Peer group:

   FOR EXAMPLE: Perform the following:

   Configure Peer Group in Router ISS

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R2 (with as-num 100) as internal peer in R1..

   ```
   iS5comm(config-router)# neighbor 14.0.0.2 remote-as 100
   ```

2. To enable *BGP* in Router R2:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R2.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R2.

   ```
   iS5comm(config)# router-id 12.0.0.2
   ```

   – Enable *BGP* in R2.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R3 (with as-num 100) as internal peer in R2

   ```
   iS5comm(config-router)# neighbor 14.0.0.1 remote-as 100
   iS5comm(config-router)# neighbor 15.0.0.3 remote-as 100
   ```

3. To enable *BGP* in Router R3:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R3.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R3.

   ```
   iS5comm(config)# router-id 12.0.0.3
   ```

   – Enable *BGP* in R3.

```
iS5comm(config)# router bgp 100
```

– Configure R2 (with as-num 100) as internal peer in R2

```
iS5comm(config-router)# neighbor 15.0.0.2 remote-as 100
```

4. Configure a Route-Map in R2 for setting the Extended Community cost Attribute.

FOR EXAMPLE: Type the following:

– At R2:

– Configure Route-map AR1 for the peer 14.0.0.1 (R1).

```
iS5comm# configure terminal
iS5comm(config)# route-map AR1
iS5comm(config-rmap-AR1)# set extcommunity cost 1 100
iS5comm(config-rmap-AR1)# exit
```

– Configure Route-map AR2 for the peer 15.0.0.3 (R3).

```
iS5comm# configure terminal
iS5comm(config)# route-map AR2
iS5comm(config-rmap-AR2)# set extcommunity cost 2 200
iS5comm(config-rmap-AR2)# exit
```

5. Verify the Route-Map Configuration in R2.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp summary
Route-map AR1, Permit, Sequence 1
Match Clauses:
--------------

Set Clauses:
--------------
extcommunity cost 1 100

Route-map AR2, Permit, Sequence 1

Match Clauses:
--------------

Set Clauses:
--------------
extcommunity cost 2 200
```

6. Relate the Route-map to the Neighbors.

   FOR EXAMPLE: Execute the following commands:

   – Relate the Route-map to the Neighbors.

```
iS5comm(config-router)# neighbor 14.0.0.1 route-map AR1 in
iS5comm(config-router)# neighbor 15.0.0.3 route-map AR2 in
```

7. Add a same Static route in R1 & R3 and redistribute the routes.

   FOR EXAMPLE: Execute the following commands:

   At R1: Add static route 15.1.0.0/16.

```
iS5comm# configure terminal
iS5comm(config)# ip route 15.1.0.0 255.255.0.0 vlan 1
iS5comm(config)# exit
```

   – At R3: Add static route 15.1.0.0 / 16.

```
iS5comm# configure terminal
iS5comm(config)# ip route 15.1.0.0 255.255.0.0 vlan 1
iS5comm(config)# exit
```

8. Now verify the output in R2. The route with minimum cost is considered the best route

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp
BGP table version is 2,local router ID is 12.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete
Type    Network     NextHop     Metric  LocPrf  Path  Origin Weight
----    -------     -------     ------  ------  ----  ------ -----
 >      15.1.0.0/16 14.0.0.1     1      100     100     ?        0
 >      15.1.0.0/16 15.0.0.3     1      100     300     ?        0
```

3.17. Configuring Conditional Aggregation with Route-map

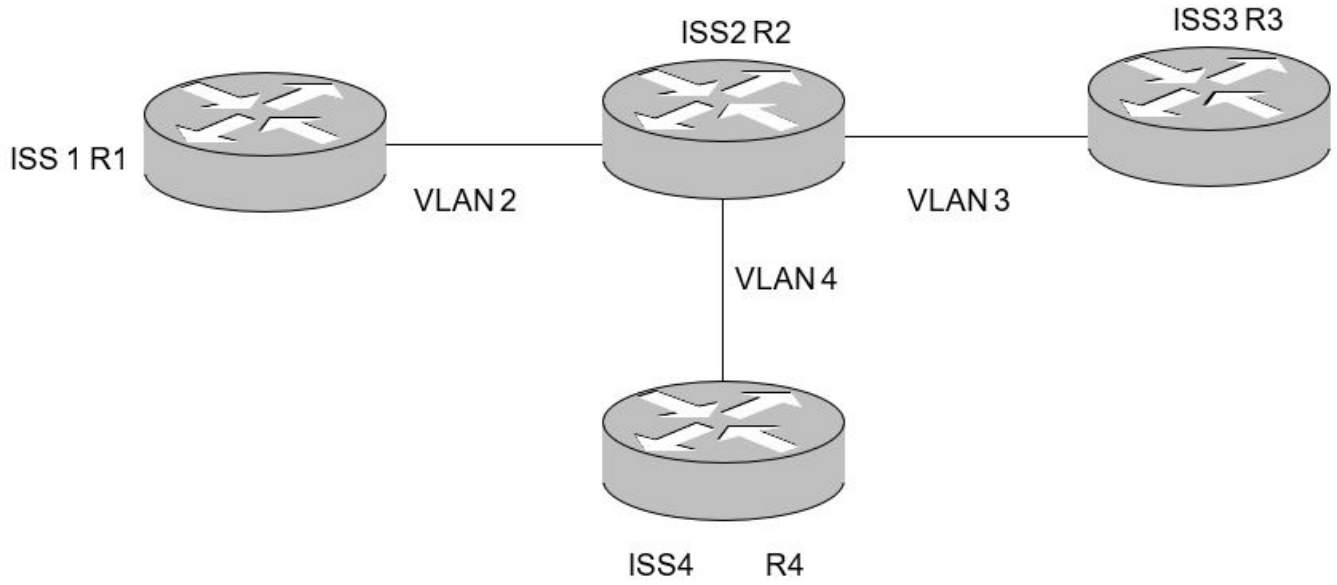
CLI Configurations

CONTEXT:

Configuring aggregation enables creating aggregate routes and minimizing the size of routing tables. The aggregation can be done conditionally using route-map to enforce the user given rules while forming the aggregate entry. The user can configure aggregate routes in *BGP* either by redistributing an aggregate route into *BGP* or by using the aggregation feature described below. An aggregate address will be added to the *BGP* table if there is at least one more specific entry in the *BGP* table.

The figure shown below depicts the topology setup used for this configuration.

Figure 18: BGP Configuration for BGP aggregation



Part A:

1. *BGP* neighbor configurations for conditional aggregation topology:

   FOR EXAMPLE: Perform the following:

   At R1:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure the R2 with as-num 200 as external peer in R1.

   ```
   iS5comm(config-router)# neighbor 13.0.0.2 remote-as 200
   iS5comm(config-router)# end
   ```

2. To configure *BGP* routing:

   FOR EXAMPLE: Execute the following commands:

   At R2: Enabling BGP in Router R2

   – Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

   – Enable *BGP* in R2.

```
iS5comm(config)# router bgp 200
```

   – Configure R1 (with as-num 100) as internal peer in R2

```
iS5comm(config-router)# neighbor 13.0.0.1 remote-as 100
```

   – Configure the R3 with as-num 300 as external peer in R2.

```
iS5comm(config-router)# neighbor 16.0.0.2 remote-as 300
```

   – Configure the R4 with as-num 400 as external peer in R2.

```
iS5comm(config-router)# neighbor 15.0.0.2 remote-as 400
iS5comm(config-router)# end
```

3. To configure *BGP* routing:

   FOR EXAMPLE: Execute the following commands:

   At R3:

   – Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

   – Enable *BGP* in R3.

```
iS5comm(config)# router bgp 300
```

   – Configure R2 (with as-num 200) as external peer in R3.

```
iS5comm(config-router)# neighbor 16.0.0.1 remote-as 200
iS5comm(config-router)# end
```

4. To configure *BGP* routing:

   FOR EXAMPLE: Execute the following commands:

   At R4:

   – Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

   – Enable *BGP* in R4.

```
iS5comm(config)# router bgp 400
```

   – Configure R2 (with as-num 100) as external peer in R3.

```
iS5comm(config-router)# neighbor 15.0.0.1 remote-as 200
iS5comm(config-router)# end
```

5. Verify that the *BGP* session between the peers R1, R3, and R4 is established, using the following show commands in R2.

   FOR EXAMPLE: Type the following:

   At R2:

```
iS5comm# show ip bgp summary
BGP router identifier is 14.0.0.2, local AS number 200
Forwarding State is enabled
BGP router identifier is 14.0.0.2, local AS number 200

BGP table version is 14
 Neighbor   Version    AS    MsgRcvd  MsgSent   Up/Down    State/PfxRcd
---------  -------    --    -------  -------   -------    ------------
 13.0.0.1     4      100        4       4     00:00:00:5  Established
 15.0.0.2     4      400        3       5    00:00:00:18  Established
 16.0.0.2     4      300        4       4     00:00:00:3  Established
```

   Part B

6. Inject static routes in R1 and in R3 and redistribute all routes in both the routers:

   FOR EXAMPLE: Perform the following:

   At R1:

   – Inject the static routes.

```
iS5comm# configure terminal
iS5comm(config)# ip route 10.0.1.0 255.255.255.0 vlan 1
iS5comm(config)# ip route 10.0.2.0 255.255.255.0 vlan 1
iS5comm(config)# endl
```

   – Redistribute the routes.

```
iS5comm# configure terminal
iS5comm(config)# as-num 100
iS5comm(config)# router-id 14.0.0.1
iS5comm(config)# end
iS5comm# configure terminal
iS5comm(config)# router bgp 100
iS5comm(config-router)# redistribute all
iS5comm(config-router)# end
```

   At R3:

   – Inject the static routes.

```
iS5comm# configure terminal
iS5comm(config)# ip route 10.0.3.0 255.255.255.0 vlan 1
```

```
iS5comm(config)# ip route 10.0.4.0 255.255.255.0 vlan 1
iS5comm(config)# endl
```

– Redistribute the routes.

```
iS5comm# configure terminal
iS5comm(config)# as-num 300
iS5comm(config)# router-id 14.0.0.3
iS5comm(config)# end
iS5comm# configure terminal
iS5comm(config)# router bgp 300
iS5comm(config-router)# redistribute all
iS5comm(config-router)# end
```

7. Verify the *BGP* route:

FOR EXAMPLE: Perform the following:

