iBiome - OSPF User Guide

RAPTOR™

Intelligent Cyber Secure Platform

Version: 1.10.06-1, Date: January 2022

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.

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)

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

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

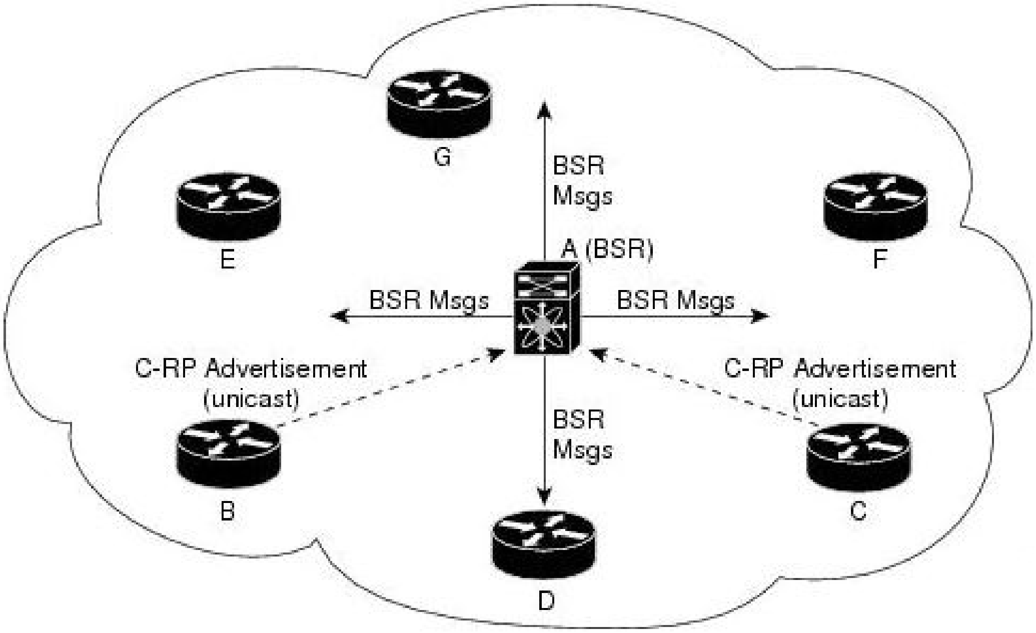
Berkeley Software Distribution (BSD)

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

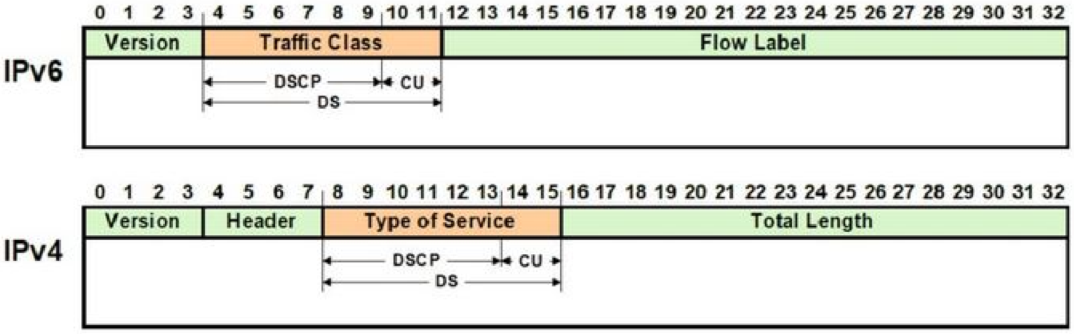
Dot1x Authentication is enabled when dot1x system-auth-control is enabled, and aaa authentication dot1x default is local. If you enable authentication on a port by using the default setting of dot1x port-control, which is force-authorized, it disables 802.1X authentication and causes the port to transition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

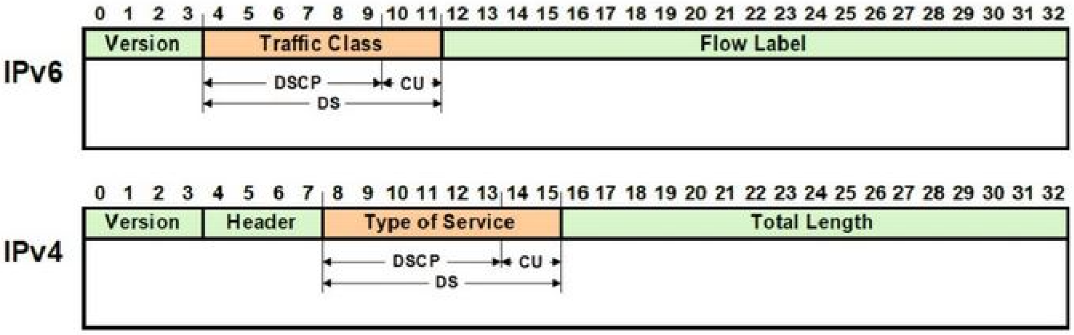
Differentiated Services (DS).



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)

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)

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).

HTTP

Hyper Text Transfer Protocol (HTTP)

HTTPS

Hyper Text Transfer Protocol Secure (HTTPS)

IANA

Internet Assigned Numbers Authority (IANA)

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).

L2GP

Layer 2 Gateway Port (L2GP)

LA

Link Aggregation

LACP

Link Aggregation Control Protocol

LAG

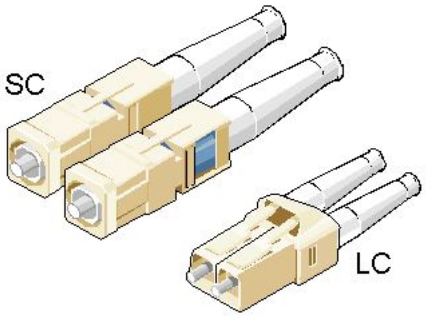
Link Aggregation Group

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)

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

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.

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.

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.

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

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.[16]-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)

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

Random early detection (RED) is where a single queue may have several different sets of queue thresholds.

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

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.

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

TFTP

Trivial File Transfer Protocol

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

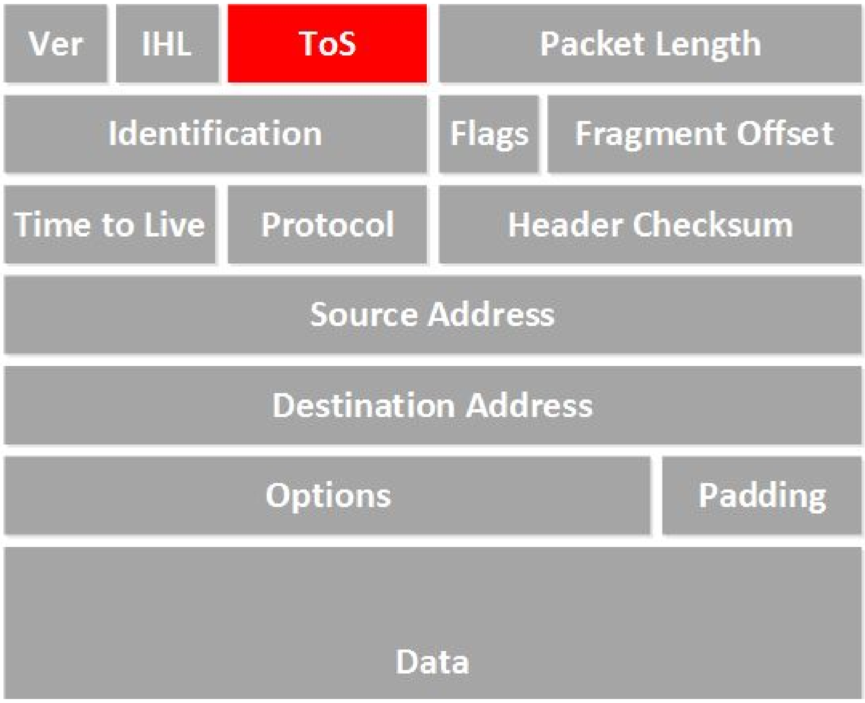
type, length, and value (TLV) traces

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

OSPF (Open Shortest Path First) protocol is an Interior Gateway Protocol used to distribute routing information within a single autonomous system. Routers use link-state algorithms to send routing information to all nodes in an inter-network by calculating the shortest path to each node based on topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations), which describes the state of its own links, and it also sends the complete routing structure (topography).

OSPF uses an *LSDB* (link state database) and fills this with *LSA*s (link state advertisement). Instead of using 1 LSA packet, OSPF has many different types of *LSA*s. The *LSA* types are as follows:

- LSA Type 1: Router *LSA*
- LSA Type 2: Network *LSA*
- LSA Type 3: Summary *LSA*
- LSA Type 4: Summary *ASBR*
- LSA Type 5: Autonomous system external *LSA*
- LSA Type 6: Multicast *OSPF LSA*
- LSA Type 7: Not-so-stubby area *LSA*
- LSA Type 8: External attribute *LSA* for *BGP*
- LSA Type 9, 10, and 11: Opaque *LSA* (used directly by *OSPF*)

Opaque *LSA*s consist of a standard LSA header followed by a 32-bit aligned application-specific information field. As other *LSA*, the Opaque LSA uses the *LSDB* distribution mechanism for flooding this information throughout the topology. For details, see RFC 2370.

A separation of control and forwarding functions creates the possibility of maintaining a router's data forwarding capability, while the router's control software is restarted/reloaded. We call such a possibility "graceful restart".

A router attempting a graceful restart originates link-local Opaque- *LSA*s (aka Grace- *LSA*s), announcing its intention to perform a graceful restart within a specified amount of time or "grace period". The Grace-*LSA*'s Age field is set to 0, and the requested grace period (in seconds) is inserted into the body of the Grace-*LSA*. During the grace period, its neighbors continue to announce the restarting router in their *LSA*s as if it were fully adjacent (i.e., OSPF neighbor state Full), but only if the network topology remains static (i.e., the contents of the *LSA*s in the *LSDB* with LS types 1-5,7 remain unchanged; periodic refreshes are allowed).

There are two roles being played by *OSPF* routers during graceful restart. First, there is a router that is being restarted. Then, there are the router's neighbors that must cooperate for the restart to be graceful. During graceful restart, such neighbors are running in "helper mode". For more details, refer to RFC 3623.

The advantage of shortest path first algorithms is that they result in smaller more frequent updates everywhere. They converge quickly, thus preventing such problems as routing loops and count-to-infinity (when routers continuously increment the hop count to a particular network). This ensures a stable network.

Before configuring *OSPF*, Route Redistribution (*RRD*) must be enabled. In addition, all *OSPF* interface related configurations, can be done only when the global *OSPF* is enabled.

1.1. Purpose and Scope

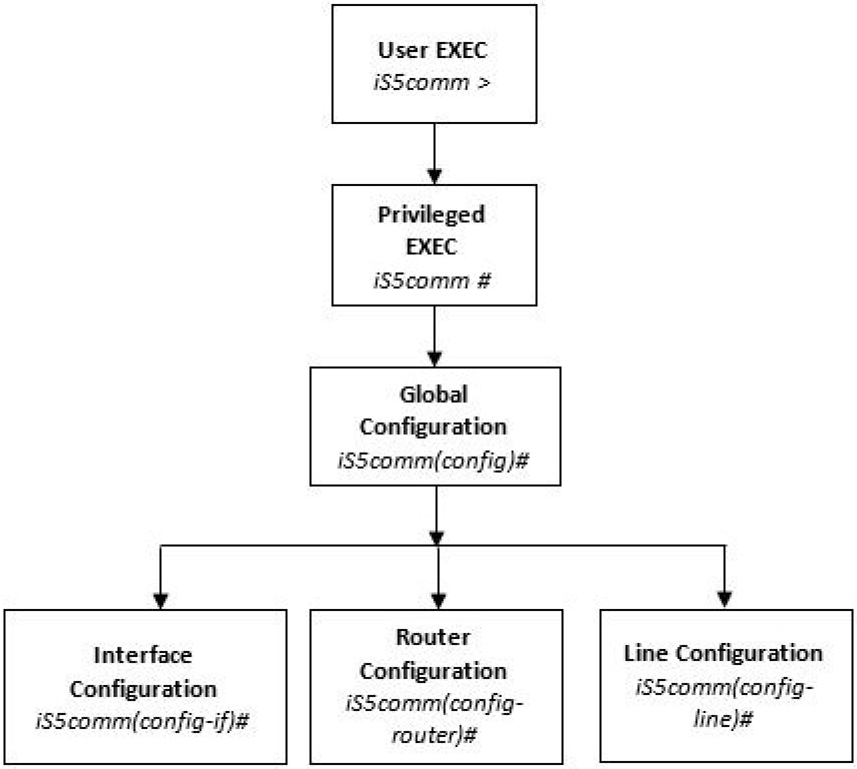
This document describes the basic and advanced configuration tasks of iS5Com's *OSPF*. The reader is expected to have a basic knowledge of the protocol as a prerequisite.

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

User Exec Mode

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

Privileged Exec Mode

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

Global Configuration Mode

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

Interface Configuration Mode

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

Port Channel Interface Configuration

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

VLAN Interface Configuration Mode

Prompt	Access method	Exit Method
`iS5comm(config-if)#`	The Global Configuration mode command `interface vlan <vlan id>` is used to enter the 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

2. Protocol Description

iS5Com's Open Shortest Path First (*OSPF*) is a routing protocol for Internet Protocol (*IP*) networks. It uses a link state routing (*LSR*) algorithm and falls into the group of interior gateway protocols (*IGP*s), operating within a single autonomous system (*AS*).

CONFIGURING OSPF

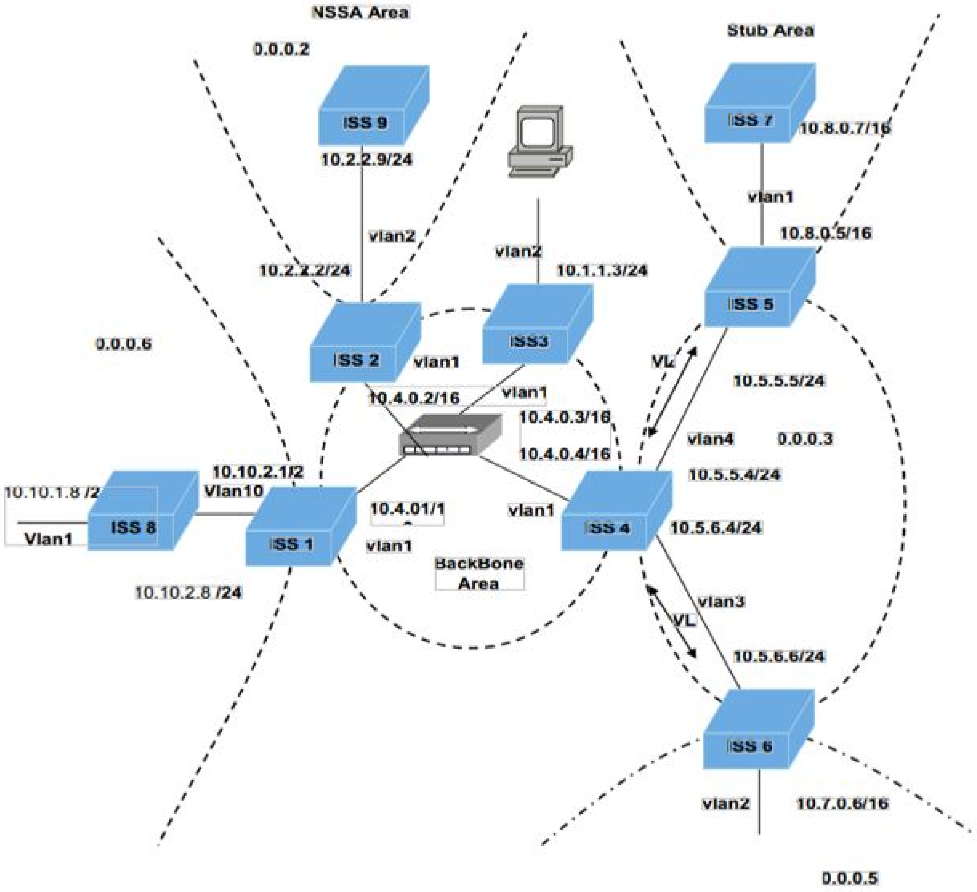
3. Configuring OSPF

The following sections describe the configuration of iS5 Communications *OSPF* running as a part of iS5 Communications *ISS*.

3.1. Configuration Topology

The Topology for testing iS5's *OSPF* is as follows:

Figure 1: Topology for Testing iS5 OSPF



3.2. Configuration Guidelines (Prerequisites)

For setup, refer to Figure Topology for Testing iS5 *OSPF*.

Configuration in ISS1

1. Configuration of *VLAN* Interfaces (*VLAN* 1 and *VLAN* 10)

   FOR EXAMPLE: Execute the following commands

```
iS5comm# configure terminal
iS5comm(config)# set gvrp disable
iS5comm(config)# set gmrp disable
iS5comm(config)# interface vlan 1
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 10.4.0.1 255.255.0.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 1
iS5comm(config-vlan)# ports gigabitethernet 0/1 untagged gigabitethernet 0/1
iS5comm(config-vlan)# exit
iS5comm(config)# interface vlan 10
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 10.10.2.1 255.255.255.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 10
iS5comm(config-vlan)# ports gigabitethernet 0/10 untagged gigabitethernet 0/10
iS5comm(config-vlan)# exit
iS5comm(config)# interface gigabitethernet 0/10
iS5comm(config-if)# switchport pvid 10
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
```

Configuration in ISS2

1. Configuration of *VLAN* Interfaces (*VLAN* 1and *VLAN* 2)

   FOR EXAMPLE: Execute the following commands

```
iS5comm# configure terminal
```

```
iS5comm(config)# set gvrp disable
iS5comm(config)# set gmrp disable
iS5comm(config)# interface vlan 1
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 10.4.0.2 255.255.0.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 1
iS5comm(config-vlan)# ports gigabitethernet 0/1 untagged gigabitethernet 0/1
iS5comm(config-vlan)# exit
iS5comm(config)# interface vlan 2
iS5comm(config-if)# ip address 10.2.2.2 255.255.255.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 2
iS5comm(config-vlan)# ports gigabitethernet 0/2 untagged gigabitethernet 0/2
iS5comm(config-vlan)# exit
iS5comm(config)# interface gigabitethernet 0/2
iS5comm(config-if)# no shutdown
iS5comm(config-if)# switchport pvid 2
iS5comm(config-if)# exit
```

Configuration in ISS3

1. Configuration of *VLAN* Interfaces (*VLAN* 1 and *VLAN* 2)

   FOR EXAMPLE: Execute the following commands

```
iS5comm# configure terminal
iS5comm(config)# set gvrp disable
iS5comm(config)# set gmrp disable
iS5comm(config)# interface vlan 1
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 10.4.0.3 255.255.0.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 1
iS5comm(config-vlan)# ports gigabitethernet 0/1 untagged gigabitethernet 0/1
```

```
iS5comm(config-vlan)# exit
iS5comm(config)# interface vlan 2
iS5comm(config-if)# ip address 10.1.1.3 255.255.255.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 2
iS5comm(config-vlan)# ports gigabitethernet 0/2 untagged gigabitethernet 0/2
iS5comm(config-vlan)# exit
iS5comm(config)# interface gigabitethernet 0/2
iS5comm(config-if)# no shutdown
iS5comm(config-if)# switchport pvid 2
iS5comm(config-if)# exit
```

Configuration in ISS4

1. Configuration of VLAN Interfaces (VLAN 1, VLAN 3, and VLAN 4)

   FOR EXAMPLE: Execute the following commands

```
iS5comm# configure terminal
iS5comm(config)# set gvrp disable
iS5comm(config)# set gmrp disable
iS5comm(config)# interface vlan 1
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 10.4.0.4 255.255.0.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 1
iS5comm(config-vlan)# ports gigabitethernet 0/1 untagged gigabitethernet 0/1
iS5comm(config-vlan)# exit
iS5comm(config)# interface vlan 3
iS5comm(config-if)# ip address 10.5.6.4 255.255.255.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 3
iS5comm(config-vlan)# ports gigabitethernet 0/3 untagged gigabitethernet 0/3
iS5comm(config-vlan)# exit
iS5comm(config)# interface gigabitethernet 0/3
```

```
iS5comm(config-if)# no shutdown
iS5comm(config-if)# switchport pvid 3
iS5comm(config-if)# exit
iS5comm(config)# interface vlan 4
iS5comm(config-if)# ip address 10.5.5.4 255.255.255.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 4
iS5comm(config-vlan)# ports gigabitethernet 0/4 untagged gigabitethernet 0/4
iS5comm(config-vlan)# exit
iS5comm(config)# interface gigabitethernet 0/4
iS5comm(config-if)# no shutdown
iS5comm(config-if)# switchport pvid 4
iS5comm(config-if)# exit
```

Configuration in ISS5

1. Configuration of *VLAN* Interfaces (*VLAN* 1 and *VLAN* 4)

   FOR EXAMPLE: Execute the following commands

```
iS5comm# configure terminal
iS5comm(config)# set gvrp disable
iS5comm(config)# set gmrp disable
iS5comm(config)# interface vlan 1
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 10.8.0.5 255.255.0.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 1
iS5comm(config-vlan)# ports gigabitethernet 0/1 untagged gigabitethernet 0/1
iS5comm(config-vlan)# exit
iS5comm(config)# interface vlan 4
iS5comm(config-if)# ip address 10.5.5.5 255.255.255.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 4
iS5comm(config-vlan)# ports gigabitethernet 0/4 untagged gigabitethernet 0/4
```

```
iS5comm(config-vlan)# exit
iS5comm(config)# interface gigabitethernet 0/4
iS5comm(config-if)# no shutdown
iS5comm(config-if)# switchport pvid 4
iS5comm(config-if)# exit
```

Configuration in ISS6

1. Configuration of *VLAN* Interfaces (*VLAN* 1 and *VLAN* 3)

   FOR EXAMPLE: Execute the following commands

```
iS5comm# configure terminal
iS5comm(config)# set gvrp disable
iS5comm(config)# set gmrp disable
iS5comm(config)# interface vlan 1
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 10.7.0.6 255.255.0.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 1
iS5comm(config-vlan)# ports gigabitethernet 0/1 untagged gigabitethernet 0/1
iS5comm(config-vlan)# exit
iS5comm(config)# interface vlan 3
iS5comm(config-if)# ip address 10.5.6.6 255.255.255.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 3
iS5comm(config-vlan)# ports gigabitethernet 0/3 untagged gigabitethernet 0/3
iS5comm(config-vlan)# exit
iS5comm(config)# interface gigabitethernet 0/3
iS5comm(config-if)# no shutdown
iS5comm(config-if)# switchport pvid 3
iS5comm(config-if)# exit
```

Configuration in ISS7

1. Configuration of *VLAN* Interface (*VLAN* 1)

   FOR EXAMPLE: Execute the following commands

```
iS5comm# configure terminal
iS5comm(config)# set gvrp disable
iS5comm(config)# set gmrp disable
iS5comm(config)# interface vlan 1
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 10.8.0.7 255.255.0.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 1
iS5comm(config-vlan)# ports gigabitethernet 0/1 untagged gigabitethernet 0/1
iS5comm(config-if)# exit
```

Configuration in ISS8

1. Configuration of *VLAN* Interfaces (*VLAN* 1 and *VLAN* 10)

   FOR EXAMPLE: Execute the following commands

```
iS5comm# configure terminal
iS5comm(config)# set gvrp disable
iS5comm(config)# set gmrp disable
iS5comm(config)# interface vlan 10
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 10.10.2.8 255.255.255.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 10
iS5comm(config-vlan)# ports gigabitethernet 0/10 untagged gigabitethernet 0/10
iS5comm(config-vlan)# exit
iS5comm(config)# interface gigabitethernet 0/10
iS5comm(config-if)# switchport pvid 10
iS5comm(config-if)# no shutdown iS5comm(config-if)# exit
iS5comm(config)# interface vlan 1
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 10.10.1.8 255.255.255.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 1
```

```
iS5comm(config-vlan)# ports gigabitethernet 0/1 untagged gigabitethernet 0/1
iS5comm(config-vlan)# exit
iS5comm(config)# interface gigabitethernet 0/1
iS5comm(config-if)# switchport pvid 1
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
```

Configuration in ISS9

1. Configuration of *VLAN* Interfaces (*VLAN* 2)

   FOR EXAMPLE: Execute the following commands

```
iS5comm# configure terminal
iS5comm(config)# set gvrp disable
iS5comm(config)# set gmrp disable
iS5comm(config)# interface vlan 2
iS5comm(config-if)# shutdown
iS5comm(config-if)# ip address 10.2.2.9 255.255.255.0
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# vlan 2
iS5comm(config-vlan)# ports gigabitethernet 0/2 untagged gigabitethernet 0/2
iS5comm(config-vlan)# exit
iS5comm(config)# interface gigabitethernet 0/2
iS5comm(config-if)# switchport pvid 2
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
```

3.3. Default Configuration

The default *OSPF* configuration is as follows.

