



Ethernet Routing Switch

8000

Virtual Services Platform

9000

Engineering

> Resilient Multicast Routing Using Split-Multilink Trunking Technical Configuration Guide

Avaya Data Solutions

Document Date: Nov 2011

Document Number: NN48500-544

Document Version: 2.0

© 2011 Avaya Inc.
All Rights Reserved.

Notices

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: <http://www.avaya.com/support>

Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright

Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support. Web site: <http://www.avaya.com/support>

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com/support>.

Abstract

This Technical Configuration Guide (TCG) describes the supported network designs and configurations for Protocol Independent Multicast Sparse Mode (PIM-SM) over Avaya's Split Multi-Link Trunking for the Ethernet Routing Switch 8300, Ethernet Routing Switch 8000, and Virtual Services Platform 9000. All configuration examples are based on the software and hardware level as shown below.

Switch	Software Level
ERS8300	4.3.x
ERS8800	7.1.x
ERS8600	5.1.x
VSP9000	3.1.x

Acronym Key

Throughout this guide the following acronyms will be used:

- AS: Autonomous System
- BSR: Bootstrap Router
- DMLT: Distributed MultiLink Trunking
- DR: Designated Router
- ERS: Ethernet Routing Switch
- IGMP: Internet Group Management Protocol
- IGP: Interior Gateway Protocol
- IPMC: IP Multicast
- IST: InterSwitch Trunk
- MHR: Multicast Host Reports
- MLT: MultiLink Trunking
- MSDP: Multicast Source Discovery Protocol
- PIM: Protocol Independent Multicast
- PIM-SM: PIM Sparse Mode
- PIM-SSM: PIM Source Specific Multicast
- PIM RP: PIM Rendezvous Point
- PIM BSR: PIM Bootstrap Router
- RP: Rendezvous Point
- RSMLT: Routed Split MultiLink Trunking
- SLPP: Simple Loop Prevention Protocol
- SLT: Single Port Split MultiLink Trunking
- SPT: Shortest Path Tree
- SMLT: Split MultiLink Trunking
- STG: Spanning Tree Group
- VLACP: Virtual Link Aggregation Control Protocol
- VSP: Virtual Services Platform
- VRRP: Virtual Router Redundancy Protocol

Revision Control

No	Date	Version	Revised By	Remarks
1	4/11/2011	2.0	John Vant Erve	

Table of Contents

Figures	10
Tables.....	11
1. Multicast Overview	13
1.1 PIM-SM Multicast Distribution Trees.....	13
1.2 Interdomain PIM-SM Multicast using Multicast Source Discovery Protocol (MSDP)	14
1.3 PIM-SSM – Source Specific Trees	15
1.4 Multicast Support on Avaya Modular Switches	16
1.5 Multicast Support on Avaya Stackable Switches	18
2. Internet Group Management Protocol.....	19
2.1 IGMP on L2 SMLT Access Switches	19
2.2 IGMP Reporting Fields on SMLT Layer 2 Access Switches.....	21
2.3 IGMP and SMLT on the ERS 8300, ERS 8000, and VSP 9000	22
2.4 SSM and IGMPv2	24
2.5 SSM and IGMPv3	24
2.6 IGMP Access Control.....	24
2.7 IGMP Fast Leave feature	25
2.8 IGAP (Internet Group Authentication and Accounting Protocol).....	25
2.9 ERS 8000 & ERS 8300 - IGMPv3 Backward Compatibility	26
3. PIM-SM Design Guidelines	27
4. PIM-SSM Design Guidelines	28
4.1 SMLT Hashing Algorithm for Multicast.....	29
4.1.1 VSP 9000	29
4.1.2 ERS 8800 (R/Rs Modules) and ERS 8600 (E-modules only)	30
4.1.3 ERS 8300.....	33
4.1.4 ERS 5000, ERS 4000, and ERS 2500	33
4.2 Multicast Scaling Numbers.....	34
4.2.1 ERS 8000.....	34
4.2.2 VSP 9000.....	35
4.3 Supported Multicast SMLT Topologies	36
4.3.1 SMLT Triangle – Layer 2 Cluster.....	36
4.3.2 SMLT Triangle – Layer 3 Cluster, Layer 2 Access	37
4.3.3 SMLT Triangle – Layer 3 Cluster, Layer 3 Access	38
4.3.4 SMLT Square – Layer 2 Cluster.....	39
4.3.5 SMLT Square – Layer 3 Cluster.....	40
4.3.6 SMLT Full Mesh – Layer 3 Cluster.....	41