At R1:

```
iS5comm# show ip bgp rib
BGP table version is 10,local router ID is 14.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i –
internal S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------
 >           10.0.1.0/24         0.0.0.0                0     -     ?
 >           10.0.2.0/24         0.0.0.0                0     -     ?
 >           10.0.3.0/24        13.0.0.2 0     100   200   300     ?
 >           10.0.4.0/24        13.0.0.2 0     100   200   300     ?
 >           13.0.0.0/ 8         0.0.0.0 0       0     -     i
13.0.0.0/ 8        13.0.0.2       0     100   200     i
 >           14.0.0.0/ 8         0.0.0.0       0       0     -     i
14.0.0.0/ 8        13.0.0.2       0     100   200     i
 >           15.0.0.0/ 8        13.0.0.2       0     100   200     i
>           16.0.0.0/ 8        13.0.0.2       0     100   200     i
```

At R2:

```
iS5comm# show ip bgp rib
BGP table version is 10,local router ID is 14.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i –
internal S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Type       Network            NextHop     Metric  LocPrf  Path  Origin
```

```
----       -------             -------     ------  ------  ----  ------
>           10.0.1.0/24        13.0.0.1            100   100     ?
>           10.0.2.0/24        13.0.0.1            100   100     ?
>           10.0.3.0/24        16.0.0.2            100   300     ?
>           10.0.4.0/24        16.0.0.2            100   300     ?
>           13.0.0.0/ 8         0.0.0.0       0       0     -     i
            13.0.0.0/ 8        13.0.0.1       0     100   100     i
>           14.0.0.0/ 8         0.0.0.0       0       0     -     i
    14.0.0.0/ 8        13.0.0.1       0     100   100     i
 14.0.0.0/ 8        16.0.0.2       0     100   300     i
14.0.0.0/ 8        15.0.0.2       0     100   400     i
>           15.0.0.0/ 8         0.0.0.0       0       0     -     i
 15.0.0.0/ 8        15.0.0.2       0     100   400     i
>           16.0.0.0/ 8         0.0.0.0       0       0     -     i
16.0.0.0/ 8        16.0.0.2       0     100   300     i
```

At R3:

```
iS5comm# show ip bgp rib
BGP table version is 10,local router ID is 14.0.0.3
Status codes: s suppressed, d damped, h history, * valid, > best, i –
internal S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Type       Network            NextHop     Metric  LocPrf  Path  Origin
----     -------          -------    ------ ------  ----  ------>
10.0.1.0/24 16.0.0.1       0     100   200   100     ?
>           10.0.2.0/24        16.0.0.1       0     100   200   100
?
>           10.0.3.0/24         0.0.0.0              0     -     ?
>           10.0.4.0/24         0.0.0.0              0     -     ?
>           13.0.0.0/ 8        16.0.0.1       0     100   200     i
>           14.0.0.0/ 8         0.0.0.0       0       0     -     i
 14.0.0.0/ 8        16.0.0.1       0     100   200     i
>           15.0.0.0/ 8        16.0.0.1       0     100   200     i
>           16.0.0.0/ 8         0.0.0.0       0       0     -     i
 16.0.0.0/ 8        16.0.0.1       0     100   200     i
```

At R4:

```
iS5comm# show ip bgp rib
BGP table version is 10,local router ID is 14.0.0.4
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i –
internal S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------>
>           10.0.1.0/24        15.0.0.1       0     100   200   100
?
>           10.0.2.0/24        15.0.0.1       0     100   200   100
?
>           10.0.3.0/24        15.0.0.1       0     100   200   300
?
>           10.0.4.0/24        15.0.0.1       0     100   200   300
?
>           13.0.0.0/ 8        15.0.0.1       0     100   200     i
>           14.0.0.0/ 8         0.0.0.0       0       0     -     i
14.0.0.0/ 8        15.0.0.1        0     100   200     i
>           15.0.0.0/ 8         0.0.0.0       0       0     -     i
 15.0.0.0/ 8        15.0.0.1        0     100   200     i
>           16.0.0.0/ 8        15.0.0.1       0     100   200     i
```

Aggregation with Advertise-map

Conditional aggregation with advertise-map allows the administrator to set rules to enforce the routes which should be allowed in forming the aggregate route entry.

1. To configure *BGP* routing:

   FOR EXAMPLE: Execute the following commands:

   At R2:

   – Configure a route-map with permit access.

```
iS5comm# configure terminal
iS5comm(config)# route-map adv permit
iS5comm(config-rmap-sup)# match destination ip 10.0.3.0 255.255.255.0
```

   – Aggregate the 10.0/8 network routes with advertisement-map option.

```
iS5comm# configure terminal
iS5comm(config)# router bgp 200
iS5comm(config-router)# aggregate-address index 1 10.0.0.0 8 as-set
advertise-map adv
```

2. Verify the as-set entry for the aggregate route and the aggregate route is learnt in R1 and in R4 but not in R3 as the path information contains its own path.

   FOR EXAMPLE: Type the following:

   At R1: View if the route 10.0.0.0 is learnt.

```
iS5comm# show ip bgp
```

```
BGP table version is 17,local router ID is 14.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------
>           10.0.0.0/ 8        13.0.0.2             100   200   300
?
>           10.0.1.0/24         0.0.0.0               0     -     ?
>           10.0.2.0/24         0.0.0.0               0     -     ?
>           10.0.3.0/24        13.0.0.2       0      100   200   300
?
>           10.0.4.0/24        13.0.0.2       0      100   200   300
?
>           13.0.0.0/ 8         0.0.0.0       0        0     -     i
 13.0.0.0/ 8        13.0.0.2       0     100   200     i
>           14.0.0.0/ 8         0.0.0.0       0        0     -     i
 14.0.0.0/ 8        13.0.0.2       0     100   200     i
>           15.0.0.0/ 8        13.0.0.2       0      100   200     i
>            16.0.0.0/ 8        13.0.0.2       0     100   200     i
```

At R2: View the route.

```
iS5comm# show ip bgp
BGP table version is 14,local router ID is 14.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best,
i – internal S Stale Origin codes: i - IGP, e - EGP, ? - incomplete

Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------
*>           10.0.0.0/ 8         0.0.0.0               0     -     e
>           10.0.1.0/24        13.0.0.1             100   100     ?
>           10.0.2.0/24        13.0.0.1             100   100     ?
s>           10.0.3.0/24        16.0.0.2             100   300     ?
>           10.0.4.0/24        16.0.0.2             100   300     ?
>           13.0.0.0/ 8         0.0.0.0       0        0     -     i
 13.0.0.0/ 8        13.0.0.1       0     100   100     i
>           14.0.0.0/ 8         0.0.0.0       0        0     -     i
 14.0.0.0/ 8        13.0.0.1       0     100   100     i
14.0.0.0/ 8        16.0.0.2       0     100   300     i
14.0.0.0/ 8        15.0.0.2       0     100   400     i
>           15.0.0.0/ 8         0.0.0.0       0        0     -     i
```

```
 15.0.0.0/ 8         15.0.0.2         0     100    400      i
>            16.0.0.0/ 8          0.0.0.0         0        0      -      i
16.0.0.0/ 8         16.0.0.2         0     100    300      i
```

At R3: View if the route in *BGP RIB* doesn't contain 10.0.0.0/8 route since the aggregated route has the as-num in its path information, and since, it contains the R3's as-num, the aggregated route is not in R3's *RIB*.

```
iS5comm# show ip bgp
BGP table version is 15,local router ID is 14.0.0.3
Status codes: s suppressed, d damped, h history, * valid, > best, i –
internal S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------
>           10.0.1.0/24        16.0.0.1        0     100   200   100
?
>           10.0.2.0/24        16.0.0.1        0     100   200   100
?
>           10.0.3.0/24         0.0.0.0                0     -     ?
>           10.0.4.0/24         0.0.0.0                0     -     ?
>          13.0.0.0/ 8       16.0.0.1       0     100   200     i>
14.0.0.0/ 8          0.0.0.0        0       0     -     i
 14.0.0.0/ 8         16.0.0.1         0     100   200      i
>           15.0.0.0/ 8        16.0.0.1        0     100   200      i
>           16.0.0.0/ 8         0.0.0.0        0       0     -      i
16.0.0.0/ 8         16.0.0.1         0     100   200
```

At R4: View the aggregate route.

```
iS5comm# show ip bgp
BGP table version is 17,local router ID is 14.0.0.4
Status codes: s suppressed, d damped, h history, * valid, > best, i –
internal S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------
>           10.0.0.0/ 8         15.0.0.1             100   200   300
?
```

```
>           10.0.1.0/24         15.0.0.1       0     100   200   100
?
>           10.0.2.0/24         15.0.0.1       0     100   200   100
?
>           10.0.3.0/24         15.0.0.1       0     100   200   300
?
>           10.0.4.0/24         15.0.0.1       0     100   200   300
?
>           13.0.0.0/ 8         15.0.0.1       0     100   200     i
>           14.0.0.0/ 8          0.0.0.0       0       0     -     i
14.0.0.0/ 8         15.0.0.1        0     100   200     i
>           15.0.0.0/ 8          0.0.0.0       0       0     -     i
 15.0.0.0/ 8         15.0.0.1        0     100   200     i
>           16.0.0.0/ 8         15.0.0.1       0     100   200     i
```

Aggregation with Suppress-map

Conditional aggregation with suppress-map allows administrators to set rules to enforce which of the routes should not be allowed to form aggregate route entry.

1. Configure *BGP* neighbor configurations and static route addition in all routers as shown in Part A and Part B of the configurations section. Aggregate the route with Suppress-map option.

   FOR EXAMPLE: Execute the following commands:

   At R2:

   – Configure a route-map with permit access.

   ```
   iS5comm# configure terminal
   iS5comm(config)# route-map sup permit
   iS5comm(config-rmap-sup)# match destination ip 10.0.3.0 255.255.255.0
   ```

   – Aggregate the 10.0/8 network routes with suppress-map option.

   ```
   iS5comm# configure terminal
   iS5comm(config)# router bgp 200
   iS5comm(config-router)# aggregate-address index 1 10.0.0.0 8 summary-only
   suppress-map sup
   ```

2. Verify the route 10.0.0.0/8 network is to be aggregated and advertised but only 10.0.3.0 is suppressed and not added to the aggregate route. That is only the route mentioned in suppress map is suppressed and all other routes are aggregated to form the aggregate route.

   FOR EXAMPLE: Type the following:

   At R1: Verify the bgp routes 10.0.3.0 is marked as history and 10.0.0.0 is received.