Feature	Default Setting
Stability interval	40
translation-role	candidate
compatible rfc1583	Enabled
abr-type	standard

Feature	Default Setting
neighbor priority	1
area default-cost	10
area tos	0
area metric	10
area - metric-type	1
area - tos	0
default-information originate always metric	10
default-information originate always metric metric-type	2
Authentication	no authentication
hello-interval	10
retransmit-interval	5
transmit-delay	1
dead-interval	40
tag	2
summary-address	advertise
translation	disabled
redist-config metric-value	10
redist-config metric-type	asExttype2
redist-config tag	manual
nssa asbr-default-route translator	disable

3.4. Enabling / Disabling OSPF

Enabling *OSPF* takes the user to the Router Configuration Mode from which the router related commands are executed. Disabling *OSPF* terminates the *OSPF* process.

1. To enable *OSPF*, execute the following commands.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

– Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

– This command takes the user to the Router Configuration Mode.

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

FOR EXAMPLE: **NOTE:** Disable *OSPF* globally in the switch ISS1 by executing the following command.

```
iS5comm(config)# no router ospf
```

3.5. Configuring OSPF Interface

Enabling *OSPF* takes the user to the Router Configuration Mode from which the router related commands are executed. Disabling *OSPF* terminates the *OSPF* process.

1. To enable *OSPF*, execute the following commands.

FOR EXAMPLE: Type the following:

– Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

– Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

– Enable *OSPF* over the *VLAN* interface and associate the interface with an *OSPF* area. *VLAN* interfaces *VLAN*1 and *VLAN*10 are created as a part of the prerequisite configuration.

```
iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
iS5comm(config-router)# exit
```

NOTE: Enabling *OSPF* over the *VLAN* interfaces defines the interfaces on which OSPF runs and the area ID for those interfaces.

NOTE: When *OSPF* routing is enabled using the “network” command, an established session is properly mapped with the interface only if the interface administrative status is up. This is because to enable *OSPF* in an interface, both *IP* address and interface index are used.

2. View the configuration details by executing the following show command.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf
OSPF Router ID 10.10.2.1
Supports only single TOS(TOS0) route
ABR Type supported is Standard ABR
It is an Area Border Router
Number of Areas in this router is 2
Area is 0.0.0.6
Number of interfaces in this area is 1
SPF algorithm executed 6 times
Area is 0.0.0.0
```

```
Number of interfaces in this area is 1
```

3. View the configuration details by executing the following show command.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf interface
vlan1 is line protocol is up
Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0AS 1, Router ID
10.10.2.1, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State 4, Priority 1 Designated RouterId
10.10.2.1, Interface address 10.4.0.1
Backup Designated RouterId 10.4.0.4, Interface address 10.4.0.4
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 8 sec

Neighbor Count is 3, Adjacent neighbor count is 3 Adjacent with the
neighbor 10.4.0.4
Adjacent with the neighbor 10.4.0.3
Adjacent with the neighbor 10.4.0.2
vlan10 line protocol is up
Internet Address 10.10.2.1, Mask 255.255.255.0, Area0.0.0.6

AS 1, Router ID 10.10.2.1, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State 4, Priority 1 Designated RouterId
10.10.2.1, Interface address
10.10.2.1
Backup Designated RouterId 10.10.1.8, Interface address 10.10.2.8
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 6 sec
Neighbor Count is 1, Adjacent neighbor count is 1 Adjacent with the
neighbor 10.10.1.8 OSPF Router ID
10.10.2.1
```

4. Execute the “no” form of the command to disable *OSPF* routing for all defined interfaces and to remove the area ID of the interface.

   FOR EXAMPLE: Type the following:

```
iS5comm(config-router)# no network 10.4.0.1 area 0.0.0.0
```

3.6. Configuring OSPF Interface Parameters

Configuration of the *OSPF* Interface parameters are described in the following sub-sections. The interface parameters are configured in the Interface Configuration mode.

1. To enable *OSPF*, execute the following commands.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

   – Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

   – Enable *OSPF* over the *VLAN* interface and associate the interface with an *OSPF* area. *VLAN* interfaces *VLAN*1 and *VLAN*10 are created as a part of the prerequisite configuration.

```
iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
iS5comm(config-router)# exit
```

NOTE: When *OSPF* routing is enabled using the “network” command, an established session is properly mapped with the interface only if the interface administrative status is up. This is because to enable *OSPF* in an interface, both *IP* address and interface index are used.

   – Enter the Interface Configuration Mode.

```
iS5comm(config)# interface vlan 1
iS5comm(config-if)#
```

Configuring OSPF Interface Priority

Configuring *LSA* (link-state advertisement) retransmission Interval specifies the time interval between the *LSA* retransmissions.

1. Execute the following command to configure the *VLAN* 1 retransmit- interval as 10 seconds.

   FOR EXAMPLE: Type the following:

```
iS5comm(config-if)# ip ospf ip ospf retransmit-interval 10
```

2. View the configuration details by executing the following show command.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf interface vlan 1
vlan1 is line protocol is up
Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0
AS 1, Router ID 10.10.2.1, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State 4, Priority 10
Designated RouterId 10.10.2.1, Interface address 10.4.0.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 4 sec
```

```
Neighbor Count is 0, Adjacent neighbor count is 0
```

NOTE: A priority value of 0 signifies that the router is not eligible to become the designated router on a particular network.

NOTE: The default interface priority value is 1.

3. Restore the default value of the *OSPF* Interface by executing the following command.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm(config-if)# no ip ospf priority
   ```

Configuring LSA Retransmission Interval

Configuring *OSPF* Interface Priority sets the interface priority of the router, which helps to determine the designated router for the link connected to the interface.

1. Execute the following command to configure the *VLAN* 1 interface priority as 10.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm(config-if)# ip ospf priority 10
   ```

2. View the configuration details by executing the following show command.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf interface vlan 1
   vlan1 is line protocol is up
   Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0
   AS 1, Router ID 10.10.2.1, Network Type BROADCAST, Cost 1
   Transmit Delay is 1 sec, State 4, Priority 10
   Designated RouterId 10.10.2.1, Interface address 10.4.0.1
   No backup designated router on this network
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 10
   Hello due in 4 sec
   Neighbor Count is 0, Adjacent neighbor count is 0
   ```

3. Restore the default value of the *OSPF* Interface by executing the following command.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm(config-if)# no ip ospf retransmit-interval
   ```

Configuring Link State Update Packet Transmission Delay

Configuring link state update packet transmission delay sets the estimated time required to transmit a link state update packet on the interface.

1. Execute the following command to configure the *VLAN* 1 transmission delay.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm(config-if)# ip ospf transmit-delay 5
   ```

2. View the configuration details by executing the following show command.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf interface vlan 1
vlan1 is line protocol is up
Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0
AS 1, Router ID 10.10.2.1, Network Type BROADCAST, Cost 1
Transmit Delay is 5 sec, State 4, Priority 10
Designated RouterId 10.10.2.1, Interface address 10.4.0.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 4 sec
Neighbor Count is 0, Adjacent neighbor count is 0
```

3. Restore the default value of the *OSPF* Interface by executing the following command.

   FOR EXAMPLE: Type the following:

   iS5comm(config-if)# no ip ospf transmit-delay

Configuring Hello-Interval

Configuring “hello interval” specifies the interval between hello packets sent on the interface.

1. Execute the following command to configure the *VLAN* 1 hello interval as 40 seconds.

   FOR EXAMPLE: Type the following:

```
iS5comm(config-if)# ip ospf hello-interval 40
```

2. View the configuration details by executing the following show command.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf interface vlan 1
vlan1 is line protocol is up
Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0
AS 1, Router ID 10.10.2.1, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State 4, Priority 10
Designated RouterId 10.10.2.1, Interface address 10.4.0.1
No backup designated router on this network
Timer intervals configured, Hello 40, Dead 40, Wait 40, Retransmit 5
Hello due in 4 sec
Neighbor Count is 0, Adjacent neighbor count is 0
```

3. Restore the default value of the *OSPF* Interface by executing the following command.

   FOR EXAMPLE: Type the following:

   iS5comm(config-if)# no ip ospf hello-interval

Configuring OSPF Dead-Interval

Configuring dead-interval sets the interval at which hello packets must not be seen before the neighbors declare the router down.

1. Execute the following command to configure the *VLAN* 1 dead-interval as 120 seconds.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm(config-if)# ip ospf dead-interval 120
   ```

2. View the configuration details by executing the following show command.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf interface vlan 1
   vlan1 is line protocol is up
   Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0
   AS 1, Router ID 10.10.2.1, Network Type BROADCAST, Cost 1
   Transmit Delay is 1 sec, State 4, Priority 10
   Designated RouterId 10.10.2.1, Interface address 10.4.0.1
   No backup designated router on this network
   Timer intervals configured, Hello 10, Dead 120, Wait 40, Retransmit 5
   Hello due in 4 sec
   Neighbor Count is 0, Adjacent neighbor count is 0
   ```

3. Restore the default value of the OSPF Interface by executing the following command.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm(config-if)# no ip ospf dead-interval
   ```

Configuring Network Type

The *OSPF* network type can be broadcast, non-broadcast, point-to-multipoint or point-to-point. The default type is broadcast. The *OSPF* network type can be configured to a type other than the default for a given media.

1. Execute the following command to configure the *VLAN* 1 network type as point-to-point.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm(config-if)# ip ospf network point-to-point
   ```

2. View the configuration details by executing the following show command.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf interface vlan 1
   vlan1 is line protocol is up
   Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0
   AS 1, Router ID 10.10.2.1, Network Type PointToPoint, Cost 1
   Transmit Delay is 1 sec, State 4, Priority 10
   Designated RouterId 10.10.2.1, Interface address 10.4.0.1
   ```

```
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 4 sec
Neighbor Count is 0, Adjacent neighbor count is 0
```

3. Restore the default value of the *OSPF* Interface by executing the following command.

   FOR EXAMPLE: Type the following:

   iS5comm(config-if)# no ip ospf network

Configuring Demand Circuit

When an *OSPF* link is configured as demand circuit, *OSPF* Hellos are suppressed and periodic LSA refreshes are not flooded over the link. These packets bring up the link only when they are exchanged for the first time, or when a change occurs in the information they contain. This allows the underlying Data Link Layer to be closed when the network topology is stable.

1. Execute the following command to configure the *VLAN* 1 as *OSPF* demand circuit.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm(config-if)# ip ospf demand-circuit
   ```

2. View the configuration details by executing the following show command.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf interface vlan 1
   vlan1 is line protocol is up
   Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0
   AS 1, Router ID 10.10.2.1, Network Type BROADCAST, Cost 1
   Configured as demand circuit.
   Run as demand
   Transmit Delay is 1 sec, State 4, Priority 10
   Designated RouterId 10.10.2.1, Interface address 10.4.0.1
   No backup designated router on this network
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 4 sec
   Neighbor Count is 0, Adjacent neighbor count is 0
   ```

3. Restore the default value of the *OSPF* Interface by executing the following command.

   FOR EXAMPLE: Type the following:

   iS5comm(config-if)# no ip ospf demand-circuit

Configuring Interface Cost

Configuring Interface Cost specifies the cost of sending a packet on an interface.

1. Execute the following command to configure the *VLAN* 1 interface cost as 20.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm(config-if)# ip ospf cost 20
   ```

2. View the configuration details by executing the following show command.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf interface vlan 1
   vlan1 is line protocol is up
   Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0
   AS 1, Router ID 10.10.2.1, Network Type BROADCAST, Cost 20
   Transmit Delay is 1 sec, State 4, Priority 10
   Designated RouterId 10.10.2.1, Interface address 10.4.0.1
   No backup designated router on this network
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 4 sec
   Neighbor Count is 0, Adjacent neighbor count is 0
   ```

3. Restore the default value of the *OSPF* Interface by executing the following command.

   FOR EXAMPLE: Type the following:

   iS5comm(config-if)# no ip ospf cost

3.7. Configuring OSPF Authentication

The authentication type for *OSPF* can be configured as Simple Password Authentication, Message-Digest Authentication, or Null Authentication. Authentication related configuration are done in Interface Configuration mode. The following sections describe the configuration of *OSPF* authentication.

1. For the configuration of *OSPF* Authentication, execute the following commands.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch ISS1.

   ```
   iS5comm(config)# router ospf
   ```

   – Enable *OSPF* over the *VLAN* interface and associate the interface with an *OSPF* area. *VLAN* interfaces *VLAN*1 and *VLAN*10 are created as a part of the prerequisite configuration.

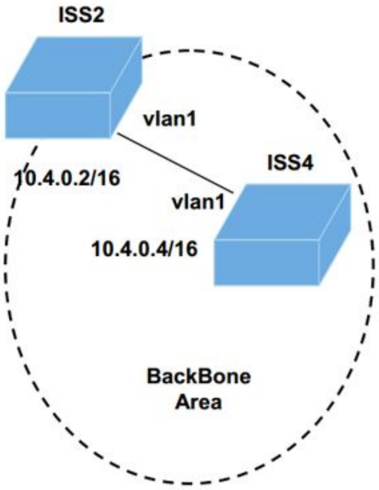
   ```
   iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
   iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
   iS5comm(config-router)# exit
   ```

– Enter the Interface Configuration Mode.

```
iS5comm(config)# interface vlan 1
iS5comm(config-if)#
```

A sample configuration for testing authentication is as follows.

Figure 2: Topology for Testing Authentication



Some prerequisite configuration (refer to Configuration Guidelines (Prerequisite) Section) must be done in the switches ISS2 & ISS4 before configuring *OSPF*.

Configuring Simple Password Authentication

For simple password authentication, a password must be specified which is to be used by the neighboring routers using the *OSPF* simple password authentication.

1. Execute the following commands in ISS2 and ISS4.

FOR EXAMPLE: Type the following:

Configuration in ISS2

– Enter the Global Configuration Mode in ISS2.

```
iS5comm# configure terminal
```

– Enable *OSPF* globally in the switch ISS2.

```
iS5comm(config)# router ospf
```

– Enable *OSPF* over the *VLAN* interface and associate the interface with an *OSPF* area. *VLAN* interfaces *VLAN*1 and *VLAN*10 are created as a part of the prerequisite configuration.

```
iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
```

NOTE: When *OSPF* routing is enabled using the “network” command, the established session is properly mapped with the interface only if the interface administrative status is up. This is because to enable *OSPF* in an interface, both *IP* address and interface index are used.

– Exit from the Router Configuration Mode.

iS5comm(config-router)# exit

– Enter the Interface Configuration mode.

```
iS5comm(config)# interface vlan 1
```

– Configure the authentication key for simple password authentication.

```
iS5comm(config-if)# ip ospf authentication-key 1234
```

– Enable simple password authentication.

```
iS5comm(config-if)# ip ospf authentication
```

– Exit from the Interface Configuration mode.

```
iS5comm(config-if)# end
```

Configuration in ISS4

– Enter the Global Configuration Mode in ISS4.

```
iS5comm# configure terminal
```

– Enable *OSPF* globally in the switch ISS4.

```
iS5comm(config)# router ospf
```

– Enable *OSPF* over the *VLAN* interface and associate the interface with an *OSPF* area. *VLAN* interfaces *VLAN*1 and *VLAN*10 are created as a part of the prerequisite configuration.

```
iS5comm(config-router)# network 10.4.0.4 area 0.0.0.0
```

NOTE: When *OSPF* routing is enabled using the “network” command, the established session is properly mapped with the interface only if the interface administrative status is up. This is because to enable *OSPF* in an interface, both *IP* address and interface index are used.

– Exit from the Router Configuration Mode.

iS5comm(config-router)# exit

– Enter the Interface Configuration mode.

```
iS5comm(config)# interface vlan 1
```

– Configure the authentication key for simple password authentication.

```
iS5comm(config-if)# ip ospf authentication-key 1234
```

– Enable simple password authentication.

```
iS5comm(config-if)# ip ospf authentication
```

– Exit from the Interface Configuration mode.

```
iS5comm(config-if)# end
```

2. View the configuration details by executing the following show command.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf interface
vlan1 is line protocol is up
Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0
AS 1, Router ID ID 10.4.0.2, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State 5, Priority 1
Designated RouterId 10.4.0.4, Interface address 10.4.0.4
Backup Designated RouterId 10.4.0.2, Interface address 10.4.0.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0 sec
```

```
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with the neighbor 10.4.0.4
Simple password authentication enabled
```

3. View the adjacency formed between the neighbors (ISS 2 and ISS 4) by executing the following command. *BDR* stands for Backup Designated Router.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf neighbor detail
Neighbor 10.4.0.4, interface address 10.4.0.4
In the area 0.0.0.0 via interface vlan1
Neighbor priority is 1,State is FULL/BACKUP, 5 state changes
DR is 10.4.0.4 BDR is 10.4.0.2
Options is 0x2
```

4. Remove a previously assigned *OSPF* password by executing the following command.

   FOR EXAMPLE: Type the following:

   iS5comm(config-if)# no ip ospf authentication-key

Configuring Message-Digest Authentication

Message-Digest Authentication is a cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the *OSPF* packet, the key, and the key-id to generate a “message-digest” that appends to the packet.

1. Execute the following commands to configure the message-digest authentication.

   FOR EXAMPLE: Type the following:

   Configuration in ISS2

   – Enter the Global Configuration Mode in ISS2.

```
iS5comm# configure terminal
```

   – Enter the Interface Configuration Mode.

```
iS5comm(config)# interface vlan 1
```

   – Delete the authentication key for simple password authentication.

```
iS5comm(config-if)# no ip ospf authentication-key
```

   – Configure the authentication key for the message-digest authentication.

```
iS5comm(config-if)# ip ospf message-digest-key 0 md5 asdf
```

   – Exit from the Interface Configuration Mode.

```
iS5comm(config-if)# end
```

   Configuration in ISS4

   – Enter the Global Configuration Mode in ISS2.

```
iS5comm# configure terminal
```

   – Enter the Interface Configuration Mode.

```
iS5comm(config)# interface vlan 1
```

– Delete the authentication key for simple password authentication.

```
iS5comm(config-if)# no ip ospf authentication-key
```

– Configure the authentication key for the message-digest authentication.

```
iS5comm(config-if)# ip ospf message-digest-key 0 md5 asdf
```

– Exit from the Interface Configuration Mode.

```
iS5comm(config-if)# end
```

2. View the configuration details by executing the following show command.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf interface
vlan1 is line protocol is up
Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0
AS 1, Router ID ID 10.4.0.2, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State 5, Priority 1
Designated RouterId 10.4.0.4, Interface address 10.4.0.4
Backup Designated RouterId 10.4.0.2, Interface address 10.4.0.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0 sec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with the neighbor 10.4.0.4
Message duest authentication enabled
```

3. View the adjacency formed between the neighbors (ISS2 and ISS4) by executing the following command. *BDR* stands for Backup Designated Router.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf neighbor detail
Neighbor 10.4.0.4, interface address 10.4.0.4
In the area 0.0.0.0 via interface vlan1
Neighbor priority is 1,State is FULL/BACKUP, 5 state changes
DR is 10.4.0.4 BDR is 10.4.0.2
Options is 0x2
```

4. Remove a previously assigned *OSPF* password by executing the following command.

FOR EXAMPLE: Type the following:

```
iS5comm(config-if)# no ip ospf authentication-key
```

Configuring Message-Digest Key with Key Constants

1. Execute the following commands to configure the message-digest authentication.

FOR EXAMPLE: Type the following:

Configuration in ISS2

– Enter the Global Configuration Mode in ISS2.

```
iS5comm# configure terminal
```

- Enter the Interface Configuration Mode.

```
iS5comm(config)# interface vlan 1
```

- Delete the authentication key for simple password authentication.

```
iS5comm(config-if)# no ip ospf authentication-key
```

- Configure the authentication key for the message-digest authentication.

```
iS5comm(config-if)# ip ospf message-digest-key 1 md5 asdf
```

- Enable message-digest authentication.

```
iS5comm(config-if)# ip ospf authentication message-digest
```

- Configure key start accept value for key-id.

```
iS5comm(config-if)# ip ospf key 1 start-accept 08-Mar-2021 09:20
```

- Configure key start accepting value for key-id.

```
iS5comm(config-if)# ip ospf key 1 start-generate 08-Mar-2021 09:20
```

- Configure key stop generating value for key-id.

```
iS5comm(config-if)# ip ospf key 1 stop-generate 08-Mar-2021 09:30
```

- Configure key stop generating value for key-id.

```
iS5comm(config-if)# ip ospf key 1 stop-accept 08-Mar-2021 09:30
```

- Exit from the Interface Configuration Mode.

```
iS5comm(config-if)# end
```

Configuration in ISS2

- Enter the Global Configuration Mode in ISS2.

```
iS5comm# configure terminal
```

- Enter the Interface Configuration Mode.

```
iS5comm(config)# interface vlan 1
```

- Delete the authentication key for simple password authentication.

```
iS5comm(config-if)# no ip ospf authentication-key
```

- Configure the authentication key for the message-digest authentication.

```
iS5comm(config-if)# ip ospf message-digest-key 1 md5 asdf
```

- Enable message-digest authentication.

```
iS5comm(config-if)# ip ospf authentication message-digest
```

- Configure key start accept value for key-id.

```
iS5comm(config-if)# ip ospf key 1 start-accept 08-Mar-2021 09:20
```

- Configure key start accepting value for key-id.

```
iS5comm(config-if)# ip ospf key 1 start-generate 08-Mar-2021 09:20
```

- Configure key stop generating value for key-id.

```
iS5comm(config-if)# ip ospf key 1 stop-generate 08-Mar-2021 09:30
```

- Configure key stop generating value for key-id.

```
iS5comm(config-if)# ip ospf key 1 stop-accept 08-Mar-2021 09:30
```

- Exit from the Interface Configuration Mode.