5.	Configuring PIM using SMLT	42
5.1	PIM-SM RSMLT Triangle Topology with L2 Edge	43
5.1.1	Configuration – ERS 8000 cluster	45
5.1.1.1	IST Configuration	45
5.1.1.2	Create Routed VLAN	46
5.1.1.3	Create Access VLANs.....	47
5.1.1.4	VLACP	49
5.1.1.5	Discard Untagged Frames	49
5.1.1.6	SLPP	50
5.1.1.7	Enable RSMLT Edge	50
5.1.1.8	Circuitless/Loopback IP address configuration	51
5.1.1.9	OSPF Configuration	51
5.1.1.10	PIM Configuration.....	52
5.1.2	Configuration – Edge Switch	54
5.1.2.1	Create VLAN	54
5.1.2.1	Create MLT	54
5.1.2.1	VLACP	54
5.1.2.2	Enable Spanning Tree FastStart and BPDU filtering on all access ports	55
5.1.2.1	Discard Untagged Frames	55
5.1.2.1	Enable IGMP Snoop/Proxy	56
5.1.3	Verify Operations.....	57
5.1.3.1	IGMP	57
5.1.3.2	PIM	61
5.1.3.3	Verify multicast routing table	65
5.2	PIM-SM Anycast-RP Triangle Topology with L2 Edge – VSP9000	71
5.2.1	Configuration – VSP 9000 cluster	73
5.2.1.1	IST Configuration	73
5.2.1.2	Create Access VLANs.....	75
5.2.1.3	Create Mgmt VLAN	77
5.2.1.4	VLACP – To Edge Switch	78
5.2.1.5	Discard Untagged Frames	78
5.2.1.6	SLPP	79
5.2.1.7	Enable RSMLT Edge	79
5.2.1.8	Loopback IP address configuration.....	80
5.2.1.9	IP Route Configuration	81

5.2.1.10	PIM Configuration.....	81
5.2.2	Configuration – Edge Switch	83
5.2.2.1	Create Management VLAN	83
5.2.2.2	Create User Traffic VLAN	83
5.2.2.3	Create MLT	84
5.2.2.4	VLACP	84
5.2.2.5	Enable Spanning Tree FastStart and BPDU filtering on all access ports	85
5.2.2.6	Discard Untagged Frames	85
5.2.2.7	Enable IGMP Snoop/Proxy	85
5.2.3	Verify Operations.....	86
5.2.3.1	IGMP	86
5.2.3.2	PIM	89
5.3	PIM-SM SMLT Triangle Topology Design with L3 Edge	91
5.3.1	8000 SMLT Cluster	93
5.3.1.1	IST Configuration	93
5.3.1.2	SMLT Configuration	94
5.3.1.3	Enable RSMLT	95
5.3.1.4	VLACP	96
5.3.1.5	Discard Untagged Frames	96
5.3.1.6	SLPP	97
5.3.1.7	Circuitless/Loopback IP address configuration	97
5.3.1.8	OSPF Configuration	98
5.3.1.9	PIM Configuration.....	99
5.3.2	ERS5000 Configuration.....	100
5.3.2.1	Create VLANs	100
5.3.2.2	Create MLT to 8000 SMLT Cluster	101
5.3.2.3	VLACP	101
5.3.2.4	Enable Spanning Tree FastStart and BPDU filtering on all access ports	102
5.3.2.5	OSPF Configuration	102
5.3.2.6	PIM Configuration.....	103
5.3.3	Verify Operation	105
5.3.3.1	IGMP	105
5.3.3.2	PIM	109
5.3.3.3	Verify Multicast Routing Table	117
5.4	PIM-SSM SMLT Triangle Topology Design with L3 Edge	130

5.4.1	8000 SMLT Cluster	131
5.4.1.1	PIM Configuration.....	131
5.4.1.1	ERS5000 Configuration	132
5.4.2	Verify Operations.....	133
5.4.2.1	IGMP	133
5.4.2.1	Verify Multicast Routing Table	138
5.5	PIM-SM RSMLT Square/Mesh Topology.....	142
5.5.1	Configuration – ERS 8000 cluster.....	144
5.5.1.1	IST Configuration	144
5.5.1.2	SMLT Configuration	146
5.5.1.3	Enable RSMLT	149
5.5.1.4	Circuitless/Loopback IP address configuration	150
5.5.1.5	OSPF Configuration	151
5.5.1.6	PIM Configuration.....	153
5.5.2	Verify Operations.....	155
5.5.2.1	IGMP	155
5.5.2.2	PIM	160
5.5.2.1	Verify multicast routing table	167
5.6	PIM-SM Static RP RSMLT Square/Mesh Design	172
5.6.1	8000 SMLT Cluster	174
5.6.1.1	PIM	174
6.	Reference Documentation	177
7.	Customer service	178
7.1	Getting technical documentation.....	178
7.2	Getting product training.....	178
7.3	Getting help from a distributor or reseller.....	178
7.4	Getting technical support from the Avaya Web site.....	178