   ```
   iS5comm# show ip bgp
   BGP table version is 17,local router ID is 14.0.0.1
   Status codes: s suppressed, d damped, h history, * valid, > best, i -
   internal S Stale
   ```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------
>           10.0.0.0/ 8        13.0.0.2             100   200     ?
>           10.0.1.0/24         0.0.0.0               0     -     ?
>           10.0.2.0/24         0.0.0.0               0     -     ?
h            10.0.3.0/24        13.0.0.2       0     100   200   300
?
>           10.0.4.0/24        13.0.0.2       0     100   200   300
?
>           13.0.0.0/ 8         0.0.0.0       0       0     -     i
 13.0.0.0/ 8        13.0.0.2       0     100   200     i   >
14.0.0.0/ 8         0.0.0.0        0       0     -     i
14.0.0.0/ 8        13.0.0.2        0     100   200     i   >
15.0.0.0/ 8        13.0.0.2        0     100   200     i   >
16.0.0.0/ 8        13.0.0.2        0     100   200     i
```

At R2: View the route 10.0.3.0 is marked as suppressed.

```
iS5comm# show ip bgp
BGP table version is 14,local router ID is 14.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best,
i – internal S Stale Origin codes: i - IGP, e - EGP, ? - incomplete

Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------
*>           10.0.0.0/ 8         0.0.0.0               0     -     e
>           10.0.1.0/24        13.0.0.1             100   100     ?
>           10.0.2.0/24        13.0.0.1             100   100     ?
s>           10.0.3.0/24        16.0.0.2              100   300     ?
>           10.0.4.0/24        16.0.0.2             100   300     ?
>           13.0.0.0/ 8         0.0.0.0       0       0     -     i
 13.0.0.0/ 8        13.0.0.1       0     100   100     i
>           14.0.0.0/ 8         0.0.0.0       0       0     -     i
 14.0.0.0/ 8        13.0.0.1       0     100   100     i
14.0.0.0/ 8        16.0.0.2        0     100   300     i
14.0.0.0/ 8        15.0.0.2        0     100   400     i
>           15.0.0.0/ 8         0.0.0.0       0       0     -     i
 15.0.0.0/ 8        15.0.0.2       0     100   400     i
>           16.0.0.0/ 8         0.0.0.0       0       0     -     i
16.0.0.0/ 8        16.0.0.2        0     100   300     i
```

At R3: View the route 10.0.0.0 is received in bgp rib.

```
iS5comm# show ip bgp
BGP table version is 15,local router ID is 14.0.0.3
Status codes: s suppressed, d damped, h history, * valid, > best, i –
internal S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------
>           10.0.0.0/ 8        16.0.0.1             100   200     ?
>           10.0.1.0/24        16.0.0.1       0     100   200   100
?
>           10.0.2.0/24        16.0.0.1       0     100   200   100
?
>           10.0.3.0/24         0.0.0.0             0     -     ?
>           10.0.4.0/24         0.0.0.0             0     -     ?
>           13.0.0.0/ 8        16.0.0.1       0     100   200     i
>           14.0.0.0/ 8         0.0.0.0       0       0     -     i
 14.0.0.0/ 8        16.0.0.1       0     100   200     i
>           15.0.0.0/ 8        16.0.0.1       0     100   200     i
>           16.0.0.0/ 8         0.0.0.0       0       0     -     i
16.0.0.0/ 8        16.0.0.1       0     100   200     i
```

At R4: Verify that the *BGP* route 10.0.3.0 is marked as history and 10.0.0.0 is received.

```
iS5comm# show ip bgp
BGP table version is 17,local router ID is 14.0.0.4
Status codes: s suppressed, d damped, h history, * valid, > best, i –
internal S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------
>           10.0.0.0/ 8        15.0.0.1             100   200     ?
>           10.0.1.0/24        15.0.0.1       0     100   200   100
?
>           10.0.2.0/24        15.0.0.1       0     100   200   100
?
h            10.0.3.0/24        15.0.0.1       0     100   200   300
?
>           10.0.4.0/24        15.0.0.1       0     100   200   300
?
```

```
>           13.0.0.0/ 8        15.0.0.1       0     100   200     i>
14.0.0.0/ 8         0.0.0.0       0       0     -     i
 14.0.0.0/ 8        15.0.0.1       0     100   200     i
>           15.0.0.0/ 8         0.0.0.0       0       0     -     i
15.0.0.0/ 8        15.0.0.1       0     100   200     i
>           16.0.0.0/ 8        15.0.0.1       0     100   200     i
```

Aggregation with Attribute-map

Conditional aggregation with attribute-map allows the administrator to set aggregate route properties.

1. Configure *BGP* neighbor configurations and static route addition in all routers as shown in Part A and Part B of the configuration section. Aggregate the route with attribute map in R2.

   FOR EXAMPLE: Execute the following commands:

   At R2:

   – Configure a route-map.

```
iS5comm# configure terminal
iS5comm(config)# route-map att
iS5comm(config-rmap-att)# set origin igp
```

   – Aggregate the 10.0 network routes with attribute-map option.

```
iS5comm# configure terminal
iS5comm(config)# router bgp 200
iS5comm(config-router)# aggregate-address index 1 10.0.0.0 8 summary-only
attribute-map sup
```

2. Verify that the route 10.0/8 network is to be summarized and its origin type is marked as i (*IGP*) though it should be *EGP*.

   FOR EXAMPLE: Type the following:

   R2: View the route 10.0.0.0 has the origin type as i (*IGP*)

```
iS5comm# show ip bgp
BGP table version is 17,local router ID is 14.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------
*>           10.0.0.0/ 8         0.0.0.0                0     -     i
s>           10.0.1.0/24        13.0.0.1              100   100     ?
s>           10.0.2.0/24        13.0.0.1              100   100     ?
s>           10.0.3.0/24        16.0.0.2              100   300     ?
s>           10.0.4.0/24        16.0.0.2              100   300     ?
>           13.0.0.0/ 8         0.0.0.0       0        0     -     i
```

```
 13.0.0.0/ 8         13.0.0.1        0     100   100     i
>            14.0.0.0/ 8          0.0.0.0         0        0     -
14.0.0.0/ 8         13.0.0.1        0     100   100     i
14.0.0.0/ 8         16.0.0.2        0     100   300     i
 14.0.0.0/ 8         15.0.0.2        0     100   400     i
>            15.0.0.0/ 8          0.0.0.0         0        0     -     i
 15.0.0.0/ 8         15.0.0.2        0     100   400     i
>            16.0.0.0/ 8          0.0.0.0         0        0     -     i
16.0.0.0/ 8         16.0.0.2        0     100   300     i
```

Aggregation with Advertise-map, Suppress-map and Attribute-map

Conditional aggregation with suppress-map allows administrators to set rules to enforce which of the routes should not be allowed to form aggregate route entry.

1. Configure *BGP* neighbor configurations and static route addition in all routers as shown in Part A and Part B of the cnfigurations section. Aggregate the route with advertise-map, suppress-map and attribute-map options.

   FOR EXAMPLE: Execute the following commands:

   At R2:

   – Configure a route-map with permit access.

```
iS5comm# configure terminal
iS5comm(config)# route-map adv permit
iS5comm(config-rmap-adv)# match destination ip 10.0.3.0 255.255.255.0
iS5comm(config-rmap-adv)# match destination ip 10.0.2.0 255.255.255.0
iS5comm(config-rmap-adv)#end
```

   – Configure a suppress route-map with permit access.

```
iS5comm# configure terminal
iS5comm(config)# route-map sup permit
iS5comm(config-rmap-sup)# match destination ip 10.0.2.0 255.255.255.0
iS5comm(config-rmap-sup)#end
```

   – Configure an attribute route-map.

```
iS5comm(config)# route-map adv permit
iS5comm(config)# route-map att permit
iS5comm(config-rmap-att)# set origin igp
iS5comm(config-rmap-att)#end
```

   – Aggregate a route for the 10.0/8 network with all above configured route-maps.

```
iS5comm# configure terminal
```

```
iS5comm(config)# router bgp 200
iS5comm(config-router)# aggregate-address index 1 10.0.0.0 8 as-set
advertise-map adv suppress-map sup attribute-map att
```

2. View the *BGP* route table.

   FOR EXAMPLE: Type the following:

   At R1: The route 10.0.0.0/8 is not there in R1's *RIB* since the aggregated route has the R1's as-num in its path information.

```
iS5comm# show ip bgp
BGP table version is 17,local router ID is 14.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------
>           10.0.1.0/24         0.0.0.0                0     -     ?
>           10.0.2.0/24         0.0.0.0                0     -     ?
>           10.0.3.0/24        13.0.0.2       0     100   200   300
?
>           10.0.4.0/24        13.0.0.2       0     100   200   300
?
>           13.0.0.0/ 8         0.0.0.0       0       0     -     i
 13.0.0.0/ 8        13.0.0.2        0     100   200     i
>           14.0.0.0/ 8         0.0.0.0       0       0     -     i
 14.0.0.0/ 8        13.0.0.2        0     100   200     i
>           15.0.0.0/ 8        13.0.0.2       0     100   200     i
```

3. Verify that the route 10.0.0.0/8 network is to be summarized and its origin type is marked as i (*IGP*) though it should be *EGP*.

   FOR EXAMPLE: Type the following:

   At R2: View the route.

```
iS5comm# show ip bgp
BGP table version is 17,local router ID is 14.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------
>           10.0.0.0/ 8         0.0.0.0                0     -     i
>           10.0.1.0/24        13.0.0.1              100   100     ?
```

```
s>           10.0.2.0/24        13.0.0.1             100   100     ?
s>           10.0.3.0/24        16.0.0.2             100   300     ?
>           10.0.4.0/24        16.0.0.2             100   300     ?
>           13.0.0.0/ 8         0.0.0.0       0       0     -     i
 13.0.0.0/ 8        13.0.0.1       0     100   100     i
>           14.0.0.0/ 8         0.0.0.0       0       0     -     i
 14.0.0.0/ 8        13.0.0.1       0     100   100     i
 14.0.0.0/ 8        16.0.0.2       0     100   300     i
14.0.0.0/ 8        15.0.0.2       0     100   400     i
>           15.0.0.0/ 8         0.0.0.0       0       0     -     i
 15.0.0.0/ 8        15.0.0.2       0     100   400     i
>           16.0.0.0/ 8         0.0.0.0       0       0     -     i
16.0.0.0/ 8        16.0.0.2       0     100   300     i
```

The route 10.0/8 is not there in R3's *RIB*, since the aggregated route has the R3's as-num in its path information.

At R3: View the route.