```
iS5comm(config-if)# end
```

2. View the configured authentication by executing the following show command.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf interface
vlan1 is line protocol is up
Internet Address 12.0.0.1, Mask 255.0.0.0, Area 0.0.0.0
AS 1, Router ID 12.0.0.1, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State 5, Priority 1 Designated RouterId
12.0.0.2, Interface address 12.0.0.2
Backup Designated RouterId 12.0.0.1, Interface address 12.0.0.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 7 sec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with the neighbor 12.0.0.2
Message digest authentication enabled
Youngest key id is 1 Key Start Accept Time is 8 Mar 2021 09:21Key Start
Generate Time is 8 Mar 2021 09:21Key Stop Generate Time is 8 Mar 2021
09:31Key Stop Generate Time is 8 Mar 2021 09:31
Connected to VRF default
```

Configuring Null Authentication

1. Execute the following commands to configure the *OSPF* authentication type as Null Authentication.

FOR EXAMPLE: Type the following:

Configuration in ISS2

– Enter the Global Configuration Mode in ISS2.

```
iS5comm# configure terminal
```

– Enter the Interface Configuration mode.

```
iS5comm(config)# interface vlan 1
```

– Delete the authentication key for message-digest authentication.

```
iS5comm(config-if)# no ip ospf message-digest-key 0
```

– Enable null authentication.

```
iS5comm(config-if)# ip ospf authentication null
```

– Exit from the Interface Configuration mode.

```
iS5comm(config-if)# end
```

Configuration in ISS4

– Enter the Global Configuration Mode in ISS4.

```
iS5comm# configure terminal
```

– Enter the Interface Configuration mode.

```
iS5comm(config)# interface vlan 1
```

– Delete the authentication key for message-digest authentication.

```
iS5comm(config-if)# no ip ospf message-digest-key 0
```

– Enable null authentication.

```
iS5comm(config-if)# ip ospf authentication null
```

– Exit from the Interface Configuration mode.

```
iS5comm(config-if)# end
```

2. View the adjacency formed between the neighbors (ISS 2 and ISS 4) by executing the following command. *BDR* stands for Backup Designated Router.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf neighbor detail
Neighbor 10.4.0.4, interface address 10.4.0.4
In the area 0.0.0.0 via interface vlan1
Neighbor priority is 1,State is FULL/BACKUP, 5 state changes
DR is 10.4.0.4 BDR is 10.4.0.2
Options is 0x2
```

Configuring Message-Digest Authentication with SHA-1

SHA-1, a 160-bit message-digest algorithm, developed by the National Security Agency, is generally considered to provide stronger cryptographic security than *MD5* (a 128-bit digest developed by RSA Data Security, Inc), because it uses a longer message digest and it is not vulnerable to some attacks that can be conducted against *MD5*.

1. Execute the following commands to configure the message-digest authentication.

FOR EXAMPLE: Type the following:

Configuration in ISS2

– Enter the Global Configuration Mode in ISS2.

```
iS5comm# configure terminal
```

– Enter the Interface Configuration mode.

```
iS5comm(config)# interface vlan 1
```

– Delete the authentication from null.

```
iS5comm(config-if)# no ip ospf authentication
```

– Configure the authentication key for the message-digest authentication. Here, same can be replaced by other “sha” algorithms like sha-224 / sha-256/ sha-384/ sha-512.

```
iS5comm(config-if)# ip ospf message-digest-key 0 sha-1 abcd
```

– Enable sha-1 authentication. Here, same can be replaced by other sha algorithms like (sha-224 / sha-256/ sha-384/ sha-512).

iS5comm(config-if)# ip ospf authentication sha-1

– Exit from the Interface Configuration mode.

```
iS5comm(config-if)# end
```

Configuration in ISS2

– Enter the Global Configuration Mode in ISS4.

```
iS5comm# configure terminal
```

– Enter the Interface Configuration mode.

```
iS5comm(config)# interface vlan 1
```

– Delete the authentication from null.

```
iS5comm(config-if)# no ip ospf authentication
```

– Configure the authentication key for the message-digest authentication. Here, same can be replaced by other “sha” algorithms like sha-224 / sha-256/ sha-384/ sha-512.

```
iS5comm(config-if)# ip ospf message-digest-key 0 sha-1 abcd
```

– Enable sha-1 authentication. Here, same can be replaced by other sha algorithms like (sha-224 / sha-256/ sha-384/ sha-512)2.

```
iS5comm(config-if)# ip ospf authentication sha-1
```

– Exit from the Interface Configuration mode.

```
iS5comm(config-if)# end
```

2. View the configuration details by executing the following show command.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf interface
vlan1 is line protocol is up
Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0
AS 1, Router ID ID 10.4.0.2, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State 5, Priority 1
Designated RouterId 10.4.0.4, Interface address 10.4.0.4
Backup Designated RouterId 10.4.0.2, Interface address 10.4.0.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0 sec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with the neighbor 10.4.0.4
Youngest key id is 0
vlan1 is line protocol is up
Adjacent with the neighbor
10.4.0.4 Message digest
Internet Address 10.4.0.2, Mask 255.255.0.0, Area 0.0.0.0
AS 1, Router ID 10.4.0.2, Network Type BROADCAST, Cost 1
demand circuit is disabled
Transmit Delay is 1 sec, State 5, Priority 1 Designated RouterId
10.4.0.4, Interface address 10.4.0.4
Backup Designated RouterId 10.4.0.2, Interface address 10.4.0.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0 sec
Neighbor Count is 1, Adjacent neighbor count is 1sha-1 authentication
key is configured
```

```
Youngest key id is 0
Key Start Accept Timeis 29-May-2013,17:01
Key Start Generate Timeis 29-May-2013,17:01
Key Stop Generate Timeis 06-Feb-2136,06:28
Key Stop Accept Timeis 06-Feb-2136,06:28
Simple AuthenticationKey is not
Connected to VRFdefault
```

3. View the adjacency formed between the neighbors (ISS 2 and ISS 4) by executing the following command. *BDR* stands for Backup Designated Router.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf neighbor detail
Neighbor 10.4.0.4, interface address 10.4.0.4
In the area 0.0.0.0 via interface vlan1
Neighbor priority is 1,State is FULL/BACKUP, 5 state changes
DR is 10.4.0.4 BDR is 10.4.0.2
Options is 0x2
```

Configuring Message-Digest Key with Key Constants

1. Execute the following commands to configure the message-digest authentication.

   FOR EXAMPLE: Type the following:

   Configuration in ISS2

   – Enter the Global Configuration Mode in ISS2.

```
iS5comm# configure terminal
```

   – Enter the Interface Configuration Mode.

```
iS5comm(config)# interface vlan 1
```

   – Delete the authentication from NULL.

```
iS5comm(config-if)# no ip ospf authentication
```

   – Configure the authentication key for the message-digest authentication. Here same can be replaced by other sha algorithms like (sha-224 / sha-256/ sha-384/ sha-512.

```
iS5comm(config-if)# ip ospf message-digest-key 0 sha-1 abcd
```

   – Enable message-digest authentication.

```
iS5comm(config-if)# ip ospf authentication message-digest
```

   – Configure key start accept value for key-id.

```
iS5comm(config-if)# ip ospf key 0 start-accept 30-Mar-2021 09:20
```

   – Configure key start accepting value for key-id.

```
iS5comm(config-if)# ip ospf key 0 start-generate 30-Mar-2021 09:20
```

   – Configure key stop generating value for key-id.

```
iS5comm(config-if)# ip ospf key 0 stop-generate 30-Mar-2021 09:30
```

   – Configure key stop generating value for key-id.

```
iS5comm(config-if)# ip ospf key 0 stop-accept 30-Mar-2021 09:30
```

– Exit from the Interface Configuration Mode.

```
iS5comm(config-if)# end
```

Configuration in ISS4

– Enter the Global Configuration Mode in ISS4.

```
iS5comm# configure terminal
```

– Enter the Interface Configuration Mode.

```
iS5comm(config)# interface vlan 1
```

– Delete the authentication from NULL.

```
iS5comm(config-if)# no ip ospf authentication
```

– Configure the authentication key for the message-digest authentication. Here same can be replaced by other sha algorithms like (sha-224 / sha-256/ sha-384/ sha-512.

```
iS5comm(config-if)# ip ospf message-digest-key 0 sha-1 abcd
```

– Enable message-digest authentication.

```
iS5comm(config-if)# ip ospf authentication message-digest
```

– Configure key start accept value for key-id.

```
iS5comm(config-if)# ip ospf key 0 start-accept 30-Mar-2021 09:20
```

– Configure key start accepting value for key-id.

```
iS5comm(config-if)# ip ospf key 0 start-generate 30-Mar-2021 09:20
```

– Configure key stop generating value for key-id.

```
iS5comm(config-if)# ip ospf key 0 stop-generate 30-Mar-2021 09:30
```

– Configure key stop generating value for key-id.

```
iS5comm(config-if)# ip ospf key 0 stop-accept 30-Mar-2021 09:30
```

– Exit from the Interface Configuration Mode.

```
iS5comm(config-if)# end
```

2. View the configured authentication by executing the following show command.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf interface
vlan1 is line protocol is up
Internet Address 10.4.0.2, Mask 255.255.0.0, Area 0.0.0.0
AS 1, Router ID 10.4.0.2, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State 5, Priority 1 Designated RouterId
10.4.0.4, Interface address 10.4.0.4
Backup Designated RouterId 10.4.0.2, Interface address 10.4.0.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0 sec
Neighbor Count is 1, Adjacent neighbor count is 1 Adjacent with the
neighbor 10.4.0.4
Youngest key id is 0
```

```
vlan1 is line protocol is up
Internet Address 10.4.0.2, Mask 255.255.0.0, Area 0.0.0.0
AS 1, Router ID 10.4.0.2, Network Type BROADCAST,Cost 1
demand circuit is disabled
Transmit Delay is 1 sec, State 5, Priority 1
Designated RouterId 10.4.0.4, Interface address 10.4.0.4
Backup Designated RouterId 10.4.0.2, Interface address 10.4.0.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0 sec
Neighbor Count is 1, Adjacent neighbor count is 1 Adjacent with the
neighbor 10.4.0.4

sha-1 authentication key is configured Youngest key id is 0
Key Start Accept Timeis 30-Mar-2021,09:20
Key Start Generate Timeis 30-Mar-2021,09:20
Key Stop Generate Timeis 30-Mar-2021,09:30
Key Stop Accept Timeis 30-Mar-2021,09:30
Simple AuthenticationKey is not Configured
Connected to VRFdefault
```

Configuring Message-Digest Key with start-generate

Configures the time when the switch will start generating *OSPF* packets with the configured key id. The mismatch in key id or password in any of the two routers in our example say either in ISS2 or ISS4 causes the *OSPF* neighborship link status to down between them. The purpose of this command is to start generating *OSPF* packets with a new key id when the configured time reaches.

1. Execute the following commands to configure the message-digest authentication.

   FOR EXAMPLE: Type the following:

   Configuration in ISS2

   – Enter the Global Configuration Mode in ISS2.

   ```
   iS5comm# configure terminal
   ```

   – Enter the Interface Configuration Mode.

   ```
   iS5comm(config)# interface vlan 1
   ```

   – Delete the authentication from NULL.

   ```
   iS5comm(config-if)# no ip ospf authentication
   ```

   – Configure the authentication key for the message-digest authentication. Here same can be replaced by other sha algorithms like (sha-224 / sha-256/ sha-384/ sha-512.

   ```
   iS5comm(config-if)# ip ospf message-digest-key 11 sha-1 abcd
   ```

   – Enable message-digest authentication. Here, same can be replaced by other sha algorithms such as sha-224 / sha-256/ sha-384/ sha-512.

   ```
   iS5comm(config-if)# ip ospf authentication sha-1
   ```

- Configure the time when the router will start using the key for packet generation.

```
iS5comm(config-if)# ip ospf key 11 start-generate 30-May-2021 09:20
```

- Exit from the Interface Configuration Mode.

```
iS5comm(config-if)# end
```

Configuration in ISS4

- Enter the Global Configuration Mode in ISS2.

```
iS5comm# configure terminal
```

- Enter the Interface Configuration Mode.

```
iS5comm(config)# interface vlan 1
```

- Delete the authentication from NULL.

```
iS5comm(config-if)# no ip ospf authentication
```

- Configure the authentication key for the message-digest authentication. Here same can be replaced by other sha algorithms like (sha-224 / sha-256/ sha-384/ sha-512.

```
iS5comm(config-if)# ip ospf message-digest-key 11 sha-1 abcd
```

- Enable message-digest authentication. Here, same can be replaced by other sha algorithms such as sha-224 / sha-256/ sha-384/ sha-512.

```
iS5comm(config-if)# ip ospf authentication sha-1
```

- Configure the time when the router will start using the key for packet generation.

```
iS5comm(config-if)# ip ospf key 11 start-generate 30-May-2021 09:20
```

- Exit from the Interface Configuration Mode.

```
iS5comm(config-if)# end
```

3.8. Configuring Passive Interface

Configuring Passive Interface suppresses routing updates on all interfaces.

Suppressing Routing Updates on All Interfaces

1. Execute the following commands to suppress routing updates on all interfaces.

   FOR EXAMPLE: Type the following:

   - Enter the Global Configuration Mode in ISS1.

   ```
   iS5comm# configure terminal
   ```

   - Enable *OSPF* globally in the switch ISS1.

   ```
   iS5comm(config)# router ospf
   ```

   - Suppress routing updates by executing the following command.

   ```
   iS5comm(config-if)# passive-interface default
   ```

NOTE: All *OSPF* interfaces created after the execution of this command will be passive. This is useful for an Internet service provider (*ISP*) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

- Enable *OSPF* over the *VLAN* interface.

```
iS5comm(config-if)# network 10.4.0.1 area 0.0.0.0
```

- Exit from the Interface Configuration mode.

```
iS5comm(config-if)# end
```

2. View the configuration details by executing the following show command.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf interface vlan 1
vlan1 is line protocol is up
Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0
AS 1, Router ID ID 10.10.2.1, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State 2, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Neighbor Count is 0, Adjacent neighbor count is 0
```

3. Restore routing updates on all interfaces by executing the following commands.

   FOR EXAMPLE: Type the following:

```
iS5comm(config-if)# no network 10.4.0.1 area 0.0.0.0
iS5comm(config-if)# no passive-interface default
```

Suppressing Routing Updates on a Specific Interface

It is also possible to suppress routing updates on a specified interface.

1. Execute the following commands to suppress routing updates on a Specific Interface.

   FOR EXAMPLE: Type the following:

- Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

- Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

- Enter the Interface Configuration Mode for *VLAN* 1.

```
iS5comm(config)# interface vlan 1
```

- Enable *OSPF* over the *VLAN* interface.

```
iS5comm(config-if)# network 10.4.0.1 area 0.0.0.0
```

- Configure the *VLAN* 1 interface as passive interface.

```
iS5comm(config-if)# passive-interface vlan 1
```

- Exit from the Interface Configuration mode.

```
iS5comm(config-if)# end
```

2. View the configuration details by executing the following show command.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf interface vlan 1
vlan1 is line protocol is up
Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0
AS 1, Router ID ID 10.10.2.1, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State 2, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Neighbor Count is 0, Adjacent neighbor count is 0
```

3. Restore routing updates on all interfaces by executing the following commands.

   FOR EXAMPLE: Type the following:

```
iS5comm(config-if)# no passive-interface vlan 1
```

3.9. Configuring OSPF Area Parameters

Area parameters can be configured only after enabling the *OSPF* process. They are configured in the Router Configuration Mode.

Configuring Stub Area

A stub area is an area in which advertisements of external routes are not allowed, which thus reduces the size of the database even more. Instead, a default summary route (0.0.0.0) is inserted into the stub area in order to reach these external routes. If you have no external routes in your network, then you have no need to define stub areas.

1. Execute the following commands to configure an area as a stub area.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

   – Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

   – Configure the *OSPF* router-id.

```
iS5comm(config-router)# router-id 10.10.2.1
```

   – Configure the *OSPF* interface.

```
iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
```

   – Configure the area 0.0.0.6 as a stub area.

```
iS5comm(config-router)# area 0.0.0.6 stub
```

NOTE: Execute the following command to reconfigure the area 0.0.0.6 as a normal area.

```
iS5comm(config-router)# no area 0.0.0.6 stub
```

NOTE: For Sample Configuration for Stub area, *ASBR* and route redistribution, refer to Figure - Topology for Configuration of Stub area, *ASBR* and route redistribution.

– Exit from the Interface Configuration mode.

```
iS5comm(config-if)# end
```

Configuring ASBR Router

Routers that act as gateways (redistribution) between *OSPF* and other routing protocols (*IGRP*, *EIGRP*, *RIP*, *BGP*, Static) or other instances of the *OSPF* routing process are called autonomous system boundary router (*ASBR*).

1. Execute the following commands to configure a router as an *ASBR* router.

FOR EXAMPLE: Type the following:

– Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

– Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

– Configure the *OSPF* router-id.

```
iS5comm(config-router)# router-id 10.10.2.1
```

– Configure the *ASBR* router.

```
iS5comm(config-router)# asbr router
```

NOTE: Disable the *ASBR* router by executing the following command

```
iS5comm(config-router)# no asbr router
```

NOTE: For Sample Configuration for Stub area, *ASBR* and route redistribution, refer to Figure - Topology for Configuration of Stub area, *ASBR* and route redistribution.

– Exit from the Interface Configuration mode.

```
iS5comm(config-if)# end
```

Configuring Redistribution

Redistribution configures the protocol from which the routes have to be redistributed into *OSPF*.

1. Execute the following commands to configure redistribution.

FOR EXAMPLE: Type the following:

– Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

– Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

– Configure the *OSPF* router-id.

```
iS5comm(config-router)# router-id 10.10.2.1
```

– Configure the *ASBR* router.

```
iS5comm(config-router)# asbr router
```

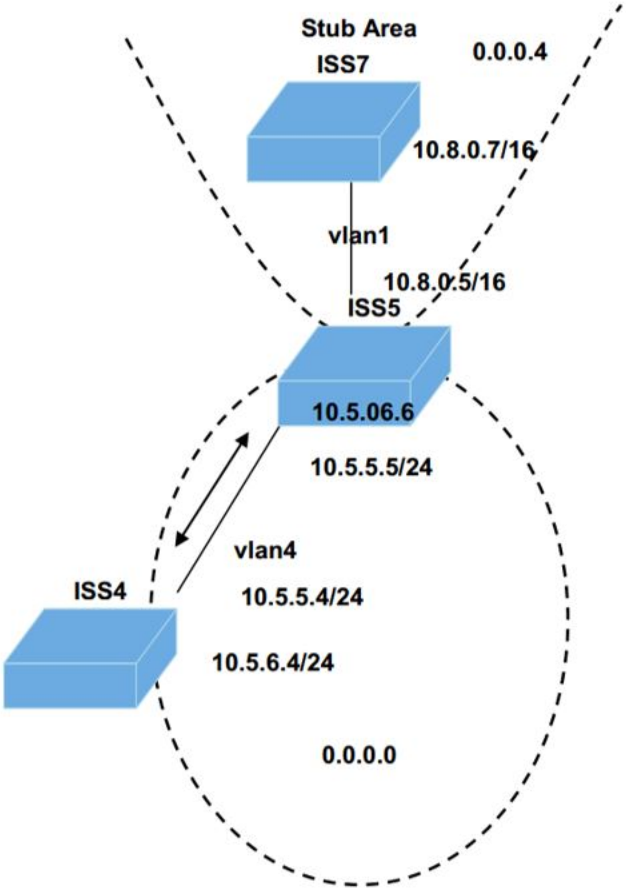
– Configure redistribution of all routes.

```
iS5comm(config-router)# redistribute all
```

NOTE: Disable redistribution of routes by executing the following command.

```
iS5comm(config-router)# no redistribute all
```

Figure 3: Topology for Configuration of Stub area, ASBR and route redistribution



Sample Configuration for Stub area, ASBR, and route redistribution

Some prerequisite configuration (refer Configuration Guidelines (Prerequisite)) must be done in the switches ISS4, ISS5, and ISS7 before configuring *OSPF*.

1. Execute the following commands in ISS4, ISS5 and ISS7.

   FOR EXAMPLE: Type the following:

   Configuration of ISS4

   ISS4 is configured as an *ASBR* (Autonomous System Border Router) for redistributing the external routes into *OSPF* domain.

```
iS5comm# configure terminal
```

```
iS5comm(config)# router ospf
iS5comm(config-router)# router-id 10.4.0.4
iS5comm(config-router)# asbr router
iS5comm(config-router)# redistribute all
iS5comm(config-router)# network 10.5.5.4 area 0.0.0.0
iS5comm(config-router)# exit
iS5comm(config)# ip route 100.0.0.0 255.0.0.0 10.5.5.5
iS5comm(config)# end
```

Configuration of ISS7

In ISS7, area 0.0.0.4 is configured as a stub area. External routes are not redistributed into the stub area.

```
iS5comm# configure terminal
iS5comm(config)# router ospf
iS5comm(config-router)# router-id 10.8.0.7
iS5comm(config-router)# network 10.8.0.7 area 0.0.0.4
iS5comm(config-router)# area 0.0.0.4 stub
iS5comm(config-router)# exit
```

2. View the configuration details by executing the following show commands.

FOR EXAMPLE: Type the following:

In ISS4

```
iS5comm# show ip ospf route
OSPF Process Routing Table
Dest/MaskTOS NextHop/Interface Cost Rt.TypeArea
-------------------/--------- ---- ------- ----
10.5.5.0/255.255.255.0  0   0.0.0.0/vlan4     1IntraArea 0.0.0.0
10.8.0.0/255.255.0.0    0   10.5.5.5/vlan4    2InterArea 0.0.0.0


iS5comm# show ip ospf 0.0.0.0 database external
OSPF Router with ID (10.4.0.4)AS External Link States
-----------------------
LS age             : 300
Options LS: (No ToS Capability, DC)
Type: AS External Link
Link State ID: 10.5.5.0
LS Seq Number      : 0x80000001
Checksum : 0x2a6
Length             : 36
Network Mask       : 255.255.0.0
Metric Type       : 0x80
Metric            : 10
Forward Address   : 0.0.0.0
Externel Route Tag: 0
AS External Link States
----------------------

Advertising Router     : 10.4.0.4
LS Seq Number          :0x80000001
Checksum               : 0xbee3
Length                 : 36
Network Mask           : 255.255.255.0
Metric Type            : 0x80
Metric                 : 10
Forward Address: 0.0.0.0
Externel Route Tag: 0
AS External Link States
-----------------------
LS age: 300
Options: (No ToS Capability, DC)
LS Type: AS External Link
Link State ID: 10.5.6.0
Advertising Router : 10.4.0.4
LS Seq Number: 0x80000001
Checksum: 0xb3ed
Length: 36
Network Mask:255.255.255.0
Metric Type: 0x80
Metric: 10
Forward Address: 0.0.0.0
Externel Route Tag: 0
AS External Link States
-----------------------
LS age:   300
Options:  (No ToS Capability, DC)
LS Type:  AS External Link
Link State ID: 100.0.0.0
Advertising Router: 10.4.0.4
LS Seq Number Checksum: 0x80000001
Advertising Router : 0xcd6b
Length: 36
```

```
Network Mask: 255.0.0.0
Metric Type     : 0x80
Metric          : 10
Forward Address : 10.5.5.5 Externel Route Tag: 0
```

In ISS5

View the external routes are redistributed in this switch

```
iS5comm# show ip ospf route
OSPF Process Routing Table
Dest/MaskTOS NextHop/Interface   Cost Rt.Type Area
------------ -------/---------    ---- -----------
10.4.0.0/255.255.0.0 0 10.5.5.4/vlan4 10 Type2Ext 0.0.0.0
10.5.5.0/255.255.255.0 0 0.0.0.0/vlan4 1 IntraArea 0.0.0.0
10.5.6.0/255.255.255.0 0 10.5.5.4/vlan4 10 Type2Ext 0.0.0.0
10.8.0.0/255.255.0.0 0 0.0.0.0/vlan1 1 IntraArea 0.0.0.4
100.0.0.0/255.0.0.0 0 10.5.5.5/vlan4 10 Type2Ext 0.0.0.0
iS5comm# show ip ospf 0.0.0.0 database external
OSPF Router with ID (10.8.0.5)
AS External Link States
LS age:   300
Options:  (No ToS Capability, DC)
LS Type:  AS External Link
Link State ID: 10.4.0.0
Advertising Router : 10.4.0.4 LS Seq Number: 0x80000001 Checksum: 0x2a6
Length: 36
Network Mask: 255.255.0.0
Metric Type: 0x80
Metric: 10
Forward Address: 0.0.0.0
Externel Route Tag: 0
AS External Link States
-----------------------
LS age: 300
Options: (No ToS Capability, DC)
LS Type: AS External Link
Link State ID: 10.5.5.0
Advertising Router : 10.4.0.4
LS Seq Number: 0x80000001 Checksum: 0xbee3
Length: 36
Network Mask: 255.255.255.0
```

```
Metric Type: 0x80
Metric: 10
Forward Address: 0.0.0.0
Externel Route Tag: 0
AS External Link States
-----------------------
LS age: 300
Options: (No ToS Capability, DC)
LS Type: AS External Link
Link State ID: 10.5.6.0
Advertising Router : 10.4.0.4
LS Seq Number: 0x80000001
Checksum: 0xb3ed
Length: 36
Network Mask: 255.255.255.0
Metric Type: 0x80
Metric: 10
Forward Address: 0.0.0.0
External Route Tag: 0
```

In ISS7

View the external routes are redistributed in this switch

```
iS5comm# show ip ospf route
OSPF Process Routing Table Dest/MaskTOSNextHop/InterfaceCostRt.TypeArea
-------------------/------------------------
0.0.0.0/0.0.0.0 0 10.8.0.5/vlan1 2 InterArea 0.0.0.4
10.5.5.0/255.255.255.0 0 10.8.0.5/vlan1 2 InterArea 0.0.0.4
10.8.0.0/255.255.0.0 0 0.0.0.0/vlan1 1 IntraArea 0.0.0.4
iS5comm# show ip ospf 0.0.0.4 database external
OSPF Router with ID (10.8.0.7)
```

Configuring NSSA Area

An *NSSA* area has the capability to import limited number of external routes. Execute the following commands to configure an area as an *NSSA* (Not-So-Stubby-Area) area.