Figures

Figure 1: IGMP Snooping Feature	19
Figure 2: IGMP Proxy Feature	19
Figure 3: The unknown-mcast-no-flood feature stops multicast traffic from flooding all ports in a vlan	20
Figure 4: IGMP Reporting Fields on L2 Switch.....	21
Figure 5: IGMP Interaction with SMLT	22
Figure 6: L2 IGMP SMLT Triangle Topology	36
Figure 7: PIM-SM SMLT Triangle Topology	37
Figure 8: PIM-SM SMLT Distribution Edge Topology.....	38
Figure 9: L2 IGMP SMLT Square Topology.....	39
Figure 10: PIM SMLT Square Design	40
Figure 11: PIM-SM SMLT Full Mesh Topology.....	41
Figure 12: PIM-SM RSMLT Triangle Design	43
Figure 13: PIM-SM anycast-RP Triangle Design	71
Figure 14: PIM-SM SMLT ERS5000 Distribution Edge	91
Figure 15: PIM-SSM SMLT ERS5000 Distribution Edge.....	130
Figure 16: PIM-SM RSMLT Mesh Topology	142
Figure 17: PIM-SM Static RP RSMLT Mesh Design	172

Tables

Table 1: PIM-SM Required Components	14
Table 2: Multicast on Avaya Module Switches.....	16
Table 3: Multicast Support on Avaya Stackable Switches.....	18
Table 4: PIM-SM Multicast Scaling Numbers for ERS 8000.....	34
Table 5: PIM-SM Multicast Scaling Numbers for VSP 9000.....	35

Conventions

This section describes the text, image, and command conventions used in this document.

Symbols



Tip – Highlights a configuration or technical tip.



Note – Highlights important information to the reader.



Warning – Highlights important information about an action that may result in equipment damage, configuration or data loss.

Text

Bold text indicates emphasis.

Italic text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

```
ERS5520-48T# show running-config
```

Output examples from Avaya devices are displayed in a Lucida Console font:

```
ERS5520-48T# show sys-info
```

```

Operation Mode:      Switch
MAC Address:         00-12-83-93-B0-00
PoE Module FW:       6370.4
Reset Count:         83
Last Reset Type:     Management Factory Reset
Power Status:        Primary Power
Autotopology:        Enabled
Pluggable Port 45:   None
Pluggable Port 46:   None
Pluggable Port 47:   None
Pluggable Port 48:   None
Base Unit Selection: Non-base unit using rear-panel switch
sysDescr:            Ethernet Routing Switch 5520-48T-PWR
HW: 02               FW: 6.0.0.10   SW: v6.2.0.009
Mfg Date: 12042004   HW Dev: H/W rev. 02
    
```

1. Multicast Overview

Applications that need to distribute data traffic to a large number of clients on different subnets can take advantage of multicast routing for its robustness, timeliness and efficiency in delivering traffic to a large number of clients. There are two common multicast routing protocols used to build a multicast distribution tree, Protocol independent multicast sparse mode, PIM-SM and Protocol independent multicast source-specific mode, PIM-SSM

Protocol Independent Multicast Sparse Mode (PIM-SM) is a multicasting protocol that utilizes an existing unicast routing table to build its multicast forwarding table. The protocol is named protocol independent as it is not dependent on any particular unicast routing protocol. Routers use PIM join and leave messages to either join or leave a particular multicast group address. To join a group address, a host identifies a multicast stream by group address alone (*,G) using IGMP join. In order to construct a multicast tree from sender to receiver, the multicast tree must be rooted by some selected router. With PIM-SM, this router is known as a Rendezvous Point (RP). At least one RP is required per PIM-SM autonomous system. The RP in turn will initially be used to build a shared tree between source and receiver. Once the PIM routers determine the source of the multicast traffic, a more specific source tree will be used to move multicast traffic more efficiently based on best path between sender and receiver. In order for PIM routers to discover the RP, some sort of RP discovery mechanism must be used including static configuration, Bootstrap Router, Anycast RP, or Auto-RP.

Protocol Independent Source-Specific Multicast (SSM), extends PIM-SM with the ability to identify not only by multicast group address, but also by source. An host, by using IGMPv3 messages, can identify a SSM group, named a channel, identified as (S,G) where S is the source address and G is the group address. This provides several advantages over PIM-SM as the source is known so no Rendezvous Point routers and associated RP discovery mechanism are required and no shared to source tree movement is used. Since a SSM channel is defined by both a source and a group address, group addresses can be re-used by multiple sources while keeping channels unique. For instance, the SSM channel (10.1.1.10/232.1.2.3) is different than (10.10.10.10/232.1.2.3), and hosts subscribed to one will not receive traffic from the other. IANA has reserved for SSM the IPv4 address range 232.0.0.0/8 and the IPv6 range FF3x::/32.

1.1 PIM-SM Multicast Distribution Trees

Internet Group Management Protocol, IGMP is a protocol used by IP Multicast routers to learn the existence of host group members on their directly attached subnets. It allows hosts to communicate their desired group memberships to their local querier router, and to receive any datagrams sent to this router which are targeted to a group with a specific IP Multicast address. A router communicates with the hosts on a local network by sending IGMP queries. Hosts respond by issuing IGMP reports.