```
iS5comm# show ip bgp
BGP table version is 17,local router ID is 14.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------
*>           10.0.0.0/ 8         0.0.0.0               0     -     i
>           10.0.1.0/24        13.0.0.1             100   100     ?
s>           10.0.2.0/24        13.0.0.1             100   100     ?
s>           10.0.3.0/24        16.0.0.2             100   300     ?
>           10.0.4.0/24        16.0.0.2             100   300     ?
>           13.0.0.0/ 8         0.0.0.0       0       0     -     i
 13.0.0.0/ 8        13.0.0.1       0     100   100     i
>           14.0.0.0/ 8         0.0.0.0       0       0     -     i
14.0.0.0/ 8        13.0.0.1       0     100   100     i
14.0.0.0/ 8        16.0.0.2       0     100   300     i
14.0.0.0/ 8        15.0.0.2       0     100   400     i
>           15.0.0.0/ 8         0.0.0.0       0       0     -     i
15.0.0.0/ 8        15.0.0.2       0     100   400     i>
16.0.0.0/ 8         0.0.0.0       0       0     -     i
              16.0.0.0/ 8        16.0.0.2       0     100   300     i
```

At R4: View the aggregate route.

```
iS5comm# show ip bgp
BGP table version is 17,local router ID is 14.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Type       Network            NextHop     Metric  LocPrf  Path  Origin
----       -------            -------     ------  ------  ----  ------

>           10.0.0.0/ 8       15.0.0.1            100   200 {100 300}
e
>           10.0.1.0/24        15.0.0.1       0     100   200   100
?
>           10.0.2.0/24        15.0.0.1       0     100   200   100
?
>           10.0.3.0/24        15.0.0.1       0     100   200   300
?
>           10.0.4.0/24        15.0.0.1       0     100   200   300
?
>           13.0.0.0/ 8        15.0.0.1       0     100   200     i
>           14.0.0.0/ 8         0.0.0.0       0       0     -     i
14.0.0.0/ 8        15.0.0.1       0     100   200     i
>           15.0.0.0/ 8         0.0.0.0       0       0     -     i
15.0.0.0/ 8        15.0.0.1       0     100   200     i
>           16.0.0.0/ 8        15.0.0.1       0     100   200     i
```

3.18. Configuring BGP Multipath

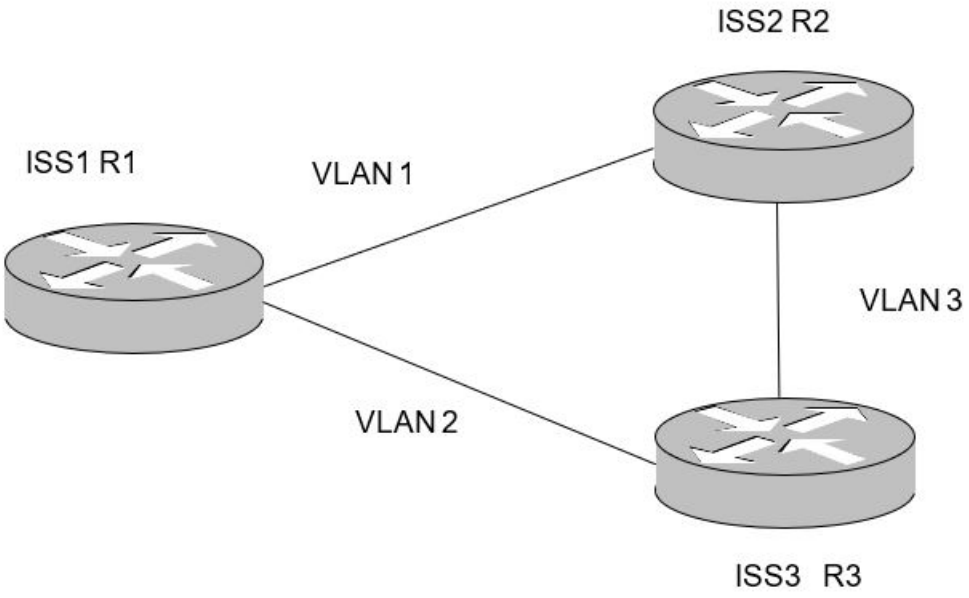
CONTEXT:

BGP multipath feature enables the user to add more than one route in IP routing table for same network from *BGP* Module. The installation of multiple–paths at IP is for load-sharing of traffic received by the self-node.

Number of multipath routes in IP Forwarding table from *BGP* is configurable per network using the CLI commands and *MIB* objects described in the following section. Configuration will have effect only after soft/hard reset.

The figure shown below depicts the topology setup used for this configuration.

Figure 19: BGP Configuration for BGP Multipath



In R1:

1. Configure *BGP* neighbors in ISS1.

   FOR EXAMPLE: Perform the following:

```
iS5comm# configure terminal
iS5comm(config)# as-num 100
iS5comm(config)# router-id 13.0.0.1
```

   – Enable *BGP* in ISS1.

```
iS5comm(config)# router bgp 100
iS5comm(config-router)# neighbor 14.0.0.2 remote-as 200
iS5comm(config-router)# neighbor 13.0.0.2 remote-as 200
```

2. Configure *BGP* multipath in ISS1.

   FOR EXAMPLE: Perform the following:

```
iS5comm(config-router)# maximum-paths 3
iS5comm(config-router)# end
iS5comm# clear ip bgp
```

In R2:

3. Configure *BGP* neighbors and redistribute connected routes in ISS2.

   FOR EXAMPLE: Perform the following:

```
iS5comm# configure terminal
iS5comm(config)# as-num 200
iS5comm(config)# router-id 14.0.0.2
```

– Enable BGP in ISS2

```
iS5comm(config)# router bgp 200
iS5comm(config-router)# neighbor 14.0.0.1 remote-as 100
iS5comm(config-router)# neighbor 16.0.0.2 remote-as 200
iS5comm(config-router)# redistribute connected
iS5comm(config-router)# end
```

In R3:

4. Configure *BGP* neighbors and redistribute connected routes in ISS3.

FOR EXAMPLE: Perform the following:

```
iS5comm# configure terminal
iS5comm(config)# as-num 200
iS5comm(config)# router-id 13.0.0.2
```

– Enable *BGP* in ISS2.

```
iS5comm(config)# router bgp 200
iS5comm(config-router)# neighbor 14.0.0.1 remote-as 100
iS5comm(config-router)# neighbor 16.0.0.2 remote-as 200
iS5comm(config-router)# redistribute connected
iS5comm(config-router)# end
```

In R1:

5. Check *BGP* multipath configuration in ISS1 using the show command given below.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp info
Context Name : VR1
-------------
Routing Protocol is "bgp 100"
Bgp Trap : Enabled
The route change interval is "60"
IGP synchronization is disabled
Both more-specific and less-specificoverlap route policy is set
Administrative Distance is 122
Default IPv4 Unicast Capability Status is set
Local Preference is 100
Non-bgp routes are advertised to bothexternal and internal peers
MED Comparision is disabled
Metric is 0
Default Originate Disable
```

```
Redistributing:
BGP GR admin status is disabled
Maximum paths: ibgp - 1 ebgp -  3 eibgp - 1
Maximum paths (Operational): ibgp - 1 ebgp -  3 eibgp - 1

Peer Table
Peer Address RemoteAS NextHop  MultiHop send-community
---- ------- -------- ------- -------- --------------
13.0.0.2     100     automatic disable  standard,extended
14.0.0.2     200     automatic disable  standard,extended
```

6. Check multipath routes in *BGP* local *RIB* in ISS1 using the “show command” as shown below.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp rib
Context Name : default
 -------------
BGP table version is 8, local router ID is 14.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
S Stale m - Multipath

Origin codes: i - IGP, e - EGP, ? - incomplete
Type       Network            NextHop     Metric  LocPrf  Path  Origin
Weight
----       -------            -------     ------  ------  ----  ------
-----
>          13.0.0.0/8         13.0.0.2       0     100   200     i
0
m          13.0.0.0/8         14.0.0.2       0     100   200     i
0
>          14.0.0.0/8         13.0.0.2       0     100   200     i
0
m          14.0.0.0/8         14.0.0.2       0     100   200     i
0
>          16.0.0.0/8         13.0.0.2       0     100   200     i
0
m          16.0.0.0/8         14.0.0.2       0     100   200     i
0
```

7. Check multipath routes in *IP* routing table manager (*RTM*) in ISS1 using the “show command”.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip route
Codes: C - connected, S - static, R - rip, B - bgp, O - ospf
```

```
IA - OSPF inter area, N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
E2 - OSPF external type 2

Vrf Name:          default
---------
C 13.0.0.0/8  is directly connected, vlan2
C 14.0.0.0/8  is directly connected, vlan1
B 16.0.0.0/8  [0] via 14.0.0.2 via 14.0.0.2
 [0] via 13.0.0.2 via 13.0.0.2
```

3.19. BGP TCP-AO Authentication

CONTEXT:

BGP Sessions can be authenticated using the *TCP* - Authentication Option (*TCP - AO*) as specified in RFC 5925 & RFC 5926. *TCP - AO* is compatible with a static Master Key Tuple (*MKT*) configuration. A *TCP MKT* needs to be configured independently and needs to be associated with a BGP peer. The *MKT* configuration will have the key ids (send / receive), a master key and optional configuration to include *TCP* options in digest calculation. The *AO* option uses the SHA-1 (96-bit digest) algorithm to calculate the digest. The *MKT* association can be changed on an authenticated session without disrupting the session. The new *MKT* association will be applied after negotiating the new key IDs with the peer and when both the peers are in sync.

The *MKT* configuration involves two steps:

- Configuring *TCP MKT*
- Associating the *MKT* with a peer

To configure a *TCP* - AO *MKT*, perform the following steps.

The following parameters are mandatory.