1. Execute the following commands to configure an area as an *NSSA* area.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

   ```
   iS5comm# configure terminal
   ```

   – Enable OSPF globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

– Configure the OSPF router-id

```
iS5comm(config-router)# router-id 10.10.2.1
```

– Configure the OSPF interface.

```
iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
```

– Configure the area 0.0.0.6 as a *NSSA* area.

```
iS5comm(config-router)# area 0.0.0.6 nssa
```

NOTE: Execute the following command to reconfigure the area 0.0.0.6 as a normal area

```
iS5comm(config-router)# no area 0.0.0.6 nssa
```

– Exit from the Interface Configuration mode.

```
iS5comm(config-if)# end
```

NOTE: Refer to Sample NSSA Configuration, summary address configuration, and area-default cost.

Configuring Summary Address

1. Execute the following commands to configure a summary address.

FOR EXAMPLE: Type the following:

– Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

– Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

– Configure the *OSPF* router-id.

```
iS5comm(config-router)# router-id 10.10.2.1
```

– Configure the *OSPF* interface.

```
iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
```

– Configure the area 0.0.0.6 as a *NSSA* area.

```
iS5comm(config-router)# area 0.0.0.6 nssa
```

– Configure the summary address for 90.0.0.0/8 in the *NSSA* area.

```
iS5comm(config-router)# summary-address 90.0.0.0  255.0.0.0 0.0.0.6
```

NOTE: Delete the summary address configuration for 90.0.0.0/8 in the *NSSA* area by executing the following command

```
iS5comm(config-router)# no summary-address 90.0.0.0  255.0.0.0 0.0.0.6
```

– Exit from the Interface Configuration mode.

```
iS5comm(config-if)# end
```

Configuring Area-default Cost

Configuring Area-default Cost specifies the cost for the default summary route sent into a stub or *NSSA*.

1. Execute the following commands to configure the Area-default Cost.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch ISS1.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* router-id.

   ```
   iS5comm(config-router)# router-id 10.10.2.1
   ```

   – Configure the *OSPF* interface.

   ```
   iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
   iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
   ```

   – Configure the area 0.0.0.6 as a *NSSA* area.

   ```
   iS5comm(config-router)# area 0.0.0.6 nssa
   ```

   – iS5comm(config-router)# area 0.0.0.6 default-cost 50.

   ```
   iS5comm(config-router)# area 0.0.0.6 default-cost 50
   ```

NOTE: Go back to default cost for the default summary route sent into *NSSA* area by executing the following command.

```
iS5comm(config-router)# no area 0.0.0.6 default-cost
```

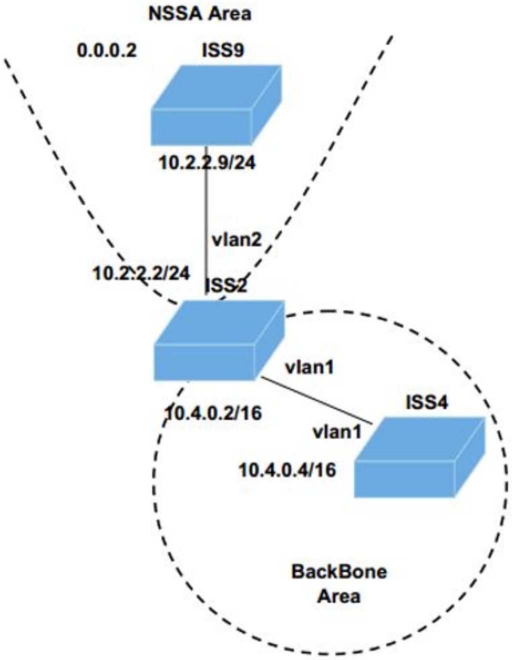
– Exit from the Interface Configuration mode.

```
iS5comm(config-if)# end
```

Sample NSSA Configuration, summary address configuration and area- default cost

CONTEXT:

Figure 4: Sample NSSA Configuration, summary address configuration and area- default cost



Configuring ISS2, ISS4 and ISS9

PREREQUISITE:

Some prerequisite configuration (refer to section 3.2 Configuration Guidelines (Prerequisite)) must be done in the switches ISS2, ISS4, ISS9 before configuring OSPF.

1. Execute the following commands in ISS2, ISS4 and ISS9.

   FOR EXAMPLE: Type the following:

   Configuration of ISS2

   ISS4 is configured as an *ASBR* (Autonomous System Border Router) for redistributing the external routes into *OSPF* domain.

```
iS5comm# configure terminal
iS5comm(config)# router ospf
iS5comm(config-router)# router-id 10.4.0.4
iS5comm(config-router)# network 10.4.0.2 area 0.0.0.0
iS5comm(config-router)# network 10.2.2.2 area 0.0.0.2
```

   – Configure the area 0.0.0.2 as a *NSSA* area.

```
iS5comm(config-router)# area 0.0.0.2 nssa
iS5comm(config-router)# end
```

   Configuration of ISS4

```
iS5comm# configure terminal
```

```
iS5comm(config)# router ospf
iS5comm(config-router)# router-id 10.4.0.4
iS5comm(config-router)# network 10.4.0.4 area 0.0.0.0
iS5comm(config-router)# end
```

Configuration of ISS9

```
iS5comm# configure terminal
iS5comm(config)# router ospf
```

– Configure *ASBR* status and redistribute static routes into the OSPF domain.

```
iS5comm(config-router)# asbr router
iS5comm(config-router)# redistribute static
iS5comm(config-router)# router-id 10.2.2.9
iS5comm(config-router)# network 10.2.2.9 area 0.0.0.2
```

– Configure the area 0.0.0.2 as an *NSSA* area.

```
iS5comm(config-router)# area 0.0.0.2 nssa
```

– Configure summary address for the range 90.0.0.0/8 in the area 0.0.0.2.

```
iS5comm(config-router)# summary-address 90.0.0.0  255.0.0.0 0.0.0.2
iS5comm(config-router)# exit
```

– Configure static routes.

```
iS5comm(config)# ip route 90.1.0.0255.255.0.010.2.2.2
iS5comm(config)# ip route 90.2.0.0255.255.0.010.2.2.2
iS5comm(config)# ip route 90.3.0.0255.255.0.010.2.2.2
iS5comm(config)# ip route 90.4.0.0255.255.0.010.2.2.2
iS5comm(config)# ip route 90.5.0.0255.255.0.010.2.2.2
iS5comm(config-router)# end
```

Viewing the configuration details of ISS2, ISS4, and ISS9

1. Execute the following commands in ISS2, ISS4 and ISS9.

   FOR EXAMPLE: Type the following:

   In ISS2

   View the two *NSSA*-external *LSA*s, one for 90.0.0.0/8 matching the summary range configured and the other for the default external route in the *NSSA* area.

   Another external *LSA* is generated in the area 0.0.0.0 corresponding to the *NSSA*-external *LSA* 90.0.0.0/8.

```
iS5comm# show ip ospf database nssa-external
OSPF Router with ID (10.4.0.2)
---------------------------------------------
LS age: 300
Options: (No ToS Capability, DC)
NSSA External Link States (Area 0.0.0.2)
LS Type: NSSA External Link
```

```
Link State ID: 90.0.0.0
Advertising Router : 10.2.2.9
LS Seq Number: 0x80000001
Checksum: 0xc84f
Length: 36
NSSA External Link States (Area 0.0.0.2)
LS age: 300
Options: (No ToS Capability, DC)
LS Type: AS External Link
Link State ID: 0.0.0.0
Advertising Router : 10.4.0.2
LS Seq Number: 0x80000002
Checksum: 0x120
Length: 36
iS5comm# show ip ospf database external
OSPF Router with ID (10.4.0.2)
AS External Link States
---------------------------------------------
LS age: 0
Options:  (No ToS Capability, DC)
LS Type:  AS External Link
Link State ID: 90.0.0.0
Advertising Router : 10.4.0.2
LS Seq Number: 0x80000001
Checksum: 0x49fd
Length: 36
Network Mask: 255.0.0.0
Metric Type: 0x80
Metric: 10
Forward Address: 10.2.2.9
External Route Tag: 0
iS5comm# show ip ospf route
OSPF Process Routing Table
Dest/Mask TOS NextHop/Interface   Cost Rt.Type Area
------------ -------/---------    ---- -----------
10.2.2.0/255.255.255.0 0 0.0.0.0/vlan2 1 IntraArea 0.0.0.2
10.4.0.0/255.255.0.0 0 0.0.0.0/vlan1 1 IntraArea 0.0.0.0
90.0.0.0/255.0.0.0 0 10.2.2.9/vlan2 10 Type2 Ext0.0.0.2
```

In ISS4

```
iS5comm# show ip ospf route
```

```
OSPF Process Routing Table
Dest/Mask TOS NextHop/Interface   Cost Rt.Type Area
------------ -------/---------    ---- -----------
10.2.2.0/255.255.255.0 0 10.4.0.2/vlan1 2 InterArea 0.0.0.0
10.4.0.0/255.255.0.0 0 0.0.0.0/vlan1 1 IntraArea 0.0.0.0
90.0.0.0/255.0.0.0 0 10.4.0.2/vlan1 10 Type2Ext 0.0.0.0
```

In ISS4

```
iS5comm# show ip ospf database nssa-external
OSPF Router with ID (10.2.2.9)
NSSA External Link States (Area 0.0.0.2)
---------------------------------------------
LS age: 300
Options:  (No ToS Capability, DC)
LS Type: NSSA External Link
Link State ID: 90.0.0.0
Advertising Router : 10.2.2.9
Advertising Router : 10.2.2.9
LS Seq Number: 0x80000001
Checksum: 0xc84f
Length: 36
NSSA External Link States (Area 0.0.0.2)
---------------------------------------------
LS age: 300
Options: (No ToS Capability, DC)
LS Type: NSSA External Link
Link State ID: 0.0.0.0
Advertising Router : 10.4.0.2
LS Seq Number: 0x80000002
Checksum: 0x120
Length: 36
iS5comm# show ip ospf summary-address
Display of Summary addresses for Type5 and Type7 from redistributed
routes
OSPF External Summary Address Configuration Information
-----------------------------------------------------
Network Mask Area Effect TranslationState
------------------------------------
90.0.0.0 255.0.0.0 0.0.0.2 advertiseMatching enabled
iS5comm# show ip route
O 0.0.0.0/0[2] via 10.2.2.2
C 10.2.2.0/24is directly connected, vlan2
```

```
O 10.4.0.0/16 [2] via 10.2.2.2
90.0.0.0 255.0.0.0 0.0.0.2 advertiseMatching enabled
C 12.0.0.0/8 is directly connected, vlan1
S90.1.0.0/16[1]via10.2.2.2
S90.2.0.0/16[1]via10.2.2.2
S90.3.0.0/16[1]via10.2.2.2
S90.4.0.0/16[1]via10.2.2.2
S90.5.0.0/16[1]via10.2.2.2
iS5comm# show ip ospf route
iS5comm# show ip ospf route
OSPF Process Routing Table
Dest/MaskTOS  NextHop/InterfaceCostRt.TypeArea
------------------/------------------------
0.0.0.0/0.0.0.0 0 10.2.2.2/vlan2 2 Type1Ext 0.0.0.2
10.2.2.0/255.255.255.0 0 0.0.0.0/vlan2 1 IntraArea
0.0.0.210.4.0.0/255.255.0.0 0 10.2.2.2/vlan2 2 InterArea0.0.0.2
```

Testing of ISS2, ISS4 and ISS9

NOTE: Test ISS9

1. Test “no summary- address” command.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# configure terminal
   iS5comm(config)# router ospf
   iS5comm(config)# ip route 90.5.0.0255.255.0.010.2.2.2
   ```

2. View the configuration detail in ISS9.

   FOR EXAMPLE: Type the following

   ```
   iS5comm# show ip ospf summary-address
   Display of Summary addresses for Type5 and Type7 from redistributed
   routes
   ```

3. Observe that nssa-external *LSA* is generated for all static routes

   FOR EXAMPLE: Type the following

   ```
   iS5comm# iS5comm# show ip ospf database
   OSPF Router with ID (10.2.2.9)
   Router Link States (Area 0.0.0.2)
   ---------------------------------------
   Link IDADV RouterAgeSeq#ChecksumLink count
   ------------------------------------------
   10.4.0.2 10.4.0.2 300 0x80000006 0x1dc6 1

   10.2.2.910.2.2.93000x800000070xec01
   ```

```
Network Link States (Area 0.0.0.2)
---------------------------------------

Link IDADV RouterAgeSeq#Checksum
--------------------------------
10.2.2.910.2.2.93000x800000020x5290
Summary Link States (Area 0.0.0.2)
-------------------------------------

Link IDADV RouterAgeSeq#Checksum
--------------------------------
10.4.0.010.4.0.23000x800000030x56c5
NSSA External Link States (Area 0.0.0.2)
----------------------------------------
Link IDADV RouterAgeSeq#Checksum
--------------------------------
90.4.0.0 10.2.2.9 300 0x80000001 0x36e4
90.5.0.0 10.2.2.9 300 0x80000001 0x2aef
0.0.0.0 10.4.0.2 300 0x80000003 0xfe21
90.1.0.0 10.2.2.9 300 0x80000001 0x5ac3
90.2.0.0 10.2.2.9 300 0x80000001 0x4ece
90.3.0.0 10.2.2.9 300 0x80000001 0x42d9
```

NOTE: Test ISS2

4. View the *OSPF* external routes corresponding to all *NSSA*-external *LSA*s.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf route
OSPF Process Routing Table
Dest/Mask TOS NextHop/Interface Cost Rt.Type Area
-------------------/------------------------
10.2.2.0/255.255.255.0 0 0.0.0.0/vlan21 IntraArea 0.0.0.2

10.4.0.0/255.255.0.0    0 0.0.0.0/vlan11 IntraArea 0.0.0.0

90.1.0.0/255.255.0.0 0 10.2.2.2/vlan210 Type2Ext 0.0.0.2

90.2.0.0/255.255.0.0    0 10.2.2.2/vlan210 Type2Ext 0.0.0.2

90.3.0.0/255.255.0.0    0 10.2.2.2/vlan210 Type2Ext 0.0.0.2

90.4.0.0/255.255.0.0    0 10.2.2.2/vlan210 Type2Ext 0.0.0.2
```

```
90.5.0.0/255.255.0.0    0 10.2.2.2/vlan210 Type2Ext 0.0.0.2
```

5. Test the area default-cost command.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# configure terminal
   iS5comm(config)# router ospf
   iS5comm(config-router)# area 0.0.0.2 default-cost 50
   ```

   Test ISS9

NOTE: ISS2 sends a type 7 *LSA* for the default route with the updated metric as 50. Therefore, the metric for the default route should be 51 in ISS9.

6. In ISS9, view the configuration.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf route
   Dest/Mask TOS NextHop/Interface  Cost Rt.Type Area
   ------------------/---------   ---------------
   0.0.0.0/0.0.0.0         0 10.2.2.2/vlan2 51 Type1Ext 0.0.0.2
   10.2.2.0/255.255.255.0 0 0.0.0.0/vlan2 1 IntraArea 0.0.0.2
   10.4.0.0/255.255.0.0 0 10.2.2.2/vlan2 2 InterArea 0.0.0.2
   ```

7. in ISS2, test the “no area default-cost” command.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# configure terminal
   iS5comm(config)# router ospf
   iS5comm(config-router)# no area 0.0.0.2 default-cost
   ```

   IN ISS9

NOTE: ISS2 must have sent a type 7 *LSA* for the default route with the updated default metric as 10. Therefore, the metric for the default route must be 11 in ISS9.

8. In ISS9, view the configuration.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf route
   Dest/Mask TOS NextHop/Interface  Cost Rt.Type Area
   ------------------/---------   ---------------
   0.0.0.0/0.0.0.0         0 10.2.2.2/vlan2 11 Type1Ext 0.0.0.2
   10.2.2.0/255.255.255.0 0 0.0.0.0/vlan2 1 IntraArea 0.0.0.2
   10.4.0.0/255.255.0.0 0 10.2.2.2/vlan2 2 InterArea 0.0.0.2
   ```

Configuring NSSA asbr-default-route translator

Configuring *NSSA* asbr-default-route translator enables/disables setting of P bit in the default Type-7 *LSA* generated by *NSSA* internal *ASBR*.

1. Execute the following commands to configure the *NSSA* asbr-default-route translator.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch ISS1.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* router-id.

   ```
   iS5comm(config-router)# router-id 10.10.2.1
   ```

   – Configure the *OSPF* interface.

   ```
   iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
   ```

   – Configure the area 0.0.0.6 as a *NSSA* area.

   ```
   iS5comm(config-router)# area 0.0.0.6 nssa
   ```

   – Enable nssa asbr-default-route translator.

   ```
   iS5comm(config-router)# set nssa asbr-default-route translator enable
   ```

   NOTE: Disable nssa asbr-default-route translator by executing the following command

   ```
   iS5comm(config-router)# set nssa asbr-default-route translator disable
   ```

   – Exit from the Interface Configuration mode.

   ```
   iS5comm(config-if)# end
   ```

Configuring NSSA Area Translation Role

Configuring *NSSA* Area Translation Role configures the translation role for the *NSSA* as always or candidate.

1. Execute the following commands to configure the *NSSA* asbr-default-route translator.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch ISS1.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* router-id.

   ```
   iS5comm(config-router)# router-id 10.10.2.1
   ```

   – Configure the *OSPF* interface.

   ```
   iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
   ```

   – Configure the area 0.0.0.6 as a *NSSA* area.

   ```
   iS5comm(config-router)# area 0.0.0.6 nssa
   ```

– Enable nssa asbr-default-route translator.

```
iS5comm(config-router)# set nssa asbr-default-route translator enable
```

NOTE: Disable nssa asbr-default-route translator by executing the following command

```
iS5comm(config-router)# set nssa asbr-default-route translator disable
```

– Exit from the Interface Configuration mode.

```
iS5comm(config-if)# end
```

Configuring Stability Interval for NSSA

This section configures the number of seconds after which an elected translator determines that its services are no longer required, and that it must continue to perform its translation duties for *NSSA*.

1. Execute the following commands to configure the stability Interval for *NSSA*.

FOR EXAMPLE: Type the following:

– Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

– Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

– Configure the *OSPF* router-id.

```
iS5comm(config-router)# router-id 10.10.2.1
```

– Configure the *ASBR* router status.

```
iS5comm(config-router)# asbr router
```

– Configure the *OSPF* interface.

```
iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
```

– Configure the area 0.0.0.6 as a *NSSA* area.

```
iS5comm(config-router)# area 0.0.0.6 nssa
```

– Configure the stability interval for the *NSSA* area 0.0.0.6 as 120 seconds.

```
iS5comm(config-router)# area 0.0.0.6 stability-interval 120
```

NOTE: Go back to the default stability interval for the *NSSA* area 0.0.0.6 by executing the following command.

```
iS5comm(config-router)# no area 0.0.0.6 stability-interval
```

NOTE: The default value for stability interval is 40 seconds and is configured using the command no area <area-id> stability-interval.

– Exit from the Interface Configuration mode.

```
iS5comm(config-if)# end
```

Configuring ABR-Type

Configuring abr-type sets the *ABR*-Type as either standard, or Cisco, or IBM.

1. Execute the following commands to configure the abr-type.

FOR EXAMPLE: Type the following:

- Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

- Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

- Configure the *OSPF* router-id

```
iS5comm(config-router)# router-id 10.10.2.1
```

- Configure the *OSPF* interface.

```
iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
```

- Configure the *ABR* type as Cisco.

```
iS5comm(config-router)# abr-type cisco
```

NOTE: The default value *ABR* type is standard.

- Exit from the Router Configuration mode.

```
iS5comm(config-router)# end
```

2. View the configuration details by executing the following show command.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf
OSPF Router ID 10.10.2.1
Supports only single TOS(TOS0) route
ABR Type supported is Cisco ABR
It is an Area Border Router
Number of Areas in this router is 2 Area is 0.0.0.6
Number of interfaces in this area is 1
SPF algorithm executed 3 times
Area is 0.0.0.0
Number of interfaces in this area is 1
SPF algorithm executed 3 times
```

Configuring RFC 1583 Compatibility

Configuring RFC 1583 Compatibility sets the OSPF compatibility list to be compatible with the RFC 1583.

1. Execute the following commands to configure the RFC 1583 Compatibility.

   FOR EXAMPLE: Type the following:

- Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

- Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

- Configure the *OSPF* router-id.

```
iS5comm(config-router)# router-id 10.10.2.1
```

– Configure the *OSPF* interface.

```
iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
```

– Configure the RFC1583 compatibility.