When the Designated Router, DR (the PIM router with the highest IP address for that VLAN) receives the IGMP message for a new group, it looks up the associated active Rendezvous Point router, RP. After determining the RP router for the group, the DR creates a (*,G) route entry in the multicast forwarding table and sends a (*,G) join to the RP. A shared tree (RP-Tree) is created between the sources and receivers and at the root of the tree is the RP.

After receiving the first packets from the RP, the DR switches from a shared tree to a shortest-path tree (SP-Tree). Switching to a SP-tree creates a direct route between the receiver and the source. The DR creates an (S,G) entry in the multicast forwarding table and sends a (S,G) join to the source and a (S,G,rpt) prune message to the RP. All intermediate routers along the path to the source create the (S,G) entry.

The DR of the first hop router (router directly connected to the source) is responsible for encapsulating the multicast data into a register message and unicasting the message towards the RP. The register message informs the RP of a new source, causing the RP to send join/prune messages back toward the

DR of the source. The RP forwards the data down the RP tree after it removes the encapsulation. The DR stops sending encapsulated packets to the RP after receiving a register-stop message from the RP.

The required components for each PIM-SM domain are listed in Table 1.

Table 1: PIM-SM Required Components

Component	Description
Unicast Routing Protocol	PIM-SM builds its multicast forwarding table using the underlying unicast routing table. The routing table can be built using dynamic routing protocols such as OSPF, RIP or by static routes.
Rendezvous Point Router (RP)	Each multicast group has a shared tree. At the root of this shared tree is the RP. It is the RPs role to match up sources with receivers.
Bootstrap Router (BSR)	The BSR is a dynamically elected router, from a given set of candidate BSRs, in a PIM domain. It is responsible for distributing RP sets via bootstrap messages to all PIM enabled routers.
Designated Router (DR)	The DR is the PIM router with the highest IP address on a given subnet. It is responsible for forwarding PIM-SM join/prune messages and encapsulating multicast data packets as registered messages.
Layer 2/3 Switch with IGMP Snoop	IGMP snoop optimizes bandwidth within a switch by creating a bridge table entry for each subscribed multicast group destination port.

1.2 Interdomain PIM-SM Multicast using Multicast Source Discovery Protocol (MSDP)

The Multicast Source Discovery Protocol (MSDP) is used for two networking applications. First, it enables the advertisement of multicast source information between different Protocol Independent Multicast Sparse Mode (PIM-SM) domains. MSDP is also used within an Autonomous System (AS) to synchronize PIM information between two or more Anycast Rendezvous Points (RPs) to provide RP redundancy.

Within a given PIM-SM domain, the PIM-SM protocol allows for only a single active RP per multicast group. MSDP allows multiple RPs, called Anycast RPs, to provide service for a given multicast group. The Anycast RP routers establish MSDP adjacencies between each other in order to synchronize information about active multicast sources.

Each Anycast RP router is also enabled with MSDP and configured with one or more adjacent MSDP peers. The peers establish a session using TCP port 639 using either a unique loopback or interface IP address. When one of the MSDP enabled routers in the PIM domain learns of a new multicast source it transmits a MSDP Source-Active (SA) message to all of its peers. The receiving MSDP router performs a Reverse Path Forward (RPF) check. The RPF check ensures that the SA is received from the MSDP peer that is "closest" to the originating RP in order to prevent SA loops [1]. Note that this RPF check is

different than the multicast routing RPF check. The end result is that all Anycast RPs in the PIM-SM learn about the multicast source.

1.3 PIM-SSM – Source Specific Trees

PIM-SSM supports source-based multicast trees where there is a single source for every multicast channel. Channel membership is through the use of IGMPv3 which in turn allows a host to specify a source or list of sources it would either like to include or exclude in combination with a unique multicast group address. In summary, channel membership is a combination of multicast group address (G) as well as the source's unicast address (S) allowing the host to specify a particular source-group (S,G) pair. The only criterion is the host has to know how to find the sources.

With PIM-SM there is no use for Rendezvous Point nor is there any use for MSDP as the source is known. As the source is known, multicast data distribution is based on the shortest path from sender to receiver. This allows the same group addresses to be used with multiple sources. For example, 10.1.1.10/232.1.1.1 is different than 10.2.2.20/232.1.1.1; the route to the 10.1.1.10 and 10.2.2.20 networks are based on the shortest path in the unicast routing table and routed independently even though they have the same group address.

SSM applications use IP addresses reserved by the Internet Assigned Numbers Authority (IANA) in the 232/8 range (232.0.0.0 to 232.255.255.255). SSM recognizes packets in this range and controls the behavior of multicast routing devices and hosts that use these addresses. The reason for this range is it provides a specific range that PIM (S,G) must use over which (*,G) cannot be used. It then allows a DR router to allow both shared trees via (*,G) and source specific trees via (S,G) as there is no overlap in multicast addressing.