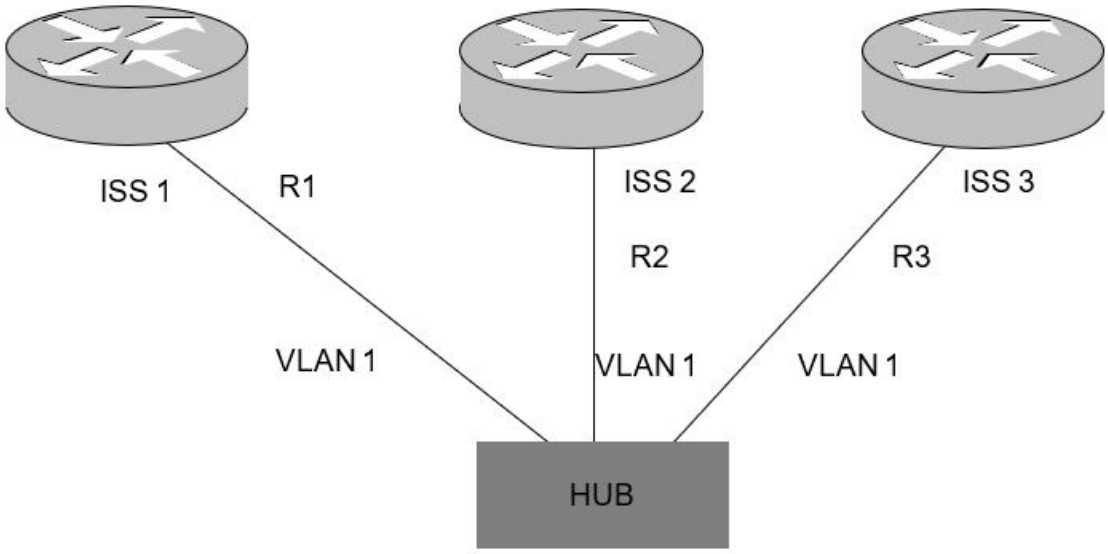
- Send Key ID (abbreviated as key-id)
- Receive Key ID
- Master key
- Algorithm

The following parameter is optional. By default, *TCP* options will be included in digest calculation.

- *TCP*-option-exclude

The figure shown below depicts the topology setup used for this configuration.

Figure 20: Configuration and Testing BGP Local Preference Value



1. Execute the following commands to configure *BGP* peer group:

   FOR EXAMPLE: Perform the following:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Configure the *AS* number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 10.0.0.1
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure *TCP - AO MKT* without tcp-option-exclude.

   ```
   iS5comm(config)# iS5comm(config-router)# tcp-ao mkt key-id 1
   receive-key-id 2 algorithm hmac-sha-1 key abcdef
   ```

   – Configure R2 (with as-num 100) as internal peer in R1.

   ```
   iS5comm(config-router)# neighbor 10.0.0.2 remote-as 100
   ```

   – Associating the above configured *MKT* to peer.

   ```
   iS5comm(config-router)# neighbor 10.0.0.2 tcp-ao mkt 1
   ```

   – Configure R3 (with as-num 100) as internal peer in R1.

   ```
   iS5comm(config-router)# neighbor fec0::1111:0:3 remote-as 100
   ```

   – Associating the above configured *MKT* to peer.

   ```
   iS5comm(config-router)# neighbor fec0::1111:0:3 tcp-ao mkt 1
   ```

2. Enabling *BGP* in Router R2.

   FOR EXAMPLE: Perform the following:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Configure the *AS* number in R2.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R2.

   ```
   iS5comm(config)# router-id 10.0.0.2
   ```

   – Enable *BGP* in R2.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R1 (with as-num 100) as internal peer in R2

   ```
   iS5comm(config-router)# neighbor 10.0.0.1 remote-as 100
   ```

   – Configure tcp-ao *MKT* without tcp-option-exclude

   ```
   iS5comm(config-router)# tcp-ao mkt key-id 2 receive-key-id 1 algorithm
   hmac-sha-1 key abcdef
   ```

   – Associating the above configured *MKT* to peer.

   ```
   iS5comm(config-router)# neighbor 10.0.0.1 tcp-ao mkt 2
   ```

3. Enabling *BGP* in Router R3.

   FOR EXAMPLE: Perform the following:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Configure the *AS* number in R3.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R3.

   ```
   iS5comm(config)# router-id 10.0.0.3
   ```

   – Enable *BGP* in R3.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R1 (with as-num 100) as internal peer in R3.

   ```
   iS5comm(config-router)# neighbor fec0::1111:0:1 remote-as 100
   ```

   – Configure tcp-ao *MKT* without tcp-option-exclude

   ```
    iS5comm(config-router)# tcp-ao mkt key-id 2 receive-key-id 1 algorithm
   hmac-sha-1 key abcdef
   ```

   – Associating the above configured MKT to peer.

   ```
   iS5comm(config-router)# neighbor fec0::1111:0:1 tcp-ao mkt 2
   ```

4. Verify that the *BGP* sessions between the peers R1, R2 and R1, R3 are established, using the following show commands in R1, R2 and R3.

   FOR EXAMPLE: Perform the following:

   – R1: View the bgp session information using ‘show ip bgp summary’, ‘show ip bgp neighbor’ and ‘show ip bgp info’ commands.

```
iS5comm# show ip bgp summary
Context Name : default
-------------

BGP router identifier is 12.0.0.1, local AS number 100
Forwarding State is enabled

BGP router identifier is 12.0.0.1, local AS number 100
BGP table version is 0
Neighbor   Version    AS    MsgRcvd  MsgSent   Up/Down    State/PfxRcd
---------  -------    --    -------  -------   -------    ------------
10.0.0.2     4      100       23      23    00:00:11:10  Established
fec0:1111::3     4      100        3       3    00:00:00:31  Established
iS5comm# show ip bgp neighbor
Context Name : BGP neighbor is 10.0.0.2, remote AS 100, internal link
 BGP version 4, remote router ID 12.0.0.2
Network Address: None
BGP state = Established, up for 2 seconds, tcp ao authenticated session
Configured BGP Maximum Prefix Limit 5000
AutomaticStart DISABLED
AutomaticStop DISABLED
DampPeer Oscillations DISABLED
DelayOpen DISABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Default-originate : DISABLED
Peer Passive : DISABLED
Peer Status : NOT DAMPED
GateWay Address : NONE
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 2 messages, 0 Updates
Sent 2 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 10.0.0.1, Local port: 49152
Foreign host: 10.0.0.2, Foreign port: 179
```

```
Last Error: Code 0, SubCode 0.
Update Source 10.0.0.1
Next-Hop is automatic
MultiHop Status - disabled
Send-Community is standard,extended
iS5comm# show bgp ipv6 neighbor
BGP neighbor is fec0:1111::3, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.3
Network Address: None
BGP state = Established, up for 4 minutes 40 seconds, tcp ao
authenticated session
Configured BGP Maximum Prefix Limit 5000
AutomaticStart DISABLED
AutomaticStop DISABLED
DampPeer Oscillations DISABLED
DelayOpen DISABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Default-originate : DISABLED
Peer Passive : DISABLED
Peer Status : NOT DAMPED
GateWay Address : NONE
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 11 messages, 0 Updates
Sent 11 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: fec0:1111::1, Local port: 49153
Foreign host: fec0:1111::3, Foreign port: 179
Last Error: Code 0, SubCode 0.
Update Source fec0:1111::1
Next-Hop is automatic
MultiHop Status - disabled
Send-Community is standard,extended
iS5comm# show ip bgp tcp-ao mkt summary
 TCP-AO MKT Table
```

```
----------------
Context Name : default
------------
ID(send)   Receive ID   Algorithm   MasterKey   OptionsExclude   Status
--------   ----------   ---------   ---------   --------------   ------

 1          2            HMAC-SHA-1  ********    1      Active
iS5comm# show bgp ipv6 tcp-ao neighbor
TCP-AO authentication neighbor summary
--------------------------------------

Context Name : default
------------
Neighbor            : fec0:1111::3
MKT Assigned         : 1
ICMP Processing      : Disabled
No MKT Discard       : Enabled
MKT In-use           : 1
iS5comm# show ip bgp info
Context Name : default
-------------

Routing Protocol is "bgp 100"
Bgp Trap : Enabled
The route change interval is "60"
IGP synchronization is disabled
Both more-specific and less-specificoverlap route policy is set
Administrative Distance is 122
Default IPv4 Unicast Capability Status is set
Local Preference is 100
Non-bgp routes are advertised to bothexternal and internal peers
MED Comparision is disabled
Metric is 0
Default Originate Disable
Redistributing:
 BGP GR admin status is disabled
Maximum paths: ibgp - 1 ebgp -  1 eibgp - 1
Maximum paths (Operational): ibgp - 1 ebgp -  1 eibgp - 1

Peer Table
```

```
Peer Address RemoteAS NextHop  MultiHop send-community
---- ------- -------- ------- -------- ------------
10.0.0.2     100     automatic disable  standard,extended
fec0:1111::3 100     automatic disable  standard,extended
```

R2: View the bgp session information using 'show ip bgp summary', 'show ip bgp neighbor' and 'show ip bgp info' commands.

```
iS5comm# show ip bgp summary
Context Name : default
-------------

BGP router identifier is 12.0.0.2, local AS number 100
Forwarding State is enabled

BGP table version is 0
Neighbor   Version    AS    MsgRcvd  MsgSent   Up/Down    State/PfxRcd
---------  -------    --    -------  -------   -------    ------------
10.0.0.1     4      100       11      11     00:00:4:57  Established


iS5comm# show ip bgp neighbor
BGP neighbor is 10.0.0.1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.1
Network Address: None
BGP state = Established, up for 5 minutes 28 seconds, tcp ao
authenticated session
Configured BGP Maximum Prefix Limit 5000
AutomaticStart DISABLED
AutomaticStop DISABLED
DampPeer Oscillations DISABLED
DelayOpen DISABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Default-originate : DISABLED
Peer Passive : DISABLED
Peer Status : NOT DAMPED
GateWay Address : NONE
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
 Route-Refresh: Advertised and received
 Address family IPv4 Unicast: Advertised and received
```

```
 Received 12 messages, 0 Updates
 Sent 12 messages, 0 Updates
Route refresh: Received 0, sent 0.
 Minimum time between advertisement runs is 5 seconds
 Connections established 1 time(s)
 Local host: 10.0.0.2, Local port: 179
Foreign host: 10.0.0.1, Foreign port: 49152
Last Error: Code 0, SubCode 0.
Update Source 10.0.0.2
 Next-Hop is automatic
 MultiHop Status - disabled
 Send-Community is standard,extended

iS5comm# show ip bgp info
Context Name : default
-------------
Routing Protocol is "bgp 100"
Bgp Trap : Enabled
The route change interval is "60"
IGP synchronization is disabled
Both more-specific and less-specificoverlap route policy is set
Administrative Distance is 122
Default IPv4 Unicast Capability Status is set
Local Preference is 100
Non-bgp routes are advertised to bothexternal and internal peers
MED Comparision is disabled
Metric is 0
Default Originate Disable
Redistributing:
BGP GR admin status is disabled
Maximum paths: ibgp - 1 ebgp -  1 eibgp - 1
Maximum paths (Operational): ibgp - 1 ebgp -  1 eibgp - 1

Peer Table
Peer Address RemoteAS NextHop  MultiHop send-community
---- ------- -------- ------- -------- ------------
10.0.0.1     100     automatic disable  standard,extended
```