```
iS5comm(config-router)# compatible rfc1583
```

NOTE: Disable RFC 1583 compatibility by executing the following command.

iS5comm(config-router)# no compatible rfc1583

Generation of a Default External Route

Configuring Default-information Originate Always enables generation of a default external route into the OSPF routing domain and other parameters related to that area.

1. Execute the following commands to configure the Default-information Originate Always.

FOR EXAMPLE: Type the following:

– Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

– Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

– Configure the *OSPF* router-id.

```
iS5comm(config-router)# router-id 10.10.2.1
```

– Configure the *OSPF* interface.

```
iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
```

– Configure the *ASBR* router status.

```
iS5comm(config-router)# asbr router
```

– Configure the generation of a default external route.

```
iS5comm(config-router)# default-information originate always metric 40
```

NOTE: Disable generation of a default external route by executing the following command.

```
iS5comm(config-router)# no default-information originate always
```

NOTE: Refer to Figure Topology for Testing Generation of a Default External Route and Redistribution Configuration.

Configuring Redistribution Configuration

Configuring redistribution configuration configures the information to be applied to routes learnt from RTM.

1. Execute the following commands to configure Redistribution.

FOR EXAMPLE: Type the following:

– Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

– Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

– Configure the *OSPF* router-id.

```
iS5comm(config-router)# router-id 10.10.2.1
```

– Configure the *ASBR* router.

```
iS5comm(config-router)# asbr router
```

– Configure the redistribution of static routes.

```
iS5comm(config-router)# redistribute static
```

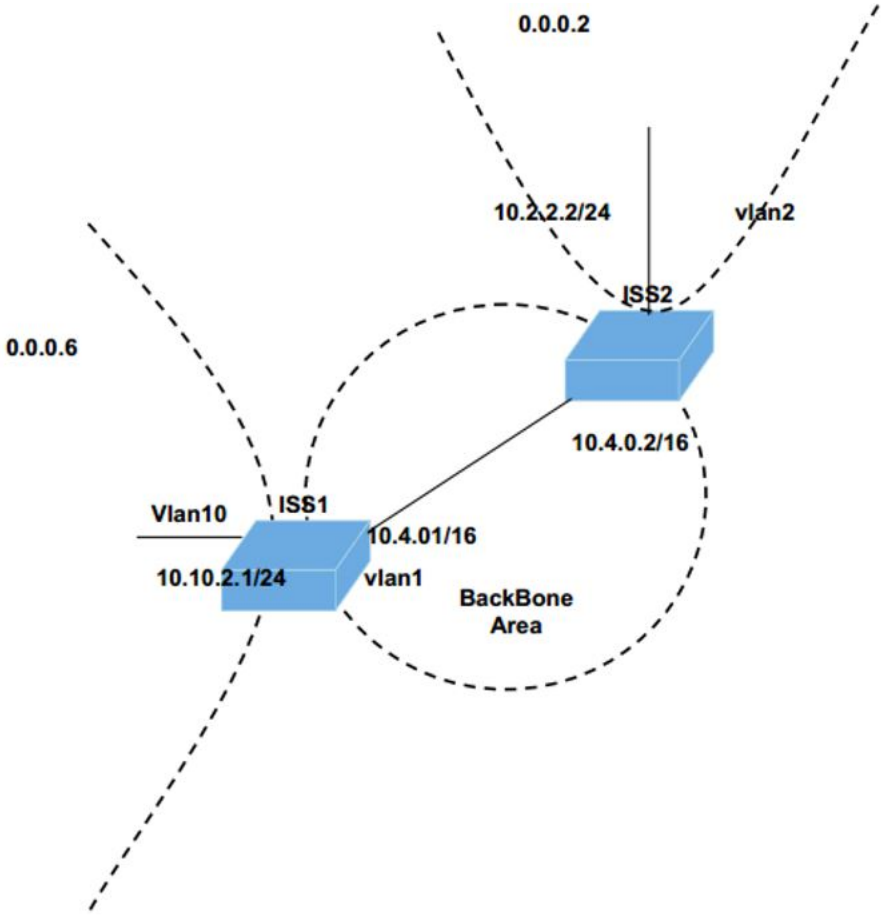
– Configure the redistribution configuration.

```
iS5comm(config-router)# redist-config 20.0.0.0 255.0.0.0 metric-value 100
metric-type asExttype1 tag 10
```

NOTE: Delete the information applied to the routes learnt from RTM by executing the following command

```
iS5comm(config-router)# no redist-config 20.0.0.0 255.0.0.0
```

Figure 5: Topology for Testing Generation of a Default External Route and Redistribution



Sample Configuration for testing default-information originate always and redist-config.

Some prerequisite configuration (refer to Section Configuration Guidelines (Prerequisite)) must be done in the switches ISS1 & ISS2 before configuring *OSPF*.

Configuration of ISS1

1. Execute the following commands in ISS1 to configure the generation of a default external route.

FOR EXAMPLE: Type the following:

– Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

– Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

– Configure the *OSPF* router-id.

```
iS5comm(config-router)# router-id 10.10.2.1
```

– Configure the *OSPF* interface.

```
iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
```

– Configure the *ASBR* router.

```
iS5comm(config-router)# asbr router
```

– Configure the generation of a default external route.

```
iS5comm(config-router)# default-information originate always metric 40
```

– Exit from the Router Configuration mode.

```
iS5comm(config-router)# end
```

Configuration of ISS2

1. Execute the following commands in ISS2.

FOR EXAMPLE: Type the following:

– Enter the Global Configuration Mode in ISS2.

```
iS5comm# configure terminal
```

– Enable *OSPF* globally in the switch ISS2

```
iS5comm(config)# router ospf
```

– Configure the *OSPF* router-id.

```
iS5comm(config-router)# router-id 10.4.0.2
```

– Configure the *OSPF* interface.

```
iS5comm(config-router)# network 10.4.0.2 area 0.0.0.0
iS5comm(config-router)# network 10.2.2.2 area 0.0.0.2
```

– Configure area 0.0.0.2 as an *NSSA* area.

```
iS5comm(config-router)# area 0.0.0.2 nssa
```

– Exit from the Router Configuration mode.

```
iS5comm(config-router)# end
```

2. View the configuration details by executing the following show command in ISS1.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf database external
OSPF Router with ID (10.10.2.1)
AS External Link States
-----------------------
LS age: 0
Options: (No ToS Capability, DC)
LS Type: AS External Link
Link State ID: 0.0.0.0
Advertising Router : 10.10.2.1
LS Seq Number: 0x80000001
Checksum: 0xb5dd
Length: 36
Network Mask: 0.0.0.0
Metric Type: 0x80
Metric: 40
Forward Address: 0.0.0.0
Externel Route Tag: 0
```

3. View the configuration details by executing the following show command in ISS2.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf route
OSPF Process Routing Table
 Dest/Mask  TOSNextHop/InterfaceCostRt.TypeArea
---------  ----------/------------------------
0.0.0.0/0.0.0.0   0 10.4.0.1/vlan1 40 Type2Ext 0.0.0.0

10.2.2.0/255.255.255.0 0 0.0.0.0/vlan2       1 IntraArea       0.0.0.2

10.4.0.0/255.255.0.0   0 0.0.0.0/vlan1       1 IntraArea       0.0.0.0

10.10.0.0/255.255.0.0  0 10.4.0.1/vlan1       2 InterArea      0.0.0.0
```

4. Execute the following commands in ISS1 to configure the generation of a default external route.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

   – Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

   – Configure the default external route.

```
iS5comm(config-router)# no default-information originate always
```

– Exit from the Router Configuration mode.

```
iS5comm(config-router)# end
```

5. View the configuration details by executing the following show command in ISS1. Type 5 External *LSA* for the default route must be flushed

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf database external
OSPF Router with ID (10.10.2.1)
```

6. View the configuration details by executing the following show command in ISS2. The route entry for the default route must be deleted.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf route
OSPF Process Routing Table
 Dest/Mask  TOSNextHop/InterfaceCostRt.TypeArea
---------  ----------/------------------------
10.2.2.0/255.255.255.0 0 0.0.0.0/vlan2      1 IntraArea      0.0.0.2

10.4.0.0/255.255.0.0   0 0.0.0.0/vlan1      1 IntraArea      0.0.0.0

10.10.0.0/255.255.0.0  0 10.4.0.1/vlan1      2 InterArea     0.0.0.0
```

1. Execute the following commands in ISS1 to configure the generation of a default external route.

   FOR EXAMPLE: Type the following:

– Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

– Enable OSPF globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

– Configure the default external route.

```
iS5comm(config-router)# no default-information originate always
```

– Exit from the Router Configuration mode.

```
iS5comm(config-router)# end
```

2. View the configuration details by executing the following show command in ISS1. Type 5 External *LSA* for the default route must be flushed

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf database external
OSPF Router with ID (10.10.2.1)
```

3. View the configuration details by executing the following show command in ISS2. The route entry for the default route must be deleted.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf route
OSPF Process Routing Table
 Dest/Mask  TOSNextHop/InterfaceCostRt.TypeArea
---------  ----------/-----------------------
10.2.2.0/255.255.255.0 0 0.0.0.0/vlan2      1 IntraArea      0.0.0.2

10.4.0.0/255.255.0.0   0 0.0.0.0/vlan1      1 IntraArea      0.0.0.0

10.10.0.0/255.255.0.0  0 10.4.0.1/vlan1      2 InterArea     0.0.0.0
```

Configuration in ISS1

4. Execute the following commands in ISS1 to test redist-config.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

   – Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

   – Configure redistribution of static routes redist-config.

```
iS5comm(config-router)# redistribute static
```

   – Configure redist-config.

```
iS5comm(config-router)# redist-config 20.0.0.0 255.0.0.0 metric-value 100
metric-type asExttype1 tag 10
iS5comm(config-router)# exit
```

   – Add a static route for 20.0.0.0/8 network.

```
iS5comm(config)# ip route 20.0.0.0 255.0.0.0 10.4.0.2
```

   – Exit from the Global Configuration mode.

```
iS5comm(config)# exit
```

5. View the configuration details by executing the following show command in ISS1. An external *LSA* is generated for 20.0.0.0 with metric as 100, metric type as asExtType1, and tag 10.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf database external
OSPF Router with ID (10.10.2.1)
AS External Link States
-----------------------
LS age: 600
Options: (No ToS Capability, DC)
LS Type: AS External Link
```

```
Link State ID: 20.0.0.0
Advertising Router : 10.10.2.1
LS Seq Number: 0x80000001
Checksum: 0xf6b2
Length: 36
Network Mask: 255.0.0.0
Metric Type: 0x0
Metric: 100
Forward Address: 10.4.0.2
```

In ISS2:

6. View the external route 20.0.0.0/8 with metric as 101.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf route
OSPF Process Routing Table
 Dest/Mask   TOSNextHop/InterfaceCostRt.TypeArea
---------  ----------/------------------------
10.4.0.0/255.255.255.0 0 0.0.0.0/vlan1 1 IntraArea       0.0.0.0

10.10.0.0/255.255.0.0   0 0.0.0.0/vlan1       2 IntraArea       0.0.0.0

20.0.0.0/255.0.0.0  0 10.4.0.2/vlan1       101 Type1Ext 0.0.0.0

10.2.2.0/255.255.255.0 0 0.0.0.0/vlan2       1 IntraArea       0.0.0.2
```

Configuration in ISS2

7. Execute the following commands in ISS1 to test no redist-config.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

   – Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

   – Configure no redist-config.

```
iS5comm(config-router)# no redist-config 20.0.0.0 255.0.0.0
```

   – Exit from the Router Configuration mode.

```
iS5comm(config-router)# exit
```

8. View the configuration details by executing the following show command. The external *LSA* generated for 20.0.0.0 with metric as 100, metric type as asExtType1, and tag as 10 is flushed and a new external *LSA* is generated with the default redistribution configuration.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf database external
```

```
OSPF Router with ID (10.10.2.1)
AS External Link States
-----------------------
LS age: 0
Options: (No ToS Capability, DC)
LS Type: AS External Link
Link State ID: 20.0.0.0
Advertising Router : 10.10.2.1
LS Seq Number: 0x80000002
Checksum: 0x3c5
Length: 36
Network Mask: 255.0.0.0
Metric Type: 0x0
Metric: 10
Forward Address: 10.4.0.2
Externel Route Tag: 0
```

Configuring Neighbor

Configuring Neighbor specifies an *NBMA* (Non Broadcast Multi Access) neighbor router and its priority.

1. Execute the following commands to configure a Neighbor.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch ISS1.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* router-id

   ```
   iS5comm(config-router)# router-id 10.10.2.1
   ```

   – Configure the *OSPF* interface.

   ```
   iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
   iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
   ```

   – Exit from the Router Configuration mode.

   ```
   iS5comm(config-router)# end
   ```

   – Enter the Interface Configuration mode.

   ```
   iS5comm(config-if)# interface vlan 1
   ```

   – Configure the network type as *NBMA*.

   ```
   iS5comm(config-if)# ip ospf network non-broadcast
   ```

   – Configure the neighbor with priority.

   ```
   iS5comm(config-if)# exit
   iS5comm(config)# router ospf
   ```

```
iS5comm(config-router)# neighbor 10.4.0.2 priority 10
```

– Configure the neighbor with default priority.

```
iS5comm(config-if)# no neighbor 10.4.0.2 priority 10
```

NOTE: Delete the configured neighbor by executing the following command.

```
iS5comm(config-router)# no neighbor 10.4.0.2
```

Configuring Virtual Link

Configuring Virtual Link defines an *OSPF* virtual link and its related parameters.

1. Execute the following commands to configure the Virtual Link.

FOR EXAMPLE: Type the following:

– Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

– Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

– Configure the OSPF router-id.

```
iS5comm(config-router)# router-id 10.10.2.1
```

– Configure the *OSPF* interface.

```
iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
```

– Configure the virtual link.

```
iS5comm(config-router)# area 0.0.0.6 virtual-link 20.0.0.1 authentication
message-digest hello-interval 100 retransmit-interval 100 transmit-delay
50 dead-interval 200 authentication-key asdf
```

NOTE: Delete the virtual link by executing the following command.

```
iS5comm(config-router)# no area 0.0.0.6 virtual-link 20.0.0.1
```

NOTE: Refer to Sample Configuration for testing virtual link and route summarization

Configuring Virtual Link with SHA-1

Configuring Virtual Link defines an *OSPF* virtual link and its related parameters.

1. Execute the following commands to configure the Virtual Link.

FOR EXAMPLE: Type the following:

– Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

– Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

– Configure the *OSPF* router-id.

```
iS5comm(config-router)# router-id 10.10.2.1
```

– Configure the *OSPF* interface.

```
iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
```

– Configure the virtual link with sha-1. Here, the sha-1 can be replaced by the sha-2 algorithms such as sha-224/ sha-256/ sha-384/ sha-512.

iS5comm(config-router)# area 0.0.0.6 virtual-link 20.0.0.1 authentication sha-1 hello-interval 100 retransmit-interval 100 transmit-delay 50 dead-interval 200 message-digest-key 1 sha-1 abcd

NOTE: Delete the virtual link by executing the following command.

```
iS5comm(config-router)# no area 0.0.0.6 virtual-link 20.0.0.1
```

NOTE: Refer to Sample Configuration for testing virtual link and route summarization

Configuring Area-range

The area-range is configured to consolidate and summarize routes at an area boundary.

1. Execute the following commands to configure the route summarization at an area border router.

FOR EXAMPLE: Type the following:

– Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

– Enable *OSPF* globally in the switch ISS1.

```
iS5comm(config)# router ospf
```

– Configure the *OSPF* router-id.

```
iS5comm(config-router)# router-id 10.10.2.1
```

– Configure the *OSPF* interface.

```
iS5comm(config-router)# network 10.4.0.1 area 0.0.0.0
iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
```

– Configure the route summarization at an area border router.

```
iS5comm(config-router)# area 0.0.0.6 range 10.10.0.0 255.255.0.0 summary
```

NOTE: Delete the route summarization information by executing the following command.

iS5comm(config-router)# no area 0.0.0.6 range 10.10.0.0 255.255.0.0

3.10. Configuring Route Map – OSPF

iS5Com’s Unified Route Map (*URM*) is a portable implementation of the route map capability for IPv4 and IPv6 unicast routing software. The *URM* provides a single interface for the administrator to set up and manage route maps. It also provides a common unified method for routing protocols and static route management software to use route maps for different purposes. The independent nature of the implementation helps to avoid the duplication of the route maps in the different routing modules in a router.

Configuring Route Map

This section lists the *CLI* configuration steps to define a route map with a specified name and the related parameters such as permission and sequence number.

1. Execute the following commands to suppress routing updates on all interfaces.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

   ```
   iS5comm# configure terminal
   ```

   – Configure the route map name, permission and sequence number.

   ```
   iS5comm(config)# route-map aa permit 1
   ```

   – Exit from the Global Configuration mode.

   ```
   iS5comm(config)# exit
   ```

2. View the configured route map.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show route-map
   Route-map aa, Permit, Sequence 1
   Match Clauses:
   --------------
   Set Clauses:
   --------------
   ```

3. Delete the route map configured by executing the following commands.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm(config)# no route-map aa 1
   ```

Configuring Route Map Match Criteria

This section lists the *CLI* configuration steps to define the filtering criteria for the route map and its related parameters.

1. Execute the following commands to suppress routing updates on all interfaces.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

   ```
   iS5comm# configure terminal
   ```

   – Configure the route map name, permission and sequence number.

   ```
   iS5comm(config)# route-map aa permit 1
   ```

   – Configure the route map match source IP address and the subnet mask.

   ```
   iS5comm (config-rmap-aa)# match source ip 34.0.0.3 255.0.0.0
   ```

   – Configure the route map match source IPv6 address and the prefix length.

   ```
   iS5comm (config-rmap-aa)# match source ipv6 2120::3 64
   ```

   – Configure the route map match destination IP address and the subnet mask

```
iS5comm (config-rmap-aa)# match destination ip 91.0.0.1 255.0.0.0
```

- Configure the route map match destination IPv6 address and prefix length.

```
iS5comm (config-rmap-aa)# match destination ipv6 2150::2 64
```

- Configure the route map match route-type as remote. (Route-type can be configured either as local or remote.)

```
iS5comm (config-rmap-aa)# match route-type remote
```

- Configure the route map match metric-type. (Metric type can be inter-area / intra-area / type-1-external / type-2-external.).

```
iS5comm (config-rmap-aa)# match metric-type inter-area
```

- Configure the route map match metric value.

```
iS5comm (config-rmap-aa)# match metric 44
```

- Configure the route map match next-hop IP address.

```
iS5comm (config-rmap-aa)# match next-hop ip 91.0.0.1.
```

- Configure the route map match next-hop IPv6 address.

```
iS5comm (config-rmap-aa)# match next-hop ipv6 3000::3
```

- Configure the route map match tag.

```
iS5comm (config-rmap-aa)# match tag 10
```

- Exit from the Route Map Configuration mode.

```
iS5comm(config)# exit
```

2. View the configured route map.

   FOR EXAMPLE: Type the following:

```
iS5comm# show running-config route-map
Building configuration...
route-map aa permit 1
match destination ip 91.0.0.1  255.0.0.0
match destination ipv6 2150::2  64
match source ip 34.0.0.3  255.0.0.0
match source ipv6 2120::3  64
match next-hop ip 91.0.0.1
match next-hop ipv6 3000::3
match metric 44
match tag 10
match metric-type inter-area
match route-type remote
end
```

3. Execute the no form of the commands to delete the configurations.

Configuring OSPF Distance

This section lists the *CLI* configuration steps to define a route map with a specified name and the related parameters such as permission and sequence number.

1. Execute the following commands to suppress routing updates on all interfaces.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

   ```
   iS5comm# configure terminal
   ```

   – Enter the *OSPF* Router Configuration Mode.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the distance for the *OSPF* routes.

   ```
   iS5comm(config-router)# distance 130
   ```

   – Exit the *OSPF* Router Configuration Mode.

   ```
   iS5comm(config- router)# end
   ```

2. View the configured route map.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show running-config ospf
   Building configuration...
   router ospf
   distance 130
   !
   router ospf
   !
   end
   ```

3. Re-configure the distance to its default value..

   FOR EXAMPLE: Type the following:

   ```
   iS5comm(config-router)# no distance
   ```

Configuring Redistribution with Route Map

This section lists the *CLI* configuration steps to define a route map with a specified name and the related parameters such as permission and sequence number.

1. Execute the following commands to suppress routing updates on all interfaces.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

   ```
   iS5comm# configure terminal
   ```

   – Enter the *OSPF* Router Configuration Mode.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* router ID.

```
iS5comm(config)# router-id 10.10.2.1
```

– Configure the router as *ASBR* (Autonomous System Boundary Router).

```
iS5comm(config-router)# ASBR Router
```

– Configure the redistribution of all routes with route-map aa.

```
iS5comm(config-router)# redistribute all route-map aa
```

– Exit the OSPF Router Configuration Mode.