The benefits of PIM-SSM include:

- Access control where the receiver is capable of specifying the source for a specific group. This also eliminates the use of shared tree (*,G) forwarding and thus reduces network resources in building shared trees
- As the multicast channel is provided on a source basis, the same multicast group address can be used again eliminating the problem of group address allocation. This allows one to build very large multicast networks as the same group address can be re-used again by different sources.
- There is no need for Rendezvous Point or MSDP for source discovery eliminating the complexity of building RP-shared tree networks and multicast forwarding between different AS's

1.4 Multicast Support on Avaya Modular Switches

Please note the number shown in brackets in the table below is the minimum software release required.

Table 2: Multicast on Avaya Module Switches

Feature	Switch Model			
	VSP9000	ERS8800	ERS8600	ERS8300
IGMPv1/v2 Proxy	Yes	Yes	Yes	Yes
IGMPv1/v2 Snooping	Yes	Yes	Yes	Yes
IGMPv3 Proxy	Yes (3.2)	Yes	Yes	Yes (4.2)
IGMPv3 Snooping	Yes (3.2)	Yes	Yes	Yes (4.2.0)
IGMPv3 Backware Compatibility	Yes (3.2)	Yes	Yes (5.1)	Yes (4.2.0)
IGMPv2 for PIM-SSM	Yes	Yes	Yes	No
IGMPv3 for PIM-SSM	Yes	Yes	Yes	No
IGMP Router Discovery Protocol	Yes	Yes	Yes	No
IGMP Fast Leave	Yes	Yes	Yes	Yes
IGAP (IGMP for user authentication)	No	Yes	Yes	No
IGMP Layer 2 Querier	No	Yes	Yes (7.0)	Yes
PIM-SM	Yes	Yes	Yes	Yes
PIM-SM with SMLT	Yes	Yes	Yes	Yes (4.0) ^{Note 1, 2}
Static RP support for PIM-SM	Yes	Yes	Yes	Yes
PIM-SSM	Yes	Yes	Yes	No
PIM-SSM with SMLT	Yes	Yes	Yes	No

Feature	Switch Model			
	VSP9000	ERS8800	ERS8600	ERS8300
Multicast Static IP Route (mroute)	No	Yes	Yes (7.0)	No
Multicast VLAN Registration (MVR)	No	Yes	Yes (7.0)	Yes (4.1)
Multicast Access Control	Yes	Yes	Yes	Yes
Multicast stream limit	Yes	Yes	Yes	No
MSDP	No	Yes	Yes (5.1)	No
Multicast Virtualization (IGMP and PIM-SM/SSM) for VRF-Lite		Yes ^{Note 3}	Yes (5.1) ^{Note 3, 4}	No

Note 1: With release 4.0 for the ERS 8300, PIM-SM is supported only in a triangle SMLT topology. PIM-SM is NOT supported in an SMLT square, SMLT partial mesh, or SMLT full mesh topologies. IGMP snoop is supported in SMLT square, SMLT partial mesh, and SMLT full mesh topologies

Note 2: With release 4.1 for the ERS 8300, PIM-SM is supported in a square SMLT providing the ERS 8300 SMLT cluster is connected to either an ERS 8000 or VSP 9000 SMLT cluster. A square SMLT is NOT supported with 4 x 8300 for multicast traffic running PIM-SM on all 4 switches – only IGMP snoop is supported with this topology.

Note 3: PIM-SM, PIM-SSM, IGMPv1/v2/v3 protocols are virtualized and can be configured in a non-zero VRF. Supported on MLT/SMLT/RSMLT topologies

Note 4: Required R/RS modules and 8692 SF

1.5 Multicast Support on Avaya Stackable Switches

Please note the number shown in brackets in the table below is the minimum software release required.

Table 3: Multicast Support on Avaya Stackable Switches

Feature	Switch Model		
	ERS5000	ERS4000	ERS2500
IGMPv1/v2 Proxy	Yes	Yes	Yes
IGMPv1/v2 Snooping	Yes	Yes	Yes
IGMPv3 Proxy	Yes (6.2)	Yes (5.6)	Yes (4.4)
IGMPv3 Snooping	Yes (6.2)	Yes (5.6)	Yes (4.4)
IGMP v3 Source Filtering	Yes ^{Note 1}	No	No
IGMP Layer 2 Querier	Yes (6.2)	Yes (5.6)	Yes (4.4)
PIM-SM	Yes ^{Note 1, Note 2}	No	No
PIM-SSM	Yes ^{Note 1, Note 2}	No	No
PIM over SMLT/IST	No	No	No
Multicast groups	240 (5510) ^{Note 2} 492 (5520/5530) 992 (5600)	512 (5.2)	244
IGMP Multicast No Flood	Yes	Yes	Yes (4.3.0)

^{Note 1:} IGMPv3 Source Filtering, PIM-SM, and PIM-SSM are not supported on the ERS 5510.