R3: View the bgp session information using ‘show ip bgp summary’, ‘show ip bgp neighbor’ and ‘show ip bgp info’ commands.

```
iS5comm# show ip bgp summary
Context Name : default-------------

BGP router identifier is 12.0.0.3, local AS number 100
Forwarding State is enabled

BGP table version is 0
Neighbor   Version    AS    MsgRcvd  MsgSent   Up/Down    State/PfxRcd
---------  -------    --    -------  -------   -------    ------------
fec0:1111::1     4      100        8       8     00:00:3:23  Established

iS5comm# show ip bgp neighbor
BGP neighbor is fec0:1111::1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.1
Network Address: None
BGP state = Established, up for 3 minutes 47 seconds, tcp ao
authenticated session
Configured BGP Maximum Prefix Limit 5000
AutomaticStart DISABLED
AutomaticStop DISABLED
DampPeer Oscillations DISABLED
DelayOpen DISABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Default-originate : DISABLED
Peer Passive : DISABLED
Peer Status : NOT DAMPED
GateWay Address : NONE
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
 Route-Refresh: Advertised and received
 Address family IPv4 Unicast: Advertised and received
 Received 9 messages, 0 Updates
 Sent 9 messages, 0 Updates
Route refresh: Received 0, sent 0.
 Minimum time between advertisement runs is 5 seconds
 Connections established 1 time(s)
 Local host: fec0:1111::3, Local port: 179
Foreign host: fec0:1111::1, Foreign port: 49152
```

```
Last Error: Code 0, SubCode 0.
Update Source fec0:1111::3
 Next-Hop is automatic
 MultiHop Status - disabled
 Send-Community is standard,extended

iS5comm# show ip bgp info
Context Name : default
-------------
Routing Protocol is "bgp 100"
Bgp Trap : Enabled
The route change interval is "60"
IGP synchronization is disabled
Both more-specific and less-specificoverlap route policy is set
Administrative Distance is 122
Default IPv4 Unicast Capability Status is set
Local Preference is 100
Non-bgp routes are advertised to bothexternal and internal peers
MED Comparision is disabled
Metric is 0
Default Originate Disable
Redistributing:
BGP GR admin status is disabled
Maximum paths: ibgp - 1 ebgp -  1 eibgp - 1
Maximum paths (Operational): ibgp - 1 ebgp -  1 eibgp - 1

Peer Table
Peer Address RemoteAS NextHop  MultiHop send-community
---- ------- -------- ------- -------- ------------
fec0:1111::1 100     automatic disable  standard,extended
```

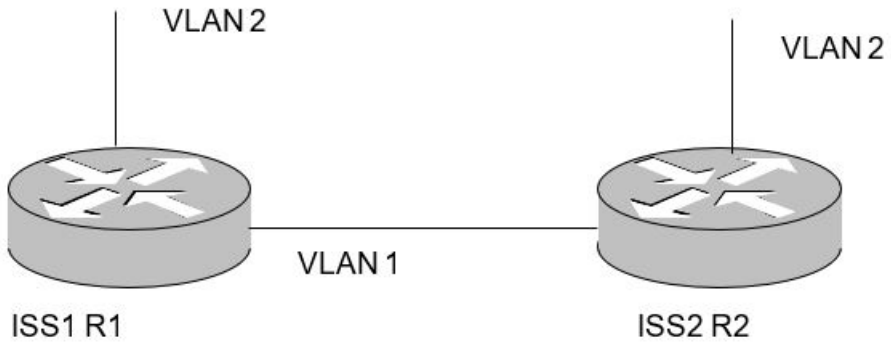
3.20. Configuring ORF capability for Neighbors

CONTEXT:

By default, Outbound Route Filtering (*ORF*) capability is disabled. *ORF* send capability or receive capability or both can be enabled via configuration. For a successful negotiation of *ORF* capability, one peer should have advertised *ORF* send capability, and the other one should have advertised *ORF* receive capability.

The figure shown below depicts the topology setup used for this configuration.

Figure 21: BGP Configuration and Testing Topology



1. To enable *BGP* routing:

   FOR EXAMPLE: Execute the following commands:

   Enabling BGP in Router R1

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R2 (with as-num 200) as external peer in R1.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 remote-as 200
   ```

   – Configure *ORF* send capability for the peer R2.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 capability orf prefix-list send
   ```

   Enabling *BGP* in Router R2

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (AS) number in R1.

   ```
   iS5comm(config)# as-num 200
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.2
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 200
   ```

   – Configure R1 (with as-num 100) as external peer in R2.

   ```
   iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100
   ```

– Configure *ORF* send capability for the peer R1.

```
iS5comm(config-router)# neighbor 12.0.0.1 capability orf prefix-list
receive
```

2. R1: View the output using the show command mentioned below.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 200, internal link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 2 minutes 43 seconds, un-authenticated
session
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Passive : DISABLED
Peer Status : NOT DAMPED
Route map for incoming advertisements is INRMAP
Route map for outgoing advertisements is RMAP
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Address family IPv4 Unicast: Advertised and received
AF-dependant capabilities:
Outbound Route Filter (ORF) type : (64) Address Prefix based ORF
Send-mode : advertised
Receive-mode : received
Received 7 messages, 0 Updates
Sent 7 messages, 1 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 12.0.0.1, Local port: 179
Foreign host: 12.0.0.2, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

3. R2: View the output using the show command mentioned below.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp neighbor
```

```
BGP neighbor is 12.0.0.1, remote AS 100, internal link
BGP version 4, remote router ID 12.0.0.1
BGP state = Established, up for 7 minutes 45 seconds, un-authenticated
session
Configured BGP Maximum Prefix Limit 10
AutomaticStart DISABLED
AutomaticStop DISABLED
DampPeer Oscillations DISABLED
DelayOpen DISABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Default-originate : DISABLED
Peer Passive : DISABLED
Peer Status : NOT DAMPED
GateWay Address : NONE
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
4-byte ASN: Advertised and received
Address family IPv4 Unicast: Advertised and received
AF-dependant capabilities:
Outbound Route Filter (ORF) type : (64) Address Prefix based ORF
Send-mode : received
Receive-mode : advertised
Received 17 messages, 0 Updates
Sent 17 messages, 0 Updates
Route refresh: Received 1, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 4 time(s)
Local host: 12.0.0.2, Local port: 179
Foreign host: 12.0.0.1, Foreign port: 65115
Last Error: Code 6, SubCode 0.
Update Source 12.0.0.2
Next-Hop is automatic
MultiHop Status - disabled
Send-Community is standard,extended
```

3.21. Configuring IP-Prefix List for Neighbors

CONTEXT:

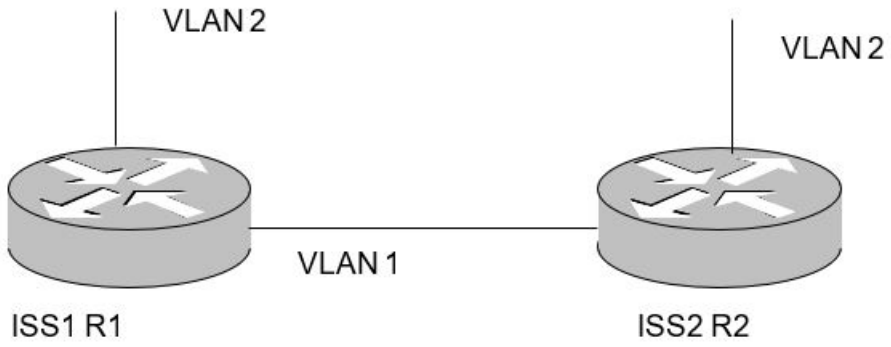
IP-Prefix lists are used to control and modify the routing information that is exchanged between routing domains. IP-Prefix lists consist of a set of filters based on network IP and prefix length. These filters' information will be sent to the remote peer when *ORF* (Outbound Route Filtering) message is triggered, and the remote peer will apply the filters whenever it sends the route update to the *BGP* speaker. The filters will be applied in order of sequence—any *ORF* filter with lowest sequence number will be applied first.

If the sequence number is not specified while creating the IP prefix entry, it will be automatically generated by incrementing the value by 5 counting from the larger sequence number used before.

When configuring In-direction Prefix list, the filter information will be sent to the peer if ORF capability is negotiated between the peers. Out direction IP-Prefix list is not supported now.

The figure shown below depicts the topology setup used for this configuration.

Figure 22: BGP Configuration and Testing Topology



1. To enable *BGP* routing:

   FOR EXAMPLE: Execute the following commands:

   Enabling BGP in Router R1

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Enable *BGP* in R1.

   ```
   iS5comm(config)# router bgp 100
   ```

   – Configure R2 (with as-num 200) as external peer in R1.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 remote-as 200
   ```

   – Configure *ORF* send capability for the peer R2.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 capability orf prefix-list send
   ```

– Configure In Direction IP Prefix list for the peer R2.

```
iS5comm(config-router)# neighbor 12.0.0.2 capability orf prefix-list send
```

– Create IP Prefix list entry for denying the 10 network route updates.

```
iS5comm(config-router)# neighbor 12.0.0.2 prefix-list INPREFIXLIST in
```

– Create IP Prefix list entry for allowing all route updates.

```
iS5comm(config)# ip prefix-list INPREFIXLIST permit 0.0.0.0/0 ge 32  le 32
```

– Trigger the *BGP* message for the neighbor 12.0.0.2.

```
iS5comm# clear ip bgp neighbor 12.0.0.2 soft in prefix-filter
```

Enabling BGP in Router R2

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enter the Autonomous System (*AS*) number in R2.

```
iS5comm(config)# as-num 200
```

– Configure the router-id in R2.

```
iS5comm(config)# router-id 12.0.0.2
```

– Enable BGP in R2.

```
iS5comm(config)# router bgp 200
```

– Configure R2 (with as-num 100) as external peer in R1.

```
iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100
```

– Configure *ORF* send capability for the peer R1.