```
iS5comm(config- router)# end
```

2. View the configured route map.

   FOR EXAMPLE: Type the following:

```
iS5comm# show running-config ospf
Building configuration...
router ospf
router-id 10.10.2.1
ASBR Router
redistribute static route-map aa
redistribute connected route-map aa
redistribute rip route-map aa
redistribute bgp route-map aa
distance 130
!
router ospf
!
end
```

3. Disable the redistribution of all routes with route-map.

   FOR EXAMPLE: Type the following:

```
iS5comm(config-router)# no redistribute all route-map aa
```

Topology Configuration for OSPF Testing

This section provides the sample configuration for testing a route map with OSPF.

CONTEXT:

Figure 6: Topology Configuration for OSPF Testing

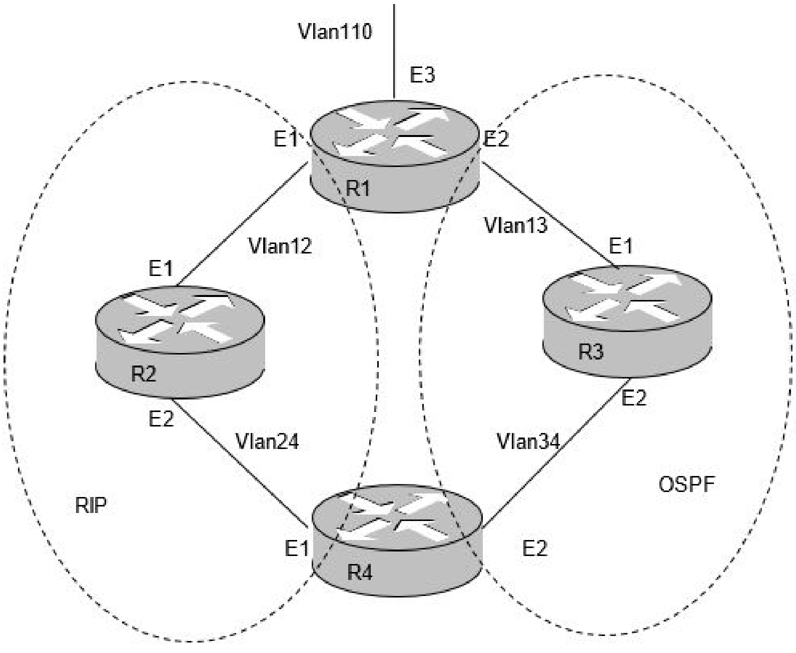


Table 1: IPv4 / IPv6 Addresses of Interfaces in the Routers – OSPF Testing

Router	Interface	Ports	IPv4 Address / Mask	IPv6 Address/ Prefix Length
R1	Vlan 12	Tagged ports E1	12.0.0.1/8	2120::1/24
	Vlan 13	Tagged ports E2	13.0.0.1/8	2130::1/24
	Vlan 110	Tagged ports E3	70.0.0.1/8	2070::1/24
R2	Vlan 12	Tagged ports E1	12.0.0.2/8	2120::2/24
	Vlan 24	Tagged ports E2	24.0.0.2/8	2240::2/24
R3	Vlan 13	Tagged ports E1	13.0.0.3/8	2130::3/24
	Vlan 34	Tagged ports E2	34.0.0.3/8	2340::3/24
R4	Vlan 24	Tagged ports E1	24.0.0.4/8	2240::4/24
	Vlan 34	Tagged ports E2	34.0.0.4/8	2340::4/24

R1 – *ASBR* router

All *OSPF* routers have router-ID 0.0.0.N, where N - number of router.

All *OSPF* routers use area 0.0.0.0.

Some prerequisite configuration must be done in the switches R1, R2, R3 and R4 before configuring *OSPF*.

1. To test the behavior of route selection, when distance command is applied to the *OSPF* router, execute the following commands in R1, R2, R3, and R4.

   FOR EXAMPLE: Type the following:

   – **R1**

   ```
   iS5comm# configure terminal
   iS5comm(config)# router ospf
   iS5comm(config-router)# router-id 0.0.0.1
   iS5comm(config-router)# ASBR Router
   iS5comm(config-router)# network 13.0.0.1 area 0.0.0.0
   iS5comm(config-router)# exit
   iS5comm(config)# router rip
   iS5comm(config-router)# network 12.0.0.1
   iS5comm(config-router)#end
   ```

   – **R2**

   ```
   iS5comm# configure terminal
   iS5comm(config)# router rip
   iS5comm(config-router)# network 12.0.0.2
   iS5comm(config-router)# network 24.0.0.2
   iS5comm(config-router)#end
   ```

   – **R3**

   ```
   iS5comm# configure terminal
   iS5comm(config)# router ospf
   iS5comm(config-router)# router-id 0.0.0.2
   iS5comm(config-router)# network 13.0.0.3 area 0.0.0.0
   iS5comm(config-router)# network 34.0.0.3 area 0.0.0.0
   iS5comm(config-router)# end
   ```

   – **R4**

   ```
   iS5comm# configure terminal
   iS5comm(config)# router ospf
   iS5comm(config-router)# router-id 0.0.0.3
   iS5comm(config-router)# network 34.0.0.4 area
   0.0.0.0iS5comm(config-router)# exit
   iS5comm(config)# router rip
   iS5comm(config-router)# network 24.0.0.4
   iS5comm(config-router)#end
   ```

2. Configure the route-map aa with match criteria at R4.

   FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# route-map aa permit 1
iS5comm(config-rmap-aa)# match source ip 34.0.0.3 255.0.0.0
iS5comm(config-rmap-aa)# exit
```

3. Apply redistribute all to *RIP* and *OSPF* routers at R4.

FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# router ospf
iS5comm(config-router)# redistribute all
iS5comm(config-router)#end
iS5comm(config)# router rip
iS5comm(config-router)# redistribute all
iS5comm(config-router)#end
iS5comm(config-rmap-aa)# match source ip 34.0.0.3 255.0.0.0
iS5comm(config-rmap-aa)# exit
```

4. View the routes at R4.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip route
Vrf Name:          default
C 12.0.0.0/8  is directly connected, vlan1
O 13.0.0.0/8  [2] via 34.0.0.3
O 15.0.0.0/8  [10] via 34.0.0.3
C 24.0.0.0/8  is directly connected, vlan24 C 34.0.0.0/8  is directly
connected, vlan34
O 70.0.0.0/8  [10] via 34.0.0.3
```

5. Set the administrative distance 130 to the OSPF router in R4.

FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# router ospf
iS5comm(config-router)# distance 130 route-map aa
iS5comm(config-router)# exit
```

6. Force routes updates in R1.

FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# router ospf
iS5comm(config-router)# no redistribute all
iS5comm(config-router)# redistribute all
iS5comm(config-router)# exit
iS5comm(config)# router rip
```

```
iS5comm(config-router)# no redistribute all
iS5comm(config-router)# redistribute all
iS5comm(config-router)# exit
```

7. View the routes at R4.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip route
Vrf Name:          default
C 12.0.0.0/8  is directly connected, vlan1
O 13.0.0.0/8  [2] via 34.0.0.3
O 15.0.0.0/8  [10] via 34.0.0.3
C 24.0.0.0/8  is directly connected, vlan24 C 34.0.0.0/8  is directly
connected, vlan34
R 70.0.0.0/8  [5] via 24.0.0.2
```

8. Reset the administrative distance to the OSPF router in R4.

   FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# router ospf
iS5comm(config-router)# no distance 130 route-map aa
iS5comm(config-router)# exit
```

9. Force routes updates in R1.

   FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# router ospf
iS5comm(config-router)# no redistribute all
iS5comm(config-router)# redistribute all
iS5comm(config-router)# exit
iS5comm(config)# router rip
iS5comm(config-router)# no redistribute all
iS5comm(config-router)# redistribute all
iS5comm(config-router)# exit
```

10. View the routes at R4.

    FOR EXAMPLE: Type the following:

```
iS5comm# iS5comm# show ip route
Vrf Name:          default
C 12.0.0.0/8  is directly connected, vlan1
O 13.0.0.0/8  [2] via 34.0.0.3
O 15.0.0.0/8  [10] via 34.0.0.3
```

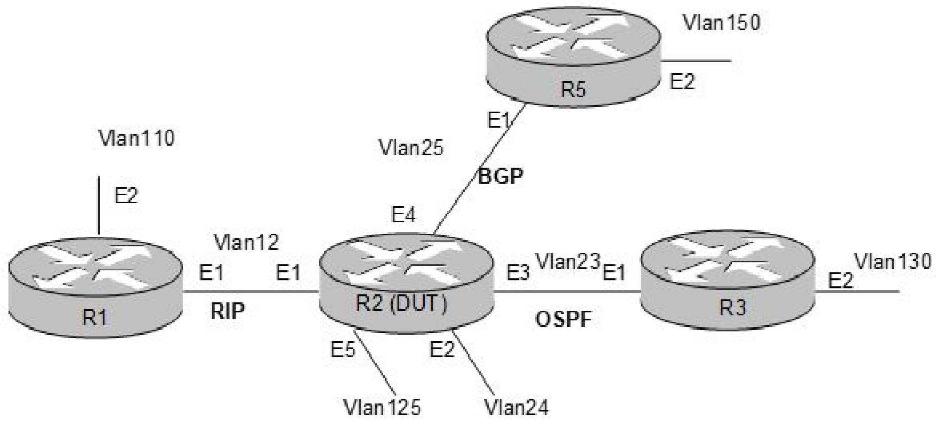
```
C 24.0.0.0/8  is directly connected, vlan24 C 34.0.0.0/8  is directly
connected, vlan34
O 70.0.0.0/8  [10] via 34.0.0.3
```

Redistribution Topology

This section provides the sample configuration for testing redistribution of routes into *OSPF* with route map.

CONTEXT:

Figure 7: Redistribution Topology Configurations



Redistribution Interface Configuration

CONTEXT:

Table 2: IPv4 / IPv6 Addresses of Interfaces in the Routers – Redistribution Topology

Router	Interface	Ports	IPv4 Address / Mask	IPv6 Address/ Prefix Length
R1	Vlan 12	Tagged ports E1	140.0.0.1/16	2140::1/24
	Vlan 110	Tagged ports E2	70.0.0.1/8	2070::1/24
R2	Vlan 12	Tagged ports E1	140.0.0.2/16	2140::2/24
	Vlan 23	Tagged ports E3	20.0.0.2/8	2140::2/24
	Vlan 24	Tagged ports E2	60.0.0.2/8	2040::2/24
	Vlan 25	Tagged ports E4	40.0.0.2/8	2060::2/24
	Vlan 125	Tagged ports E5	50.0.0.2/8	2050::2/24
R3	Vlan 23	Tagged ports E1	13.0.0.3/8	2020::3/24
	Vlan 130	Tagged ports E2	34.0.0.3/8	2011::3/24

Table 2: IPv4 / IPv6 Addresses of Interfaces in the Routers – Redistribution Topology

Router	Interface	Ports	IPv4 Address / Mask	IPv6 Address/ Prefix Length
R5	Vlan 24	Tagged ports E1	24.0.0.4/8	2060::5/24
	Vlan 34	Tagged ports E2	34.0.0.4/8	2014::5/24

Protocol Configuration

CONTEXT:

Table 3: Protocol Configuration

Router	Interface
R1	Interface Vlan 12 Enable *RIP*v2.
R2	Interface Vlan 12 Enable *RIP*v2. Interface Vlan 23 Enable OSPFv2 with Area 0. Configure this as the *ASBR* router. Enable OSPFv3 with Area 0. Configure this as the *ASBR* router. Interface Vlan 25 Enable BGP with peer Vlan 25 interface on R5 with remote AS 300.
R3	Interface Vlan 23Enable OSPFv2 with Area 0.Enable OSPFv3 with Area 0
R5	Interface Vlan 25Enable BGP with peer as VLAN 25 interface on R2 with remote AS 100.

1. To test the following behaviors, execute the following commands:
   a. redistribution of static routes into OSPFv2 with the route map with <match destination ip> clause
   b. redistribution of static routes into OSPFv2, when the route map is modified or deleted
   c. redistribution of static routes into OSPFv2, when static routes for redistribution are added or deleted.

   FOR EXAMPLE: Type the following:

   – **Configuration at R1**

```
iS5comm# configure terminal
iS5comm(config)# router rip
iS5comm(config-router)# network 140.0.0.1
iS5comm(config-router)#end
```

   – **Configuration at R2**

```
iS5comm# configure terminal
iS5comm(config)# router rip
iS5comm(config-router)# network 140.0.0.1
```

```
iS5comm(config-router)# exit
iS5comm(config)# router ospf
iS5comm(config-router)# router-id 0.0.0.1
iS5comm(config-router)# ASBR Router
iS5comm(config-router)# network 20.0.0.2 area 0.0.0.0
iS5comm(config-router)# exit
iS5comm(config)# as-num 100
iS5comm(config)# router-id 40.0.0.2
iS5comm(config)# router bgp 100
iS5comm(config-router)# neighbor 40.0.0.5 remote-as 300
iS5comm(config-router)#end
iS5comm# configure terminal
iS5comm(config)# router ospf
iS5comm(config-router)# router-id 0.0.0.3
iS5comm(config-router)# network 34.0.0.4 area 0.0.0.0
iS5comm(config-router)# exit
iS5comm(config)# router rip
iS5comm(config-router)# network 24.0.0.4
iS5comm(config-router)#end
```

– **Configuration at R3**

```
iS5comm# configure terminal
iS5comm(config)# router ospf
iS5comm(config-router)# router-id 0.0.0.2
iS5comm(config-router)# network 20.0.0.3 area 0.0.0.0
iS5comm(config-router)# exit
```

– **Configuration at R5**

```
iS5comm# configure terminal
iS5comm(config)# as-num 300
iS5comm(config)# router-id 40.0.0.5
iS5comm(config)# router bgp 300
iS5comm(config-router)# neighbor 40.0.0.2 remote-as
100iS5comm(config-router)# exit
```

2. Perform the following configurations in R2. In R2, create static routes and create a route-map aa

FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# ip route 91.0.0.0 255.0.0.0 vlan 24
iS5comm(config)# ip route 92.0.0.0 255.0.0.0 vlan 24
iS5comm(config)# route-map aa permit 1
iS5comm(config-rmap-aa)# match destination ip 91.0.0.0 255.0.0.0
iS5comm(config-rmap-aa)# end
```

```
iS5comm#configure terminal
iS5comm(config)# route-map aa deny 2
iS5comm(config-rmap-aa)# match destination ip 93.0.0.0 255.0.0.0
```

3. Enable redistribution of static routes into *OSPF*v2 with route map aa

   FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# router ospf
iS5comm(config-router)# redistribute static route-map aa
```

4. Verify the route in R3, verify 91.0.0.0/8 is present in the general routing table

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip route
Vrf Name:          default
C 11.0.0.0/8  is directly connected, vlan130
C 12.0.0.0/8  is directly connected, vlan1
C 20.0.0.0/8  is directly connected, vlan23
O 91.0.0.0/8  [10] via 20.0.0.2
```

5. In R2, modify the route map aa.

   FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# route-map aa permit 1
iS5comm(config-rmap-aa)# no match destination ip 91.0.0.0 255.0.0.0
iS5comm(config-rmap-aa)# match destination ip 92.0.0.0 255.0.0.0
iS5comm(config-rmap-aa)# exit
```

6. In R3, verify 91.0.0.0/8 is removed from the general routing table and 92.0.0.0/8 is present in the general routing table.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip route
Vrf Name:          default
C 11.0.0.0/8  is directly connected, vlan130
C 12.0.0.0/8  is directly connected, vlan1
C 20.0.0.0/8  is directly connected, vlan23
O 92.0.0.0/8  [10] via 20.0.0.2
```

7. In R2, add/remove static routes.

   FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# ip route 93.0.0.0 255.0.0.0 vlan 24
iS5comm(config)# no ip route 92.0.0.0 255.0.0.0 vlan 24
iS5comm(config)# end
```

8. In R3, verify 92.0.0.0/8 is removed from the general routing table and 92.0.0.0/8 is present in the general routing table.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip route
Vrf Name:          default
C 11.0.0.0/8  is directly connected, vlan130
C 12.0.0.0/8  is directly connected, vlan1
C 20.0.0.0/8  is directly connected, vlan23
O 93.0.0.0/8  [10] via 20.0.0.2
```

9. Delete the route map aa.

   FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# no route-map aa 1
iS5comm(config)# no route-map aa 2
iS5comm(config)# exit
```

10. In R3, verify 91.0.0.0/8 is removed from the general routing table and 92.0.0.0/8 is present in the general routing table.

    FOR EXAMPLE: Type the following:

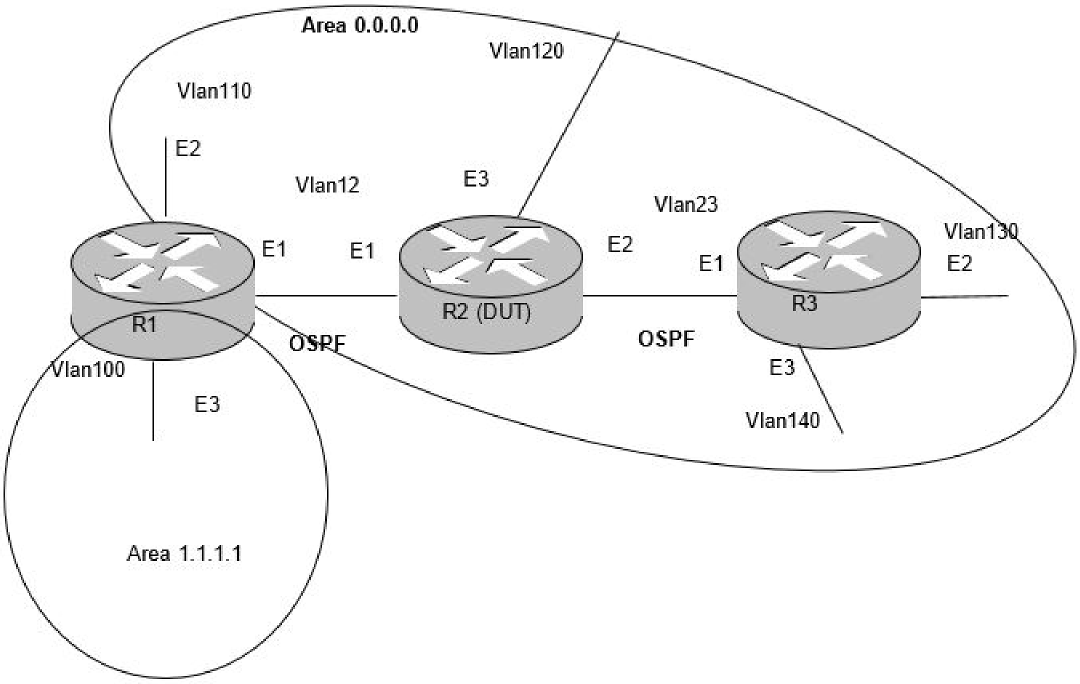
```
iS5comm# show ip route
Vrf Name:          default
C 11.0.0.0/8  is directly connected, vlan130
C 12.0.0.0/8  is directly connected, vlan1
C 20.0.0.0/8  is directly connected, vlan23
O 93.0.0.0/8 [10] via 20.0.0.2
```

OSPF Inbound Filtering with Route Map

This section provides the sample configuration for testing *OSPF* inbound filtering with route map.

CONTEXT:

Figure 8: Distribute-list In Topology Configuration



Interface Configuration

CONTEXT:

Table 4: IPv4 / IPv6 Addresses of Interfaces in the Routers – OSPF Inbound Filtering

Router	Interface	Ports	IPv4 Address / Mask	IPv6 Address/ Prefix Length
R1	Vlan 12	Tagged ports E1	10.0.0.1/8	1111::1/64
	Vlan 100	Tagged ports E3	20.0.0.1/8	2222::1/64
	Vlan 110	Tagged ports E2	130.0.0.1/8	1234::1/64
R2	Vlan 12	Tagged ports E1	10.0.0.2/8	1111::2/64
	Vlan 23	Tagged ports E2	30.0.0.2/8	3333::2/64
	Vlan 120	Tagged ports E3	100.0.0.2/8	3214::2/64
R3	Vlan 23	Tagged ports E1	30.0.0.3/8	3333::3/64
	Vlan 130	Tagged ports E2	120.0.0.3/8	4444::3/64
	Vlan 140	Tagged ports E2	150.0.0.3/8	5555::3/64

Protocol Configuration

CONTEXT:

Table 5: Protocol Configuration

Router	Interface
R1	Configure this as *ASBR* router. Interface Vlan 12 Enable OSPFv2/OSPFv3 with Area 0.0.0.0. Interface Vlan 100 Enable OSPFv2/OSPFv3 with Area 1.1.1.1. Interface Vlan 110 Enable OSPFv2/OSPFv3 with Area 0.0.0.0.
R2	Interface Vlan 12 Enable OSPFv2/OSPFv3 with Area 0.0.0.0. Interface Vlan 23 Enable OSPFv2/OSPFv3 with Area 0.0.0.0. Interface Vlan 120 Enable OSPFv2/OSPFv3 with Area 0.0.0.0
R3	Configure this as *ASBR* router. Interface Vlan 23 Enable OSPFv2/OSPFv3 with Area 0.0.0.0. Interface Vlan 130 Enable OSPFv2/OSPFv3 with Area 0.0.0.0. Interface Vlan 140 Enable OSPFv2/OSPFv3 with Area 0.0.0.0

1. Perform the following configurations in R1, R2 and R3:

   FOR EXAMPLE: Type the following:

   – **Configuration at R1**

   – Configure R1 as *ASBR* Router.

```
iS5comm# configure terminal
iS5comm(config)# router ospf
iS5comm(config-router)# router-id 0.0.0.1
iS5comm(config-router)# network 10.0.0.1 area 0.0.0.0
iS5comm(config-router)# network 130.0.0.1 area 0.0.0.0
iS5comm(config-router)# network 20.0.0.1 area 1.1.1.1
iS5comm(config)# router rip
iS5comm(config-router)#end
```

   – **Configuration at R2**

```
iS5comm# configure terminal
iS5comm(config)# router ospf
```

```
iS5comm(config-router)# router-id 0.0.0.2
iS5comm(config-router)# network 10.0.0.2 area 0.0.0.0
iS5comm(config-router)# network 30.0.0.2 area 0.0.0.0
iS5comm(config-router)# network 100.0.0.2 area 0.0.0.0
iS5comm(config-router)#end
```

– **Configuration at R3**

```
iS5comm# configure terminal
iS5comm(config)# router ospf
iS5comm(config-router)# router-id 0.0.0.3
iS5comm(config-router)# network 30.0.0.3 area 0.0.0.0
iS5comm(config-router)# network 120.0.0.3 area 0.0.0.0
S5comm(config-router)# network 150.0.0.3 area 1.1.1.1
iS5comm(config-router)# exit
```

2. In R3, create static routes and enable redistribution of static routes.

   FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# ip route 91.0.0.0 255.0.0.0 40.0.24.4
iS5comm(config)# router ospf
iS5comm(config-router)# redistribute static
iS5comm(config-router)#  end
```

3. In R2, shutdown interfaces Vlan12 and Vlan23

   FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# interface vlan 12
iS5comm(config-if)# shutdown
iS5comm(config-if)# end
iS5comm# configure terminal
iS5comm(config)# interface vlan 23
iS5comm(config-if)# shutdown
iS5comm(config-if)#
```

4. In R2, create route map aa and enable incoming filtering of routes in *OSPF*v2 with route map aa.

   FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# route-map aa permit 10
iS5comm(config-rmap-aa)# exit
iS5comm(config)# route-map aa deny 1
iS5comm(config-rmap-aa)# match destination ip 150.0.0.0 255.0.0.0
iS5comm(config-rmap-aa)# match destination ip 91.0.0.0 255.0.0.0
iS5comm(config-rmap-aa)# end
```

```
iS5comm(config)# router ospf
iS5comm(config-router)# distribute-list route-map aa in
```

5. In R2, shutdown interfaces Vlan12 and Vlan23

FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# interface vlan 12
iS5comm(config-if)# no shutdown
iS5comm(config-if)# end
iS5comm# configure terminal
iS5comm(config)# interface vlan 23
iS5comm(config-if)# no shutdown
iS5comm(config-if)#end
```

6. Wait for one minute for all route updates, and verify the routes in R2.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip route
Vrf Name:          default
C 10.0.0.0/8  is directly connected, vlan12
C 12.0.0.0/8  is directly connected, vlan1
O 20.0.0.0/8  [2] via 10.0.0.1
C 30.0.0.0/8  is directly connected, vlan23
C 100.0.0.0/8  is directly connected, vlan120
O 120.0.0.0/8  [2] via 30.0.0.3
O 130.0.0.0/8  [2] via 10.0.0.1
```

7. In R2, shutdown interfaces: Vlan12 and Vlan23

FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# interface vlan 12
iS5comm(config-if)# shutdown
iS5comm(config-if)# exit
iS5comm(config)# interface vlan 23
iS5comm(config-if)# shutdown
```

8. In R2, modify the route map aa.

FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# route-map aa permit 1
iS5comm(config-rmap-aa)# no match destination ip 91.0.0.0 255.0.0.0
iS5comm(config-rmap-aa)# match destination ip 92.0.0.0 255.0.0.0
iS5comm(config-rmap-aa)# exit
```

9. Start interfaces Vlan12 and Vlan23.

   FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# interface vlan 12
iS5comm(config-if)# no shutdown
iS5comm(config-if)# exit
iS5comm(config)# interface vlan 23
iS5comm(config-if)# no shutdown
iS5comm(config-if)# end
```

10. Wait for one minute for all route updates and verify the routes in R2.

    FOR EXAMPLE: Type the following:

```
iS5comm# show ip route
Vrf Name:          default
C 10.0.0.0/8  is directly connected, vlan12
C 12.0.0.0/8  is directly connected, vlan1
O 20.0.0.0/8  [2] via 10.0.0.1
C 30.0.0.0/8  is directly connected, vlan23
C 100.0.0.0/8  is directly connected, vlan120
O 120.0.0.0/8  [2] via 30.0.0.3
O 150.0.0.0/8  [2] via 30.0.0.3
```

11. In R2, shutdown interfaces Vlan12 and Vlan23.

    FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# interface vlan 12
iS5comm(config-if)# shutdown
iS5comm(config-if)# exit
iS5comm(config)# interface vlan 23
iS5comm(config-if)# shutdown
```

12. Delete the route map aa.

    FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# no route-map aa 1
iS5comm(config)# exit
```

13. Start interfaces Vlan12 and Vlan23.

    FOR EXAMPLE: Type the following:

```
iS5comm# configure terminal
iS5comm(config)# interface vlan 12
iS5comm(config-if)# no shutdown
```

```
iS5comm(config-if)# exitiS5comm(config)# interface vlan
23iS5comm(config-if)# no shutdowniS5comm(config-if)#end
iS5comm(config)# exit
```

14. Wait for one minute for all route updates, and verify the routes in R2.

    FOR EXAMPLE: Type the following:

```
iS5comm# show ip route
Vrf Name:         default
C 10.0.0.0/8  is directly connected,
vlan12C 12.0.0.0/8  is directly connected,
vlan1O 20.0.0.0/8  [2] via 10.0.0.1
C 30.0.0.0/8  is directly connected, vlan23
O 91.0.0.0/8  [10] via 30.0.0.2
C 100.0.0.0/8  is directly connected, vlan120
O 120.0.0.0/8  [2] via 30.0.0.3
O 130.0.0.0/8  [2] via 10.0.0.1
O 150.0.0.0/8  [2] via 30.0.0.3
```

3.11. Configuring OSPF Graceful Restart Support

The *OSPF GR* (Graceful Restart) support helps in increasing the availability of your network by allowing *OSPF* routers to stay on the forwarding path even if their *OSPF* software is restarted. The restarting router informs the neighbors about its capability to restart gracefully. The neighbors wait for a certain time interval before recalculating routes and diverting traffic. During this time interval, the *OSPF* software can be started up again and brought to its original state. The end result is that the traffic remains undisturbed.

CONTEXT:

OSPF supports two types of graceful restart:

- Planned
- Unplanned

Enabling / Disabling Graceful Restart Support

This configuration makes an OSPF router to support *GR* functionality. This section lists CLI configurations for enabling and disabling *GR* support on an OSPF router.

1. To enable the graceful support for the switch (ISS1):

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

   – Enable OSPF globally in the switch and enter the Router Configuration mode.