^{Note 2:} PIM-SM and PIM-SSM are not supported over SMLT/IST or on Brouter ports. Software release 6.0.x and 6.1.x support PIM-SM in standalone mode only. Release 6.2 supports PIM-SM stacking on pure 55xx stacks, pure 56xx stacks, and hybrid 55xx/56xx stacks. On a hybrid stack, up to 492 groups can be supported. If a stack contains an ERS 5510, avoid configuring VLANs on the ERS 5510 running IP multicast traffic.

^{Note 3:} Requires software release 6.2 or higher. Prior to release 6.2, only 240 groups are supported. New ACLI command added to increase scaling; *ip igmp op-mode [5510/non-5510]*

2. Internet Group Management Protocol

2.1 IGMP on L2 SMLT Access Switches

IGMP Snooping

The Avaya Ethernet switches build an IGMP Snoop table upon receiving IGMP host membership requests for each specific multicast group. Only host ports requesting a multicast stream receive that stream; the switch automatically prunes the other ports and does not send multicast traffic to hosts that did not request it. In this way IGMP snoop makes efficient use of the available bandwidth to each of the hosts on the switch.

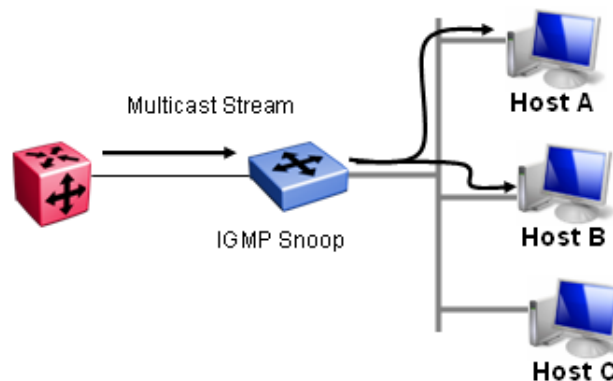


Figure 1: IGMP Snooping Feature

IGMP Proxy

The Avaya Ethernet switches provide a single proxy report upstream for all members within the same multicast group on the same switch/stack. By consolidating all the IGMP host membership requests into a single request, the switch does not flood the network with superfluous copies of the same request. IGMP Snooping must be enabled for this feature to work.

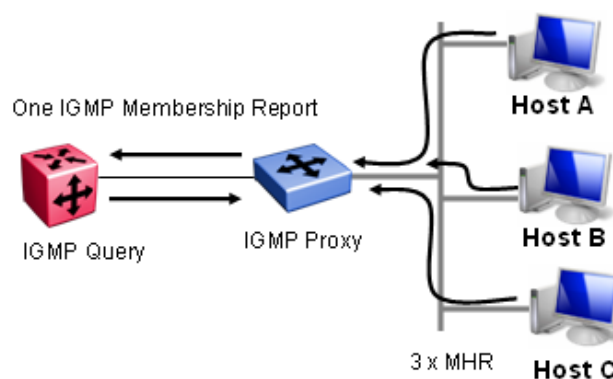


Figure 2: IGMP Proxy Feature

Unknown-mcast-no-flood

In situations in which there is a multicast source that is not participating in IGMP and there are no multicast receivers on the same VLAN on the same switch, the multicast traffic transmitted by the source is flooded to all ports in the VLAN. Flooding unknown multicast traffic is a behavior that is configurable (on or off) on some models of the Ethernet edge switches. The "vlan igmp unknown-mcast-no-flood" command provides this functionality. The "Unknown-mcast-no-flood" command for IGMP will stop flooding of unknown multicast traffic to all ports in a vlan except to IGMP static mrouter ports, as shown in Figure 3. When turning off flooding ensure that static mrouter ports become the destination of unknown multicast traffic.

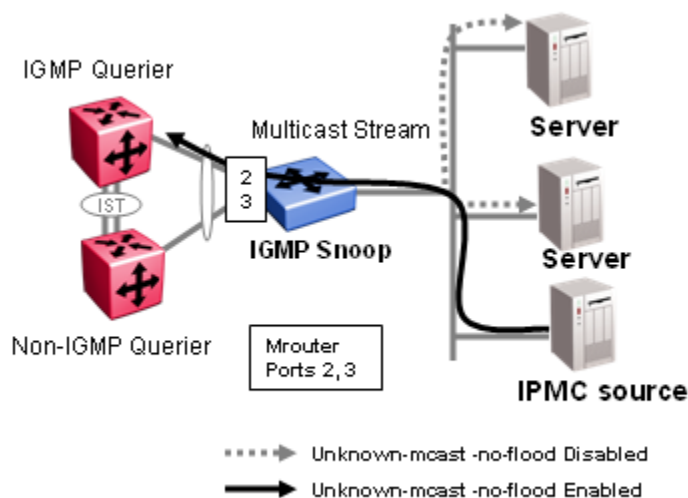


Figure 3: The unknown-mcast-no-flood feature stops multicast traffic from flooding all ports in a vlan

Design Recommendation

Enable both IGMP Snooping and Proxy on the Layer 2 edge switches when multicast is enabled in the network

If multicast is not being used in the network, disable IGMP Snooping and Proxy on the switches. By default, IGMP Snooping and Proxy are already disabled.