```
iS5comm(config-router)# neighbor 12.0.0.1 capability orf prefix-list
receive
```

2. R2: Add static route 16.0.0.0/8.
3. R2: Add static route 10.0.0.0/8 and verify the results.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 200, internal link
BGP version 4, remote router ID 12.0.0.2
BGP state = Established, up for 2 minutes 43 seconds, un-authenticated
session
Configured BGP Maximum Prefix Limit 100
Configured Connect Retry Count 5
Current Connect Retry Count 0
Peer Passive : DISABLED
Peer Status : NOT DAMPED
Route map for incoming advertisements is INRMAP
Route map for outgoing advertisements is RMAP
```

```
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Address family IPv4 Unicast: Advertised and received
AF-dependant capabilities:
Outbound Route Filter (ORF) type : (64) Address Prefix based ORF
Send-mode : advertised
Receive-mode : received
Ip Prefix-list IN  : INPREFIXLIST
Received 7 messages, 0 Updates
Sent 7 messages, 1 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 12.0.0.1, Local port: 179
Foreign host: 12.0.0.2, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

4. R2: View the output using the show command mentioned below.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp neighbor 12.0.0.1 received prefix-filter
seq 5 deny 10.0.0.0/8
seq 10 permit 0.0.0.0/0 ge 32 le 32
```

– R2: View the output using the show command mentioned below

```
iS5comm# show ip bgp rib
Context Name : default
-------------
BGP table version is 7,local router ID is 12.0.0.2
Status codes: s suppressed, d damped, h history,
* valid, > best, i - internal
S Stale m - Multipath
Origin codes: i - IGP, e - EGP, ? - incomplete
Type Network NextHop Metric LocPrf Path Origin Weight
---  ------  ------  -----  -----  ---- -----  ----
>  10.0.0.0/8 0.0.0.0  10     -       ?       0
>  16.0.0.0/8 0.0.0.0  1      100     -       ?       0
```

– R1: View the output using the show command mentioned below

```
iS5comm# show ip bgp rib
Context Name : default
-------------
BGP table version is 7,local router ID is 12.0.0.1
Status codes: s suppressed, d damped, h history,
* valid, > best, i - internal
S Stale m - Multipath
Origin codes: i - IGP, e - EGP, ? - incomplete
Type Network NextHop Metric LocPrf Path Origin Weight
---  ------  ------  -----  -----  ---- -----  ----
>  16.0.0.0/8 12.0.0.2 1       100      -    ?   0
```

3.22. BGP Send Community

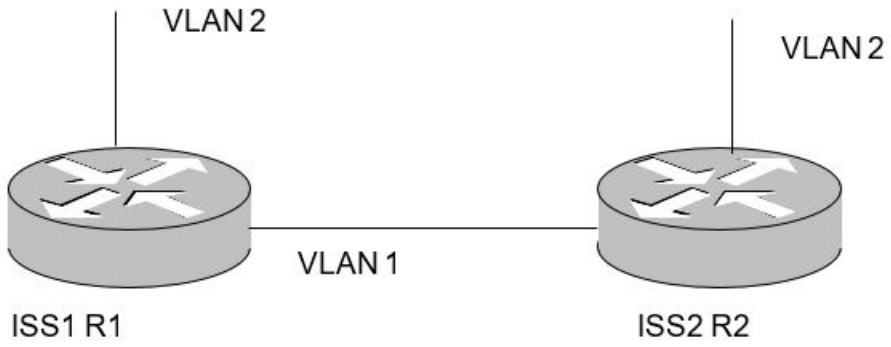
CONTEXT:

This command sends community attributes to a *BGP* neighbor and enables advertisement of community attributes (standard/extended) to a peer.

The no form of the command disables advertisement of community attributes (standard/extended) to a peer.

The figure shown below depicts the topology setup used for this configuration.

Figure 23: BGP Configuration and Testing Topology



1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

```
iS5comm(config)# router-id 12.0.0.1
```

– Enable BGP in R1.

```
iS5comm(config)# router bgp 100
```

– Configure R2 (with as-num 100) as internal peer in R1.

```
iS5comm(config-router)# neighbor 14.0.0.2 remote-as 100
```

2. To enable *BGP* in Router R2:

FOR EXAMPLE: Execute the following commands:

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enter the Autonomous System (*AS*) number in R2.

```
iS5comm(config)# as-num 100
```

– Configure the router-id in R2.

```
iS5comm(config)# router-id 12.0.0.2
```

– Enable *BGP* in R2.

```
iS5comm(config)# router bgp 100
```

– Configure R2 (with as-num 100) as internal peer in R1.

```
iS5comm(config-router)# neighbor 14.0.0.1 remote-as 100
```

3. Configure a route map in R1 for setting a community attribute.

FOR EXAMPLE: Type the following:

At R1:

– Configure Route-map AR1 for the peer 14.0.0.1 (R1)

```
iS5comm# configure terminal
iS5comm(config)# route-map AR1
iS5comm(config-rmap-AR1)# match destination ip 55.0.0.1 255.0
iS5comm(config-rmap-AR1)# set community Internet
iS5comm(config-rmap-AR1)# exit
```

4. Verify the route-map configuration in R2.

FOR EXAMPLE: Type the following:

```
iS5comm# show route-map
Route-map SW1, Permit, Sequence 1
Match Clauses:
--------------
destination ip 55.0.0.1  255.0.0.0
Set Clauses:
--------------
```

```
community internet
```

5. Relate the route-map to the neighbor.

   FOR EXAMPLE: Type the following:

   At R1:

```
iS5comm(config-router)# neighbor 14.0.0.2 route-map AR1 out
```

6. Configure the send-community attribute for the neighbor.

   FOR EXAMPLE: Type the following:

   At R1:

```
iS5comm# configure terminal
iS5comm(config)# router bgp 100
iS5comm(config)# neighbor 14.2 send-community both
iS5comm(config)# exit
```

7. Now verify the output in R1.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp info
Context Name : default
-------------
Routing Protocol is "bgp 100"
Bgp Trap : Enabled
The route change interval is "60"
IGP synchronization is disabled
Both more-specific and less-specificoverlap route policy is set
Administrative Distance is 122
Default IPv4 Unicast Capability Status is set
Local Preference is 100
Non-bgp routes are advertised to bothexternal and internal peers
MED Comparision is disabled
Metric is 0
Default Originate Disable
Redistributing:direct,static,rip,ospf
BGP GR admin status is disabled

Peer Table
Peer Address RemoteAS NextHop  MultiHop send-community
---- ------- -------- ------- -------- --------------
```

```
14.0.0.2      200     self           disable   standard,extended
```

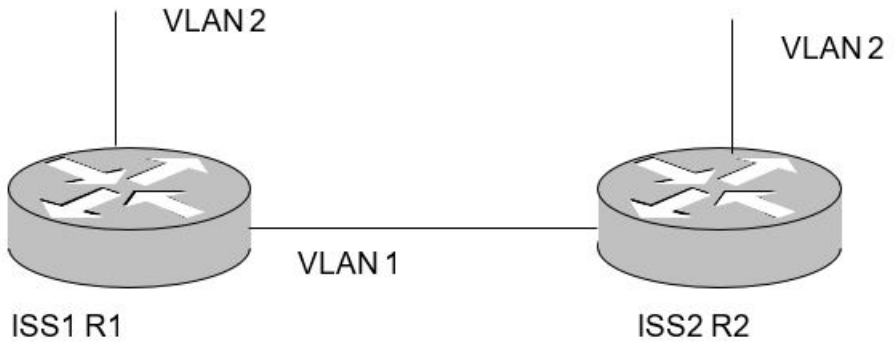
3.23. BGP 4-Byte ASN

CONTEXT:

BGP 4-Byte autonomous system numbers (*ASN*) feature supports configuration of 4-byte *ASN* to *BGP* routers. This has been added as a separate capability which is enabled by default.

The figure shown below depicts the topology setup used for this configuration.

Figure 24: BGP Configuration and Testing Topology



1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (*AS*) number in R1.

   ```
   iS5comm(config)# as-num 100
   ```

   – Configure the router-id in R1.

   ```
   iS5comm(config)# router-id 12.0.0.1
   ```

   – Enable *BGP* in R1 (assigning a 4-byte ASN).

   ```
   iS5comm(config)# router bgp 100.1
   ```

   – Configure R2 (with as-num 100.2) as external peer in R1.

   ```
   iS5comm(config-router)# neighbor 12.0.0.2 remote-as 100.2
   ```

2. To enable *BGP* in Router R2:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Autonomous System (AS) number in R2.

```
iS5comm(config)# as-num 100
```

– Configure the router-id in R2.

```
iS5comm(config)# router-id 12.0.0.2
```

– Enable BGP in R2 (assigning a 4 byte ASN).

```
iS5comm(config)# router bgp 100.2
```

– Configure R2 (with as-num 100.1) as external peer in R1.

```
iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100.1
```

3. Verify that the *BGP* session between the internal peers R1 and R2 is established, using the following show commands in R1 and R2.

FOR EXAMPLE: Type the following:

– R1: View the BGP summary information using 'show ip bgp summary'

```
iS5comm# show ip bgp summary
Context Name : default
-------------
BGP router identifier is 12.0.0.1, local AS number 6553601
Forwarding State is enabled
BGP table version is 0
Neighbor   Version    AS    MsgRcvd  MsgSent   Up/Down    State/PfxRcd
---------  -------   ---    -------  -------   -------    ------------
12.0.0.2      4    6553602     2        2     00:00:00:3  Established
R2: View the bgp summary information using 'show ip bgp summary'

iS5comm# show ip bgp summary
Context Name : default
-------------
BGP router identifier is 12.0.0.2, local AS number 6553602
Forwarding State is enabled

 BGP table version is 0
Neighbor   Version    AS    MsgRcvd  MsgSent   Up/Down    State/PfxRcd
---------  -------   ---    -------  -------   -------    ------------
12.0.0.1      4    6553601    11       11      00:00:5:5  Established
```

NOTE: The display notation of *ASN* (in show commands) is in asplain format (i.e. represented by its decimal value e.g. 6553601) by default. It can be changed to *Asdot* format (i.e. the 4-byte ASN are represented by their decimal value e.g. 100.1)

4. Enabling *Asdot* notation in Router R1.

FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# router bgp 100.1
iS5comm(config)# bgp asnotation dot
iS5comm(config)# end
```

5. Enabling *Asdot* notation in Router R2.

FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# router bgp 100.2
iS5comm(config)# bgp asnotation dot
iS5comm(config)# end
```

– R1: View the bgp summary information using 'show ip bgp summary'

```
iS5comm# show ip bgp summary
Context Name : default
-------------
Forwarding State is enabled
BGP table version is 0
Neighbor   Version    AS    MsgRcvd  MsgSent   Up/Down    State/PfxRcd
---------  -------   ---    -------  -------   -------    ------------
 12.0.0.2      4      100.2    2       2       00:00:00:3  Established
```

– R2: View the bgp summary information using 'show ip bgp summary'