```
iS5comm(config)# router ospf
```

– Configure the OSPF router ID.

```
iS5comm (config-router)# router-id 10.10.2.1
```

– Enable opaque functionality.

```
iS5comm (config-router)# capability opaque
```

– Enable GR support. This configuration enables ISS1 to support both planned an un-planned restart.

```
iS5comm (config-router)# nsf ietf restart-support
```

– Exit from the Router Configuration mode.

```
iS5comm (config-router)# exit
```

2. View the graceful restart related configuration in ISS1.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf
OSPF Router with ID (10.10.2.1) (Vrf  default)
Supports multiple TOS routes
ABR Type supported is Standard ABR
Number of Areas in this router is 1
Area is 0.0.0.0
Number of interfaces in this area is 0
 SPF algorithm executed 0 times
Planned & Unplanned Non-Stop Forwarding enabled
Restart-interval limit: 120
Grace LSA Retransmission Count: 2
Helper Grace LSA ACK :Required
Restart Reason is:
Unknown
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

3. Execute the no form of the command to disable GR support.

FOR EXAMPLE: Type the following:

```
iS5comm(config-router)# no nsf ietf restart-support
```

Configuring Graceful Restart Interval

Graceful restart (*GR*) interval is the period of time during which the router can reacquire OSPF neighbors that are fully operational prior to the restart. The value ranges between 1 and 1800 seconds. The value is provided as an intimation of the grace period to all neighbors.

1. To enable the graceful restart interval for the switch (ISS1):

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

   ```
   iS5comm# configure terminal
   ```

   – Enable OSPF globally in the switch and enter the Router Configuration mode.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* router ID.

   ```
   iS5comm (config-router)# router-id 10.10.2.1
   ```

   – Configure the graceful restart timeout interval as 200 seconds.

   ```
   iS5comm(config-router)# nsf ietf restart-interval 200
   ```

   – Exit from the Router Configuration mode.

   ```
   iS5comm (config-router)# exit
   ```

2. View the graceful restart related configuration in ISS1.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf
   OSPF Router with ID (10.10.2.1) (Vrf  default)Supports multiple TOS
   routes
   ABR Type supported is Standard ABR
   Number of Areas in this router is 1
   Area is 0.0.0.0
   Number of interfaces in this area is 0
    SPF algorithm executed 0 times
   Planned & Unplanned Non-Stop Forwarding enabled
   Restart-interval limit: 200
   Grace LSA Retransmission Count: 2
   Helper Grace LSA ACK :Required
   Restart Reason is:
   Unknown
   Helper is Giving Support for:
   Unknown
   Software Restart
   Software Reload/Upgrade
   Switch To Redundant
   Helper Grace Time Limit: 0
   Strict LSA checking State Is:Disabled
   ```

```
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

3. Execute the no form of the command to reset the graceful restart interval to default value (120 seconds.

   FOR EXAMPLE: Type the following:

```
iS5comm(config-router)# no nsf ietf restart-interval
```

Configuring Grace LSA Acknowledgement Required

This configuration enables Grace Ack Required state in the restarting router. If the Grace Ack Required state is enabled, then the Grace -LSAs sent by this router need to be acknowledged by peers. By default, this state is enabled in the restarting router.

1. To enable Grace LSA Ack required state for the switch (ISS1):

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

```
iS5comm(config)# router ospf
```

   – Configure the *OSPF* router ID.

```
iS5comm (config-router)# router-id 10.10.2.1
```

   – Configure the Grace-LSA Ack required state as enabled in ISS1.

```
iS5comm(config-router)# nsf ietf grace lsa ack required
```

   – Exit from the Router Configuration mode.

```
iS5comm (config-router)# exit
```

2. View the configuration done in ISS1.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf
OSPF Router with ID (10.10.2.1) (Vrf  default)Supports multiple TOS
routes
ABR Type supported is Standard ABR
Number of Areas in this router is 1
Area is 0.0.0.0
Number of interfaces in this area is 0
 SPF algorithm executed 0 times
Planned & Unplanned Non-Stop Forwarding enabled
Restart-interval limit: 200
Grace LSA Retransmission Count: 2
Helper Grace LSA ACK :Required
Restart Reason is:
Unknown
```

```
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

3. Execute the no form of the command to reset the graceful restart interval to default value (120 seconds.

   FOR EXAMPLE: Type the following:

```
iS5comm(config-router)# no nsf ietf restart-interval
```

Configuring Grace LSA Retransmission Count

This section lists CLI configurations for configuring the maximum number of retransmissions for unacknowledged GraceLSA. This value ranges between 0 and 180.

1. To configure Grace-LSA retransmission count to 100 for the switch (ISS1):

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

```
iS5comm(config)# router ospf
```

   – Configure the *OSPF* router ID.

```
iS5comm (config-router)# router-id 10.10.2.1
```

   – Configure the Grace LSA retransmission count as 100 in ISS1.

```
iS5comm(config-router)# nsf ietf grlsa retrans count 100
```

   – Exit from the Router Configuration mode.

```
iS5comm (config-router)# exit
```

2. View the configuration done in ISS1.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf
OSPF Router with ID (10.10.2.1) (Vrf  default)Supports multiple TOS
routes
ABR Type supported is Standard ABR
Number of Areas in this router is 1
Area is 0.0.0.0
Number of interfaces in this area is 0
 SPF algorithm executed 0 times
```

```
Planned & Unplanned Non-Stop Forwarding enabled
Restart-interval limit: 200
Grace LSA Retransmission Count: 100
Helper Grace LSA ACK :Required
Restart Reason is:
Unknown
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

Configuring Graceful Restart Reason

This section lists the configuration to set the incidence for which *GR* feature is applied. *GR* reason can be unknown, softwareRestart, swReloadUpgrade, and switchToRedundant. By default, restart reason is set as unknown.

1. To enable Grace LSA Ack required state for the switch (ISS1):

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* router ID.

   ```
   iS5comm (config-router)# router-id 10.10.2.1
   ```

   – Configure the restart reason as software Restart in ISS1.

   ```
   iS5comm(config-router)# nsf ietf restart-reason softwareRestart
   ```

   – Exit from the Router Configuration mode.

   ```
   iS5comm (config-router)# exit
   ```

2. View the configuration done in ISS1.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf
   OSPF Router with ID (10.10.2.1) (Vrf  default)
   Supports multiple TOS routes
   ABR Type supported is Standard ABR
   Number of Areas in this router is 1
   ```

```
Area is 0.0.0.0
Number of interfaces in this area is 0
 SPF algorithm executed 0 times
Planned & Unplanned Non-Stop Forwarding enabled
Restart-interval limit: 200
Grace LSA Retransmission Count: 2
Helper Grace LSA ACK :Required
Restart Reason is:
Software Restart
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

Configuring Graceful Restart Helper Support

The neighbors of the restarting routers can act as helpers depending on their helper support configurations. This section lists the *CLI* configurations related to helper support.

Enabling / Disabling Graceful Restart Helper Support

The neighbors of the restarting routers acts as helper during the graceful restart based on their support configurations. By default the routers are enabled to act as a helping neighbor and can support all four types of restart reasons such as unknown, softwareRestart, swReloadUpgrade and switchToRedundant

1. To enable Grace *LSA* Ack required state for the switch (ISS1):

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* router ID.

   ```
   iS5comm (config-router)# router-id 10.10.2.1
   ```

   – Configure the helper support as softwareRestart in ISS1.

   ```
   iS5comm(config-router)# nsf ietf helper-support softwareRestart
   ```

   – Exit from the Router Configuration mode.

   ```
   iS5comm (config-router)# exit
   ```

2. View the configuration done in ISS1.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf
OSPF Router with ID (10.10.2.1) (Vrf  default)
Supports multiple TOS routes
ABR Type supported is Standard ABR
Number of Areas in this router is 1
Area is 0.0.0.0
Number of interfaces in this area is 0
 SPF algorithm executed 0 times
Planned & Unplanned Non-Stop Forwarding enabled
Restart-interval limit: 200
Grace LSA Retransmission Count: 2
Helper Grace LSA ACK :Required
Restart Reason is:
Software Restart
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

3. Execute the no form of the command to disable the helper support in the router (ISS1).

   FOR EXAMPLE: Type the following:

```
iS5comm(config-router)# no nsf ietf helper-support softwareRestart
```

Configuring Grace Time Limit for the Helper

The neighbors of the restarting routers acts as helper during the graceful restart based on their support configurations. By default the routers are enabled to act as a helping neighbor and can support all four types of restart reasons such as unknown, softwareRestart, swReloadUpgrade and switchToRedundant

1. To enable Grace LSA Ack required state for the switch (ISS1):

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

```
iS5comm(config)# router ospf
```

- Configure the *OSPF* router ID.

```
iS5comm (config-router)# router-id 10.10.2.1
```

- Enable the helper support in ISS1.

```
iS5comm(config-router)# nsf ietf helper-support softwareRestart
```

- Configure the helper grace time limit as 100 in ISS1.

```
iS5comm(config-router)# nsf ietf helper gracetimelimit 100
```

- Exit from the Router Configuration mode.

```
iS5comm (config-router)# exit
```

2. View the configuration done in ISS1.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf
OSPF Router with ID (10.10.2.1) (Vrf  default)
Supports multiple TOS routes
ABR Type supported is Standard ABR
Number of Areas in this router is 1
Area is 0.0.0.0
Number of interfaces in this area is 0
 SPF algorithm executed 0 times
Planned & Unplanned Non-Stop Forwarding enabled
Restart-interval limit: 200
Grace LSA Retransmission Count: 2
Helper Grace LSA ACK :Required
Restart Reason is:
Software Restart
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 100
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

Configuring Strict-LSA Check Option in Helper

The strict *LSA* check option allows the helper to terminate the graceful restart, once a changed LSA that causes flooding during the restart process is detected.

1. To configure the strict-*LSA* check option for the helping switch (ISS1):

FOR EXAMPLE: Type the following:

- Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

- Enable *OSPF* globally in the switch and enter the Router Configuration mode.

```
iS5comm(config)# router ospf
```

- Configure the *OSPF* router ID.

```
iS5comm (config-router)# router-id 10.10.2.1
```

- Configure the helper support as softwareRestart in ISS1.

```
iS5comm(config-router)# nsf ietf helper-support softwareRestart
```

- Enable the strict *LSA* check option in ISS1.

```
iS5comm(config-router)# nsf ietf helper strict-lsa-checking
```

- Exit from the Router Configuration mode.

```
iS5comm (config-router)# exit
```

2. View the configuration done in ISS1.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf
OSPF Router with ID (10.10.2.1) (Vrf  default)
Supports multiple TOS routes
ABR Type supported is Standard ABR
Number of Areas in this router is 1
Area is 0.0.0.0
Number of interfaces in this area is 0
 SPF algorithm executed 0 times
Planned & Unplanned Non-Stop Forwarding enabled
Restart-interval limit: 200
Grace LSA Retransmission Count: 2
Helper Grace LSA ACK :Required
Restart Reason is:
Software Restart
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Enabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

3. Execute the no form of the command to disable the strict-*LSA* check option for the helping switch (ISS1)

   FOR EXAMPLE: Type the following:

   ```
   iS5comm(config-router)# no nsf ietf helper strict-lsa-checking
   ```

3.12. Sample Configuration for Testing OSPF Planned Graceful Restart

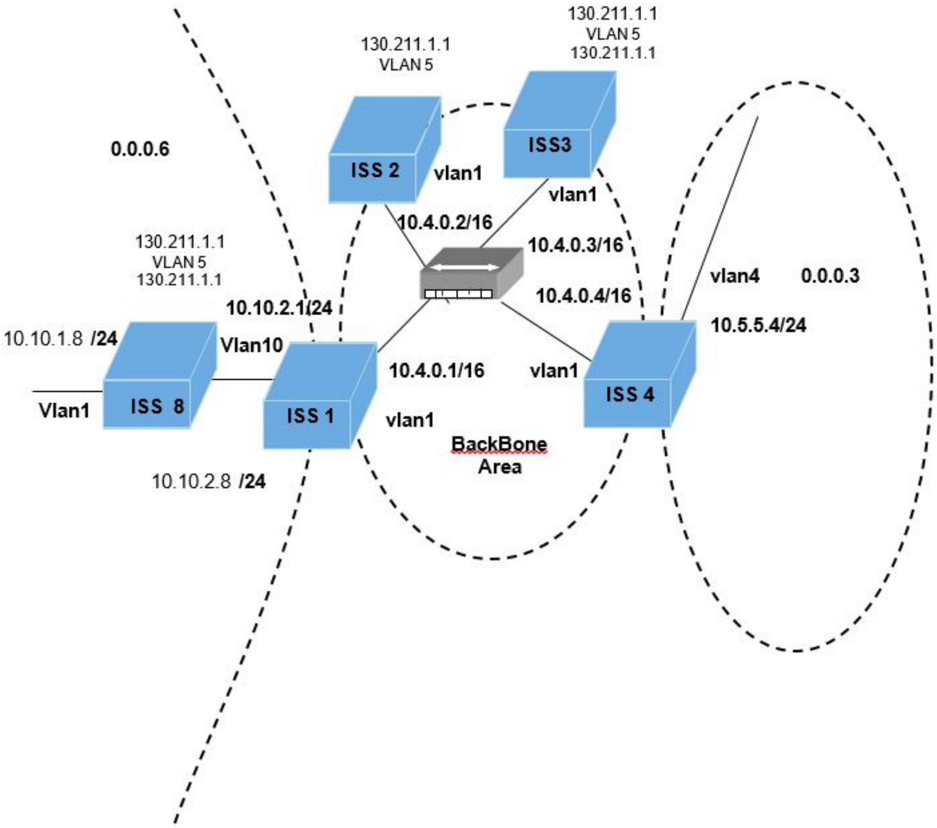
During a planned restart, the restarting router informs the neighbors before restarting. The neighbors act as if the router is still within the network topology and continue forwarding traffic to the restarting router. A grace period is set to specify the time period till which the neighbors should consider the restarting router as part of the topology.

PREREQUISITE:

The prerequisite configuration mentioned in section 3.2 Configuration Guidelines (Prerequisite) should be done in the switches ISS1, ISS2, ISS3, ISS4, and ISS8 before configuring *OSPF*.

CONTEXT:

Figure 9: Topology for Testing OSPF Planned Graceful Restart



Configurations in ISS1:

1. Execute the following commands.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* router ID.

   ```
   iS5comm (config-router)# router-id 10.10.2.1
   ```

   – Configure the *OSPF* interfaces.

   ```
   iS5comm (config-router)# network 10.4.0.1 area 0.0.0.0
   ```

   – Enable opaque functionality in ISS1.

   ```
   iS5comm (config-router)# capability opaque
   ```

   – Enable graceful restart support in ISS1. This configuration enables ISS1 to support planned restart.

   ```
   iS5comm (config-router)# nsf ietf restart-support plannedOnly
   ```

   – Configure the graceful restart timeout interval as 50 seconds in ISS1.

   ```
   iS5comm (config-router)# nsf ietf restart-interval 50
   ```

   – Configure the Grace-LSA Ack required state as enabled in ISS1.

   ```
   iS5comm (config-router)# nsf ietf grace lsa ack required
   ```

   – Configure the Grace LSA retransmission count as 100 in ISS1.

   ```
   iS5comm (config-router)# nsf ietf grlsa retrans count 100
   ```

   – Exit the Router Configuration Mode.

   ```
   iS5comm (config-router)# end
   ```

2. View the Configuration done in ISS1.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf
   OSPF Router with ID (10.10.2.1) (Vrf  default)
   Supports only single TOS(TOS0) route
   ABR Type supported is Standard ABR
   It is an Area Border Router
   Number of Areas in this router is 2
   Area is 0.0.0.6
   Number of interfaces in this area is 1
   SPF algorithm executed 9 times
   Area is 0.0.0.0
   Number of interfaces in this area is 1
   SPF algorithm executed 9 times
   Planned Non-Stop Forwarding enabled
   ```

```
Restart-interval limit: 50
Grace LSA Retransmission Count: 100
Helper Grace LSA ACK :Required
Restart Reason is:
Unknown
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

Configurations in ISS2

3. Execute the following commands.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS2.

   ```
   iS5comm# configure terminal
   ```

   – Enable OSPF globally in the switch and enter the Router Configuration mode.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the OSPF router ID.

   ```
   iS5comm (config-router)# router-id 10.10.2.2
   ```

   – Configure the OSPF interfaces.

   ```
   iS5comm (config-router)# network 10.4.0.2 area 0.0.0.0
   ```

   – Exit the Router Configuration Mode.

   ```
   iS5comm (config-router)# end
   ```

4. View the Configuration done in ISS2. Also check, if by default ISS2 is providing helper support for all four type of restart reasons.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf
   OSPF Router with ID (10.10.2.2) (Vrf  default)
   Supports only single TOS(TOS0) route
   ABR Type supported is Standard ABR
   It is an Area Border Router
   Number of Areas in this router is 2
   Area is 0.0.0.6
   Number of interfaces in this area is 1
   ```

```
SPF algorithm executed 9 times
Area is 0.0.0.0
Number of interfaces in this area is 1
SPF algorithm executed 9 times
Planned Non-Stop Forwarding enabled
Restart-interval limit: 50
Grace LSA Retransmission Count: 100
Helper Grace LSA ACK :Required
Restart Reason is:
Unknown
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

Configurations in ISS3

5. Execute the following commands.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS3.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* router ID.

   ```
   iS5comm (config-router)# router-id 10.1.1.3
   ```

   – Configure the *OSPF* interfaces.

   ```
   iS5comm (config-router)# network 10.4.0.3 area 0.0.0.0
   ```

   – Exit the Router Configuration Mode.

   ```
   iS5comm (config-router)# end
   ```

6. View the configuration done in ISS3. Also check, if by default ISS3 is providing helper support for all four type of restart reasons.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf
   OSPF Router with ID (10.1.1.3) (Vrf  default)
   Supports only single TOS(TOS0) route
   ```

```
ABR Type supported is Standard ABR
It is an Area Border Router
Number of Areas in this router is 2
Area is 0.0.0.6
Number of interfaces in this area is 1
SPF algorithm executed 9 times
Area is 0.0.0.0
Number of interfaces in this area is 1
SPF algorithm executed 9 times
Planned Non-Stop Forwarding enabled
Restart-interval limit: 50
Grace LSA Retransmission Count: 100
Helper Grace LSA ACK :Required
Restart Reason is:
Unknown
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

Configurations in ISS4

7. Execute the following commands.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS4.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* router ID.

   ```
   iS5comm (config-router)# router-id 10.5.5.4
   ```

   – Configure the *OSPF* interfaces.

   ```
   iS5comm(config-router)# network 10.5.5.4 area 0.0.0.0
   iS5comm(config-router)# network 10.4.0.4 area 0.0.0.0
   ```

   – Exit the Router Configuration Mode.

   ```
   iS5comm (config-router)# end
   ```

8. View the Configuration done in ISS3. Also check, if by default ISS3 is providing helper support for all four type of restart reasons.

   FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf
OSPF Router with ID (10.5.5.4)(Vrf  default)
Supports only single TOS(TOS0) route
ABR Type supported is Standard ABR
It is an Area Border Router
Number of Areas in this router is 2
Area is 0.0.0.6
Number of interfaces in this area is 1
SPF algorithm executed 9 times
Area is 0.0.0.0
Number of interfaces in this area is 1
SPF algorithm executed 9 times
Planned Non-Stop Forwarding enabled
Restart-interval limit: 50
Grace LSA Retransmission Count: 100
Helper Grace LSA ACK :Required
Restart Reason is:
Unknown
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

Configurations in ISS8

9. Execute the following commands.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS8.

```
iS5comm# configure terminal
```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

```
iS5comm(config)# router ospf
```

   – Configure the *OSPF* router ID.

```
iS5comm (config-router)# router-id 10.10.2.8
```

– Configure the *OSPF* interfaces.

```
iS5comm(config-router)# network 10.10.2.8 area 0.0.0.6
iS5comm(config-router)# network 10.10.1.8 area 0.0.0.6
```

– Exit the Router Configuration Mode.