Presently, the Avaya Ethernet edge switches support both IGMP v1 and IGMP v2. Any Avaya Layer 2 switch configured for IGMPv2 will also be able to handle IGMPv1.



Use IGMP static router ports when multiple IGMP Queriers are present and on different ports.

On access switches where multicast senders are connected but for which no receivers exit on the same VLAN on the same switch, enable "Unknown-mcast-no-flood" in conjunction with IGMP snooping. In older stackable software versions (pre-IGMPv3) once "Unknown-mcast-no-flood" is enabled it is necessary to also configure static mrouter ports to ensure that the sender's multicast stream is always forwarded to the IGMP Querier (if one exists); otherwise "Unknown-mcast-no-flood" will prevent the stream from being forwarded to the IGMP querier and the stream cannot be IP routed to receivers in other IP subnets.

The ERS 8000 and VSP 9000 treat multicast data packet with a Time To Live (TTL) of 1 as an expired packet and sends them to the CPU before dropping them. To avoid high load on the CPU, set the TTL on multicast application to a TTL greater than 2.



The ERS 8000 and VSP 9000 will drop IGMP packets with a TTL not equal to 1.

2.2 IGMP Reporting Fields on SMLT Layer 2 Access Switches

On Avaya Switches IGMP snooping and proxy must be enabled on each VLAN participating in multicast, as shown in Figure 4.

```
ERS-Stackable(config)#vlan igmp <vid> snooping enable
```

```
ERS-Stackable(config)#vlan igmp <vid> proxy enable
```

Id	ReportProxyEnable	Enable	Robustness	QueryInterval	MRouterPorts	Ver1MRouterPorts	Ver2MRouterPorts	ActiveMRouterPorts	ActiveQuerier	QuerierPort
1	false	false	2	125				0.0.0.0	0	
99	false	false	2	125				0.0.0.0	0	
100	false	false	2	125				10.40.1.2	0	
104	false	false	2	125				10.40.104.1	0	
108	false	false	2	125				0.0.0.0	0	
203	false	false	2	125				0.0.0.0	0	
1400	true	true	2	125				1/19-1/20	10.12.140.1	1/19

Figure 4: IGMP Reporting Fields on L2 Switch



Mrouter ports should be configured on uplink ports when IGMP queries are not discovered through passive detection. IGMP snoop considers the port on which the IGMP query is received as the active IGMP multicast router (mrouter) port.

When IGMP snooping is enabled on an Ethernet switch or Ethernet Routing Switch, a membership table is created based on the ingress membership host reports. This membership table maps which port is subscribed to a multicast group.

```
ERS-Stackable#show vlan multicast membership 200
```

Multicast Group Address	Unit	Port
-----	----	----
239.110.110.100	2	2
239.110.110.101	2	2
239.110.110.102	3	3

2.3 IGMP and SMLT on the ERS 8300, ERS 8000, and VSP 9000

On the ERS 8000 and VSP 9000 IGMP is enabled by default when PIM-SM is enabled on a VLAN. As shown in Figure 5, the IGMP querier queries the locally attached subnet for clients subscribing to multicast groups. Multicast clients either initiate an IGMP membership report “join” or respond to an IGMP querier. Generated and received IGMP messages are multicast across the IST to the SMLT peer as documented in IST statistics shown below. If the receiving SMLT peer is not the lowest IP address in the subnet then it becomes an IGMP non-querier. The SMLT peer will update its IGMP table and won’t send out an IGMP query message on the locally attached subnet.

IGMP messages are sent on the lowest MLT port index number. In some situations the edge switch may send an IGMP membership report, “join”, to the non-IGMP querier. In this case the SMLT peer switch will forward IGMP membership report to its SMLT peer switch via an IST-IGMP message. Both SMLT peers IGMP tables will be synchronized and both SMLT peers will be aware of the multicast receivers on their SMLT ports.