```
iS5comm# show ip bgp summary
Context Name : default
 -------------
BGP router identifier is 12.0.0.2, local AS number 100.2
Forwarding State is enabled
BGP table version is 0
Neighbor   Version    AS    MsgRcvd  MsgSent   Up/Down    State/PfxRcd
---------  -------   ---    -------  -------   -------    ------------
12.0.0.1      4       100.1    11       11      00:00:5:5  Established
```

6. Disabling *Asdot* notation in Router R1.

FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# router bgp 100.1
iS5comm(config)# no bgp asnotation dot
iS5comm(config)# exit
```

7. Disabling *Asdot* notation in Router R2.

FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# router bgp 100.2
iS5comm(config)# no bgp asnotation dot
iS5comm(config)# exit
```

– R1: View the bgp summary information using 'show ip bgp summary'

```
iS5comm# show ip bgp summary
Context Name : default
-------------
BGP router identifier is 12.0.0.1, local AS number 6553601Forwarding
State is enabled
BGP table version is 0
Neighbor   Version    AS    MsgRcvd  MsgSent   Up/Down    State/PfxRcd
---------  -------   ---    -------  -------   -------    -----------
12.0.0.2      4     6553602    2        2      00:00:00:3  Established
```

– R2: View the bgp summary information using 'show ip bgp summary'

```
iS5comm# show ip bgp summary
Context Name : default
-------------
BGP router identifier is 12.0.0.2, local AS number 6553602Forwarding
State is enabled
BGP table version is 0
Neighbor   Version    AS    MsgRcvd  MsgSent   Up/Down    State/PfxRcd
---------  -------   ---    -------  -------   -------    -----------
12.0.0.1      4     655361    11        11      00:00:5:5  Established
```

NOTE: The 4-byte *AS* Number capability can be disabled only when BGP Global Admin Status is down.

8. Disabling 4-byte *ASN* capability in Router R1.

FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# do shutdown ip bgp
iS5comm(config)# no ip bgp four-byte-asn
iS5comm(config)# no shutdown ip bgp
iS5comm(config)# end
```

9. Establishing *BGP* session between R1 and R2.

FOR EXAMPLE: Type the following:

– Configuring Local AS and Peer Remote AS at R1.

```
iS5comm# configure terminal
iS5comm(config)# router-id 12.0.0.1
iS5comm(config)# router bgp 100
```

– Configure the peer remote *AS* as AS_TRANS (23456), if and only if, the peer is 4-byte ASN enabled router and its *AS* number is greater than 65535. If the peer's *AS* number is less than or equal to 65535, the same should be configured as peer remote *AS*.

```
iS5comm(config-router)# neighbor 12.0.0.2 remote-as 23456
iS5comm(config-router)# end
```

– Configuring local *AS* and peer remote *AS* at R2.

```
iS5comm# configure terminal
iS5comm(config)# router-id 12.0.0.2
iS5comm(config)# router bgp 100.2
iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100
iS5comm(config-router)# end
```

10. Verify that 4-byte *ASN* capability is not advertised/received in R1.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.2, remote AS 23456, external link
BGP version 4, remote router ID 12.0.0.2
Network Address: None
BGP state = Established, up for 7 seconds, un-authenticated session
Configured BGP Maximum Prefix Limit 5000
AutomaticStart DISABLED
AutomaticStop DISABLED
DampPeer Oscillations DISABLED
DelayOpen DISABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Default-originate : DISABLED
Peer Passive : DISABLED
Peer Status : NOT DAMPED
GateWay Address : NONE
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
AF-dependant capabilities:
Outbound Route Filter (ORF) type : (64) Address Prefix based ORF
```

```
Send-mode : not supported
Receive-mode : not supported
Received 2 messages, 0 Updates
Sent 2 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
Connections established 1 time(s)
Local host: 12.0.0.1, Local port: 179
Foreign host: 12.0.0.2, Foreign port: 63916
Last Error: Code 0, SubCode 0.
Update Source 12.0.0.1
Next-Hop is automatic
MultiHop Status - disabled
Send-Community is standard,extended
```

11. Verify that 4-byte *ASN* capability is not advertised/received in R2.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp neighbor
BGP neighbor is 12.0.0.1, remote AS 100, external link
BGP version 4, remote router ID 12.0.0.1
Network Address: None
BGP state = Established, up for 1 minute 10 seconds, un-authenticated
session
Configured BGP Maximum Prefix Limit 5000
AutomaticStart DISABLED
AutomaticStop DISABLED
DampPeer Oscillations DISABLED
DelayOpen DISABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Default-originate : DISABLED
Peer Passive : DISABLED
Peer Status : NOT DAMPED
GateWay Address : NONE
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
AF-dependant capabilities:
Outbound Route Filter (ORF) type : (64) Address Prefix based ORF
```

```
Send-mode : not supported
Receive-mode : not supported
Received 4 messages, 0 Updates
Sent 4 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
Connections established 1 time(s)
Local host: 12.0.0.2, Local port: 63916
Foreign host: 12.0.0.1, Foreign port: 179
Last Error: Code 0, SubCode 0.
Update Source 12.0.0.2
Next-Hop is automatic
MultiHop Status - disabled
Send-Community is standard,extended
```

3.24. Enabling BFD Monitoring for BGP Neighbors

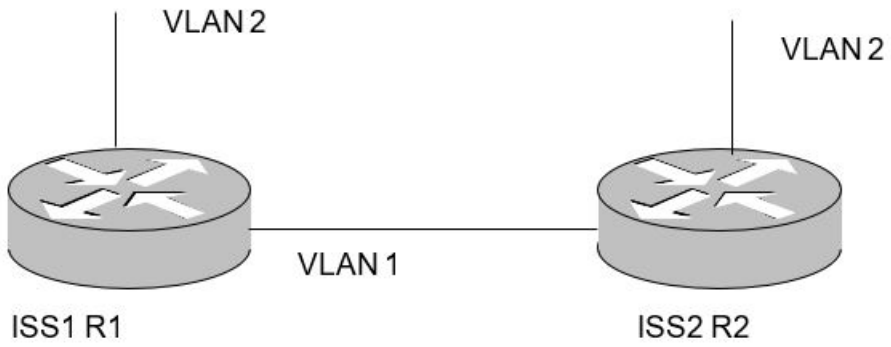
CONTEXT:

By default, Bidirectional Forwarding Detection (*BFD*) monitoring is disabled for the *BGP* peers. When *BFD* monitoring is enabled, *BGP* registers with *BFD* for monitoring the particular neighbor path after the BGP session becomes ESTABLISHED.

When *BFD* detects the path failure, it informs *BGP* about the path status change.

The figure shown below depicts the topology setup used for this configuration.

Figure 25: BGP Configuration and Testing Topology



1. To enable *BGP* in Router R1:

   FOR EXAMPLE: Execute the following commands:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

– Enable *BGP* in R1.

```
iS5comm(config)# router bgp 100
```

– Configure R2 (with as-num 200) as external peer in R1.

```
iS5comm(config-router)# neighbor 12.0.0.2 remote-as 100.2
```

– Configure *BFD* monitoring for the peer R2.

```
iS5comm(config-router)# neighbor 12.0.0.2 fall-over bfd
```

2. To enable *BGP* in Router R2:

FOR EXAMPLE: Execute the following commands:

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Enable *BGP* in R2 (assigning a 4 byte *ASN*).

```
iS5comm(config)# router bgp 100.2
```

– Configure R1 (with as-num 100) as external peer in R2.

```
iS5comm(config-router)# neighbor 12.0.0.1 remote-as 100
```

– Configure *BFD* monitoring for the peer R1.

```
iS5comm(config-router)# neighbor 12.0.0.1 fall-over bfd
```

3. R1: View the output using the show command mentioned below.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp neighbor
Context Name : default
-------------
BGP router identifier is 12.0.0.2, remote AS 200, external linkBGP
version 4, remote router ID 12.0.0.2
Network Address: None
BGP state = Established, up for 7 seconds, un-authenticated session
Configured BGP Maximum Prefix Limit 5000
AutomaticStart DISABLED
AutomaticStop DISABLED
DampPeer Oscillations DISABLED
DelayOpen DISABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Default-originate : DISABLED
Peer Passive : DISABLED
Peer Status : NOT DAMPED
GateWay Address : NONE
```

```
Rcvd update before 5 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
4-byte ASN: Advertised and received
Address family IPv4 Unicast: Advertised and received
AF-dependant capabilities:
Outbound Route Filter (ORF) type : (64) Address Prefix based ORF
Send-mode : not supported
Receive-mode : not supported
BFD Monitoring : Enabled
Received 3 messages, 1 Updates
Sent 3 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
Connections established 1 time(s)
Graceful Restart Capability: advertised and received
Remote Restart timer is 90
Local host: 12.0.0.1, Local port: 179
Foreign host: 12.0.0.2, Foreign port: 52696
Last Error: Code 0, SubCode 0.
Update Source 12.0.0.1
Next-Hop is automatic
MultiHop Status - disabled
Send-Community is standard,extended
```

4. R2: View the output using the show command mentioned below.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip bgp neighbor
Context Name : default
-------------
BGP router identifier is 12.0.0.1, remote AS 100, external linkBGP
version 4, remote router ID 12.0.0.1
Network Address: None
BGP state = Established, up for 2 minutes 10 seconds, un-authenticated
session
Configured BGP Maximum Prefix Limit 5000
AutomaticStart DISABLED
AutomaticStop DISABLED
DampPeer Oscillations DISABLED
```

```
DelayOpen DISABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Default-originate : DISABLED
Peer Passive : DISABLED
Peer Status : NOT DAMPED
GateWay Address : NONE
Rcvd update before 5 secs, hold time is 90, keepalive interval is 30
secs
Neighbors Capability:
Route-Refresh: Advertised and received
4-byte ASN: Advertised and received
Address family IPv4 Unicast: Advertised and received
AF-dependant capabilities:
Outbound Route Filter (ORF) type : (64) Address Prefix based ORF
Send-mode : not supported
Receive-mode : not supported
BFD Monitoring : Enabled
Received 7 messages, 1 Updates
Sent 7 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
Connections established 1 time(s)
Graceful Restart Capability: advertised and received
Remote Restart timer is 90
Local host: 12.0.0.2, Local port: 52696
Foreign host: 12.0.0.1, Foreign port: 179
Last Error: Code 0, SubCode 0.
Update Source 12.0.0.1
Next-Hop is automatic
MultiHop Status - disabled
Send-Community is standard,extended
```

Index