```
iS5comm (config-router)# end
```

10. View the configuration done in ISS8. Also check, if by default ISS8 is providing helper support for all four type of restart reasons.

    FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf
OSPF Router with ID (10.10.2.8) (Vrf  default)
Supports only single TOS(TOS0) route
ABR Type supported is Standard ABR
It is an Area Border Router
Number of Areas in this router is 2
Area is 0.0.0.6
Number of interfaces in this area is 1
SPF algorithm executed 9 times
Area is 0.0.0.0
Number of interfaces in this area is 1
SPF algorithm executed 9 times
Planned Non-Stop Forwarding enabled
Restart-interval limit: 50
Grace LSA Retransmission Count: 100
Helper Grace LSA ACK :Required
Restart Reason is:
Unknown
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

Configurations for checking GR functionality

11. Observe the *IP* routing Table in ISS4. It should have route to 10.10.2.0 network with next hop as ISS1's vlan1 interface.

    FOR EXAMPLE: Type the following:

    ```
    iS5comm# show ip route
    Codes: C - connected, S - static, R - rip, B - bgp, O - ospf
    Vrf Name:          default
    ---------
    C 10.4.0.0/16 is directly connected, vlan1
    C 10.5.5.0/24 is directly connected, vlan4
    C 10.5.6.0/24 is directly connected, vlan3
    O 10.10.1.0/24 [3] via 10.4.0.1
    O 10.10.2.0/24 [2] via 10.4.0.1
    ```

12. Observe the *IP* routing Table in ISS4. It should have route to 10.10.2.0 network with next hop as ISS1's vlan1 interface.

    FOR EXAMPLE: Type the following:

    ```
    iS5comm(config)# shutdown ospf
    ```

13. View the packets sent on vlan1 interface of ISS1. You can see the Grace-LSA from ISS1 sent on that interface.

    FOR EXAMPLE: Type the following:

    ```
    Frame 2 (106 bytes on wire, 106 bytes captured)
    Arrival Time: Feb 17, 2011 10:05:57.329311000
    [Time delta from previous packet: 1.781175000 seconds]
    [Time since reference or first frame: 1.781175000 seconds]

    Open Shortest Path First
    OSPF Header
    OSPF Version: 2
    Message Type: LS Update (4)
    Packet Length: 72Source OSPF Router: 10.10.2.1 (10.10.2.1)
    Area ID: 0.0.0.0 (Backbone)
    Packet Checksum: 0xaaed [correct]
    Auth Type: Null
    Auth Data (none)
    LS Update Packet
    Number of LSAs: 1
    LS Type: Opaque LSA, Link-local scope
    LS Age: 1 seconds
    Options: 0x00 ()
    0... .... = DN: DN-bit is NOT set
    .0.. .... = O: O-bit is NOT set
    ```

```
..0. .... = DC: Demand circuits are NOT supported
...0 .... = L: The packet does NOT contain LLS data block
.... 0... = NP: Nssa is NOT supported
.... .0.. = MC: NOT multicast capable
.... ..0. = E: NO ExternalRoutingCapability
Link-State Advertisement Type: Opaque LSA, Link-local scope (9)
Link State ID Opaque Type: grace-LSA (3)
Link State ID Opaque ID: 0
Advertising Router: 10.10.2.1 (10.10.2.1)
LS Sequence Number: 0x80000001
LS Checksum: ac31
Length: 44
Unknown LSA Type 3
```

14. Observe the *IP* routing Table in ISS4. It should have route to 10.10.2.0 network with next hop as ISS1's vlan1 interface.

    FOR EXAMPLE: Type the following:

```
Open Shortest Path First
OSPF Header
OSPF Version: 2
Message Type: LS Acknowledge (5)
Packet Length: 44
Source OSPF Router: 10.1.1.3 (10.1.1.3)
Area ID: 0.0.0.0 (Backbone)
Packet Checksum: 0xb756 [correct]
Auth Type: Null
Auth Data (none)
LSA Header
LS Age: 1 seconds
Options: 0x00 ()
0... .... = DN: DN-bit is NOT set
.0.. .... = O: O-bit is NOT set
..0. .... = DC: Demand circuits are NOT supported
...0 .... = L: The packet does NOT contain LLS data block
.... 0... = NP: Nssa is NOT supported
.... .0.. = MC: NOT multicast capable
.... ..0. = E: NO ExternalRoutingCapability
Link-State Advertisement Type: Opaque LSA, Link-local scope (9)Link
State ID Opaque Type: grace-LSA (3)
Link State ID Opaque ID: 0
Advertising Router: 10.10.2.1 (10.10.2.1)
```

15. View the output in ISS1. You can see the value of remaining restart-interval and Restart Reason being changed as Software Restart.

    FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf
OSPF Router with ID (10.10.2.8) (Vrf  default)
Supports only single TOS(TOS0) route
ABR Type supported is Standard ABR
It is an Area Border Router
Number of Areas in this router is 1
Area is 0.0.0.6
Number of interfaces in this area is 1
SPF algorithm executed 32 times
Area is 0.0.0.0
Number of interfaces in this area is 1
SPF algorithm executed 9 times
Planned Non-Stop Forwarding enabled
Restart-interval limit: 50
Grace LSA Retransmission Count: 100
Helper Grace LSA ACK :Required
Restart Reason is:
Software Restart
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

16. Ping ISS8's VLAN 1 Interface (10.10.2.8) from ISS4. It should be successful.

    FOR EXAMPLE: Type the following:

```
iS5comm# ping 10.10.2.8
Reply Received From :10.10.2.8, TimeTaken : 60 msecs
Reply Received From :10.10.2.8, TimeTaken : 60 msecs
Reply Received From :10.10.2.8, TimeTaken : 60 msecs
--- 10.10.2.8 Ping Statistics ---
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
```

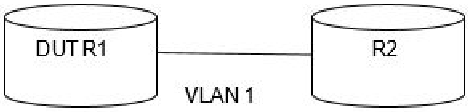
    NOTE: This shows that ISS1 is still in forwarding path although ISS1's *OSPF* module's state is set to shut down.

3.13. Configuring BFD over OSPF

Topology for Configuring and Testing OSPF-BFD

CONTEXT:

Figure 10: OSPF-BFD Configuration and Testing Topology



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

- R1 and R2 represent the routers.
- *VLAN* 1 represent the *VLAN* interfaces of the ISS routers.
- Each *ISS* switch has a router ID. *DUT* stands for device under test.

For the list of the IPv4 and IPv6 addresses of the interfaces and hosts provided in the figure above, refer to the table as follows.

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

Router	Interface	Slot	IPv4 Address / Mask	IPv6 Address/ Prefix Length
R1	VLAN 1	0/2	20.0.0.1 / 255.0.0.0	fe80::201:2ff:fe03:401 2001::2:0:0:1/64
R2	VLAN 1	0/2	20.0.0.1 / 255.0.0.0	fe80::202:2ff:fe03:401 2001::2:0:0:1/64

CLI Configurations

BFD can be used to monitor the IP path between *OSPF*v2 neighbors. For the Topology, refer to Figure *OSPF-BFD* Configuration and Testing Topology.

1. Execute the following commands at R1.

   FOR EXAMPLE: Type the following to configure OSPF router and BFD on OSPF router:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the O*OSPF*SPF interfaces.

   ```
   iS5comm (config-router)# network 20.0.0.1 area 0.0.0.0
   ```

   – Enable *BFD*.

   ```
   iS5comm(config)# enable bfd
   ```

   – Enable *BFD* on all interfaces.

```
iS5comm (config-router)# bfd all-interface
```

– Exit from the Router Configuration mode.

```
iS5comm(config-router)# end
```

2. Execute the following commands at R2.

   FOR EXAMPLE: Type the following to configure *OSPF* router and *BFD* on *OSPF* router:

   – Enter the Global Configuration Mode.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* interfaces.

   ```
   iS5comm (config-router)# network 20.0.0.2 area 0.0.0.0
   ```

   – Enable *BFD*.

   ```
   iS5comm(config)# enable bfd
   ```

   – Enable *BFD* on all interfaces.

   ```
   iS5comm (config-router)# bfd all-interface
   ```

   – Exit from the Router Configuration mode.

   ```
   iS5comm(config-router)# end
   ```

3. View the *BFD* status.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf neighbor
    Vrf  default
   Neighbor-ID  Pri   State        DeadTime   Address      Interface Helper
   -----------  ---   -----        --------   -------      ---------
   ---------   ------------ ---------  -----
   12.0.0.2     1     FULL/DR  33         20.0.0.2    vlan1     Not Helping
   HelperAge    HelperER Bfd
   ---------------   --------------- --------
   0                  None       enabled
   ```

4. Shutdown interface gi 0/2 at R2.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# configure terminal
   iS5comm(config)# int gi 0/2
   iS5comm(config)# shutdown
   iS5comm(config)# exit
   ```

5. Verify if the *BFD* status becomes disabled and the BFD session goes down.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf neighbor
    Vrf  default
   ```

```
Neighbor-ID  Pri   State        DeadTime   Address     Interface Helper
-----------  ---   -----        --------   -------     ---------
---------   ------------ ---------  -----
12.0.0.2     1     FULL/DR  33         20.0.0.2    vlan1     Not Helping
HelperAge    HelperER Bfd
---------------   --------------- --------
0                 None       disabled
```

SNMP Configurations

1. Enable *BFD* in *OSPF*.

   FOR EXAMPLE: Type the following:

   ```
   snmp0 set {{fsMIOspfBfdStatus.0 1}}
   {1.3.6.1.4.1.2076.145.1.3.1.33.0 Integer32 enabled}
   ```

2. Enable *BFD* in *OSPF* on all *OSPF* interfaces.

   FOR EXAMPLE: Type the following:

   ```
   snmp0 set {{fsMIOspfBfdAllIfState.0 1}}
   ```

   {1.3.6.1.4.1.2076.145.1.3.1.34.0 Integer32 enabled}

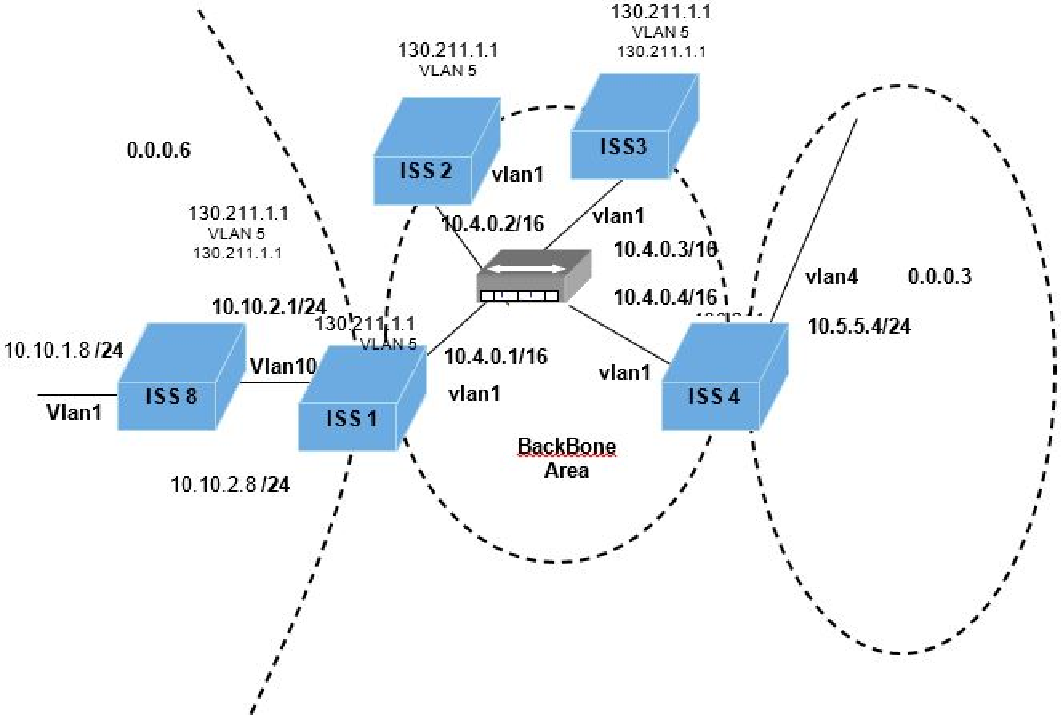
3.14. Sample Configuration for Testing OSPF Unplanned Graceful Restart

The restarting router will not send any Grace *LSA*s before shutdown, if the *OSPF GR* is configured as Un-Planned Restart. After restarting, the restarted router will send Grace *LSA*s in all its interfaces to inform that the unplanned-restart is successful.

PREREQUISITE:

The prerequisite configuration mentioned in section 3.2 Configuration Guidelines (Prerequisite) should be done in the switches ISS1, ISS2, ISS3, ISS4, and ISS8 before configuring *OSPF*.

CONTEXT: Topology for Testing OSPF Un-Planned Graceful Restart



Configurations in ISS1:

1. Execute the following commands.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS1.

```
iS5comm# configure terminal
```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

```
iS5comm(config)# router ospf
```

   – Configure the *OSPF* router ID.

```
iS5comm (config-router)# router-id 10.10.2.1
```

   – Configure the *OSPF* interfaces.

```
iS5comm (config-router)# network 10.4.0.1 area 0.0.0.0
iS5comm(config-router)# network 10.10.2.1 area 0.0.0.6
```

- Enable opaque functionality in ISS1

```
iS5comm (config-router)# capability opaque
```

- Enable graceful restart support in ISS1. This configuration enables ISS1 to support both planned and unplanned restart.

```
iS5comm (config-router)# nsf ietf restart-support
```

- Configure the graceful restart timeout interval as 50 seconds in ISS1

```
iS5comm (config-router)# nsf ietf restart-interval 50
```

- Exit the Router Configuration Mode.

```
iS5comm (config-router)# end
```

2. View the Configuration done in ISS1.

FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf
OSPF Router with ID (10.10.2.1) (Vrf  default)
Supports only single TOS(TOS0) route
ABR Type supported is Standard ABR
It is an Area Border Router
Number of Areas in this router is 2
Area is 0.0.0.6
Number of interfaces in this area is 1
SPF algorithm executed 9 times
Area is 0.0.0.0
Number of interfaces in this area is 1
SPF algorithm executed 9 times
Planned & Unplanned Non-Stop Forwarding enabled
Restart-interval limit: 50
Grace LSA Retransmission Count: 100
Helper Grace LSA ACK :Required
Restart Reason is:
Unknown
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

Configurations in ISS2

3. Execute the following commands.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS2.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* router ID.

   ```
   iS5comm (config-router)# router-id 10.10.2.2
   ```

   – Configure the *OSPF* interfaces.

   ```
   iS5comm (config-router)# network 10.4.0.2 area 0.0.0.0
   ```

   – Exit the Router Configuration Mode.

   ```
   iS5comm (config-router)# end
   ```

4. View the configuration done in ISS2. Also check, if by default ISS2 is providing helper support for all four type of restart reasons.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf
   OSPF Router with ID (10.10.2.2) (Vrf  default)
   Supports only single TOS(TOS0) route
   ABR Type supported is Standard ABR
   It is an Area Border Router
   Number of Areas in this router is 2
   Area is 0.0.0.6
   Number of interfaces in this area is 1
   SPF algorithm executed 9 times
   Area is 0.0.0.0
   Number of interfaces in this area is 1
   SPF algorithm executed 10 times
   Non-Stop Forwarding disabled
   Restart-interval limit: 50
   Grace LSA Retransmission Count: 100
   Helper Grace LSA ACK :Required
   Restart Reason is:
   Unknown
   Helper is Giving Support for:
   Unknown
   Software Restart
   Software Reload/Upgrade
   ```

```
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

Configurations in ISS3

5. Execute the following commands.

   For example: Type the following:

   – Enter the Global Configuration Mode in ISS3.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* router ID.

   ```
   iS5comm (config-router)# router-id 10.1.1.3
   ```

   – Configure the *OSPF* interfaces.

   ```
   iS5comm (config-router)# network 10.4.0.3 area 0.0.0.0
   ```

   – Exit the Router Configuration Mode.

   ```
   iS5comm (config-router)# end
   ```

6. View the Configuration done in ISS3. Also check, if by default ISS3 is providing helper support for all four type of restart reasons.

   For example: Type the following:

   ```
   iS5comm# show ip ospf
   OSPF Router with ID (10.1.1.3) (Vrf  default)
   Supports only single TOS(TOS0) route
   ABR Type supported is Standard ABR
   It is an Area Border Router
   Number of Areas in this router is 2
   Area is 0.0.0.6
   Number of interfaces in this area is 1
   SPF algorithm executed 9 times
   Area is 0.0.0.0
   Number of interfaces in this area is 1
   SPF algorithm executed 11 times
   Non-Stop Forwarding disabled
   Restart-interval limit: 50
   Grace LSA Retransmission Count: 100
   Helper Grace LSA ACK :Required
   Restart Reason is:
   ```

```
Unknown
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

Configurations in ISS4

7. Execute the following commands.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS4.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* router ID.

   ```
   iS5comm (config-router)# router-id 10.5.5.4
   ```

   – Configure the *OSPF* interfaces.

   ```
   iS5comm(config-router)# network 10.5.5.4 area 0.0.0.0
   iS5comm(config-router)# network 10.4.0.4 area 0.0.0.0
   ```

   – Exit the Router Configuration Mode.

   ```
   iS5comm (config-router)# end
   ```

8. View the Configuration done in ISS3. Also check, if by default ISS3 is providing helper support for all four type of restart reasons.

   FOR EXAMPLE: Type the following:

   ```
   iS5comm# show ip ospf
   OSPF Router with ID (10.5.5.4)(Vrf  default)
   Supports only single TOS(TOS0) route
   ABR Type supported is Standard ABR
   It is an Area Border Router
   Number of Areas in this router is 2
   Area is 0.0.0.6
   Number of interfaces in this area is 1
   SPF algorithm executed 9 times
   Area is 0.0.0.0
   Number of interfaces in this area is 1
   ```

```
SPF algorithm executed 9 times
Non-Stop Forwarding disabled
Restart-interval limit: 50
Grace LSA Retransmission Count: 100
Helper Grace LSA ACK :Required
Restart Reason is:
Unknown
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

Configurations in ISS8

9. Execute the following commands.

   FOR EXAMPLE: Type the following:

   – Enter the Global Configuration Mode in ISS8.

   ```
   iS5comm# configure terminal
   ```

   – Enable *OSPF* globally in the switch and enter the Router Configuration mode.

   ```
   iS5comm(config)# router ospf
   ```

   – Configure the *OSPF* router ID.

   ```
   iS5comm (config-router)# router-id 10.10.2.8
   ```

   – Configure the *OSPF* interfaces.

   ```
   iS5comm(config-router)# network 10.10.2.8 area 0.0.0.6
   iS5comm(config-router)# network 10.10.1.8 area 0.0.0.6
   iS5comm(config-router)# network 10.10.1.8 area 0.0.0.6
   ```

   – Exit the Router Configuration Mode.

   ```
   iS5comm (config-router)# end
   ```

10. View the configuration done in ISS8. Also check, if by default ISS8 is providing helper support for all four type of restart reasons.

    FOR EXAMPLE: Type the following:

    ```
    iS5comm# show ip ospf
    OSPF Router with ID (10.10.2.8) (Vrf  default)
    Supports only single TOS(TOS0) route
    ABR Type supported is Standard ABR
    ```

```
It is an Area Border Router
Number of Areas in this router is 2
Area is 0.0.0.6
Number of interfaces in this area is 1
SPF algorithm executed 9 times
Area is 0.0.0.0
Number of interfaces in this area is 1
SPF algorithm executed 9 times
Non-Stop Forwarding disabled
Restart-interval limit: 50
Grace LSA Retransmission Count: 100
Helper Grace LSA ACK :Required
Restart Reason is:
Unknown
Helper is Giving Support for:
Unknown
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

Configurations for checking GR functionality

11. Observe the *IP* routing Table in ISS4. It should have route to 10.10.2.0 network with next hop as ISS1's vlan1 interface.

    FOR EXAMPLE: Type the following:

```
iS5comm# show ip route
Codes: C - connected, S - static, R - rip, B - bgp, O - ospf
Vrf Name:          default
---------
C 10.4.0.0/16 is directly connected, vlan1
C 10.5.5.0/24 is directly connected, vlan4
C 10.5.6.0/24 is directly connected, vlan3
O 10.10.1.0/24 [3] via 10.4.0.1
O 10.10.2.0/24 [2] via 10.4.0.1
```

12. Observe the *IP* routing Table in ISS4. It should have route to 10.10.2.0 network with next hop as ISS1's vlan1 interface.

    FOR EXAMPLE: Type the following:

    ```
    iS5comm(config)# shutdown ospf
    ```

13. View the packets sent on vlan1 interface of ISS1. You can see the Grace-LSA from ISS1 sent on that interface.

    FOR EXAMPLE: Type the following:

    ```
    iS5comm# show ip ospf
    OSPF Router with ID (10.10.2.8) (Vrf  default)
    Supports only single TOS(TOS0) route
    ABR Type supported is Standard ABR
    It is an Area Border Router
    Number of Areas in this router is 2
    Area is 0.0.0.6
    Number of interfaces in this area is 1
    SPF algorithm executed 9 times
    Area is 0.0.0.0
    Number of interfaces in this area is 1
    SPF algorithm executed 9 times
    Non-Stop Forwarding disabled
    Restart-interval limit: 50
    Grace LSA Retransmission Count: 100
    Helper Grace LSA ACK :Required
    Restart Reason is:
    Unknown
    Helper is Giving Support for:
    Unknown
    Software Restart
    Software Reload/Upgrade
    Switch To Redundant
    Helper Grace Time Limit: 0
    Strict LSA checking State Is:Disabled
    Route calculation staggering is enabled
    Route calculation staggering interval is  10 seconds
    ```

14. Observe the *IP* routing Table in ISS4. It should have route to 10.10.2.0 network with next hop as ISS1's vlan1 interface.

    FOR EXAMPLE: Type the following:

    ```
    Open Shortest Path First
    OSPF Header
    OSPF Version: 2
    ```

```
Message Type: LS Acknowledge (5)
Packet Length: 44
Source OSPF Router: 10.1.1.3 (10.1.1.3)
Area ID: 0.0.0.0 (Backbone)
Packet Checksum: 0xb756 [correct]
Auth Type: Null
Auth Data (none)
LSA Header
LS Age: 1 seconds
Options: 0x00 ()
0... .... = DN: DN-bit is NOT set
.0.. .... = O: O-bit is NOT set
..0. .... = DC: Demand circuits are NOT supported
...0 .... = L: The packet does NOT contain LLS data block
.... 0... = NP: Nssa is NOT supported
.... .0.. = MC: NOT multicast capable
.... ..0. = E: NO ExternalRoutingCapability
Link-State Advertisement Type: Opaque LSA, Link-local scope (9)Link
State ID Opaque Type: grace-LSA (3)
Link State ID Opaque ID: 0
Advertising Router: 10.10.2.1 (10.10.2.1)
```

15. View the output in ISS1. You can see the value of remaining restart-interval and Restart Reason being changed as Software Restart.

    FOR EXAMPLE: Type the following:

```
iS5comm# show ip ospf
OSPF Router with ID (10.10.2.1) (Vrf  default)
Supports only single TOS(TOS0) route
ABR Type supported is Standard ABR
It is an Area Border Router
Number of Areas in this router is 2
Area is 0.0.0.6
Number of interfaces in this area is 1
SPF algorithm executed 7 times
Area is 0.0.0.0
Number of interfaces in this area is 1
SPF algorithm executed 7 times
Planned & Unplanned Non-Stop Forwarding enabled
Restart-interval limit: 50
Grace LSA Retransmission Count: 100
Helper Grace LSA ACK :Required
```

```
Restart Reason is:
Software Restart
Helper is Giving Support for:
Software Restart
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled
Route calculation staggering is enabled
Route calculation staggering interval is  10 seconds
```

16. Ping ISS8's vlan 1 Interface (10.10.2.8) from ISS4. It should be successful.

    FOR EXAMPLE: Type the following:

```
iS5comm# ping 10.10.2.8
Reply Received From :10.10.2.8, TimeTaken : 60 msecs
Reply Received From :10.10.2.8, TimeTaken : 60 msecs
Reply Received From :10.10.2.8, TimeTaken : 60 msecs
--- 10.10.2.8 Ping Statistics ---
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
```

NOTE: This shows that ISS1 is still in forwarding path although ISS1's OSPF module's state is set to shut down.