Figure 5: IGMP Interaction with SMLT

```
8000-1:3# show mlt ist stat
```

Mlt IST Message Statistics	
PROTOCOL MESSAGE	COUNT

```
Ist Down           : 0
Hello Sent         : 226996
Hello Recv         : 234099
Learn MAC Address Sent : 2930
Learn MAC Address Recv : 350
MAC Address AgeOut Sent : 2707
MAC Address AgeOut Recv : 199
MAC Address Expired Sent : 0
MAC Address Expired Recv : 0
```

```
8000-2:3# show mlt ist stat
```

Mlt IST Message Statistics	
PROTOCOL MESSAGE	COUNT

```
Ist Down           : 1
Hello Sent         : 238096
Hello Recv         : 230872
Learn MAC Address Sent : 575
Learn MAC Address Recv : 3040
MAC Address AgeOut Sent : 376
MAC Address AgeOut Recv : 2766
MAC Address Expired Sent : 0
MAC Address Expired Recv : 0
```

Delete Mac Address Sent	: 0	Delete Mac Address Sent	: 0
Delete Mac Address Recv	: 0	Delete Mac Address Recv	: 7
Smlt Down Sent	: 7	Smlt Down Sent	: 6
Smlt Down Recv	: 6	Smlt Down Recv	: 13
Smlt Up Sent	: 14912	Smlt Up Sent	: 15923
Smlt Up Recv	: 14912	Smlt Up Recv	: 15933
Send MAC Address Sent	: 475	Send MAC Address Sent	: 497
Send MAC Address Recv	: 481	Send MAC Address Recv	: 489
IGMP Sent	: 3756	IGMP Sent	: 0
IGMP Recv	: 0	IGMP Recv	: 3762
Port Down Sent	: 6	Port Down Sent	: 11
Port Down Recv	: 7	Port Down Recv	: 64
Request MAC Table Sent	: 16	Request MAC Table Sent	: 17
Request MAC Table Recv	: 4	Request MAC Table Recv	: 67
Unknown Msg Type Recv	: 0	Unknown Msg Type Recv	: 0



It is recommended that the IGMP Query Interval is greater than 5 to prevent dropping multicast traffic.



In a routed network, the IGMP Querier should reside as close as possible to the receivers of the multicast group. This is usually the last hop router/switch of the multicast distribution tree.



The ERS8300, ERS8000, or VSP9000 can be used as an access switch. They support IGMPv1, IGMPv2, and IGMPv3. The versions IGMPv1 and IGMPv2 are backward compatible and can exist together on a multicast network.



Many IGMP features that are useful for multicast-based TV distribution applications such as Fast Leave, tunable LMQI, IGMP access control policies are available.

2.4 SSM and IGMPv2

SSM-configured switches can accept reports from IGMPv2 hosts on IGMPv2 interfaces if the group uses an SSM channel table entry. However, the IGMPv2 host groups must exist in the SSM range defined on the switch, which is 232/8 by default.

- After the SSM switch receives an IGMPv2 report for a group that is in the SSM channel table, it joins the specified source immediately.
- After the SSM switch receives an IGMPv2 report for a group that uses an enabled static SSM channel table entry, it triggers PIM-SSM processing as if it received an equivalent IGMPv3 report.
- After the SSM switch receives an IGMPv2 report for a group out of the SSM range, it processes the report as if it is in PIM-SM mode.

2.5 SSM and IGMPv3

With IGMPv3, a host can selectively request or filter traffic from sources within the multicast group. IGMPv3 is an interface-level configuration.



IGMPv3 works only with PIM-SSM or SSM-snoop enabled on the interface.

The following rules apply to IGMPv3-enabled interfaces:

- Send only IGMPv3 (source-specific) reports for addresses in the SSM range
- Accept IGMPv3 reports
- Drop IGMPv2 reports

The IGMPv2 report mentioned in SSM and IGMPv2 above is processed because it is an IGMPv2 report that is received on an IGMPv2 interface. If an IGMPv2 interface receives an IGMPv3 report, the report is dropped even if PIM-SSM is enabled and the entry is in the SSM channel table. The IGMP version must match.

- Discard IGMP packets with a group address out of the SSM range.

2.6 IGMP Access Control

IGMP access control policies allow for restriction of multicast groups. This feature provides added security by either not allowing users from receiving certain multicast channels or preventing users from sending multicast streams, i.e. spoofing a multicast group. Multicast access control is not a regular filtering configuration and does not use filters.

The following paragraph describes a typical application.

Your local cable television company offers three packages; each one includes 35 channels (35 multicast groups). Each package is configured in an access control policy. This policy is applied to a set of VLANs or ports to prevent users from viewing the channels on those VLANs. Use the same policy to prevent users from sending traffic to those groups (also known as spoofing) by specifying the deny-tx option for that port. After you define the packages, you can use them for access policy configuration. You can easily change the package by changing the group range, without changing all the port configurations.

2.7 IGMP Fast Leave feature

The fast leave feature is useful for multicast-based television distribution applications. Fast leave relies on an alternative leave process where the switch stops sending traffic for the group immediately after receiving a leave message, without issuing a query to check if other group members are present on the network. Fast leave alleviates the network from additional bandwidth demand when you change television channels.

2.8 IGAP (Internet Group Authentication and Accounting Protocol)

Multicast feature extension - IGAP full implementation/ IGAP options: Accounting on/off, Authentication on/off/IGAP Fast leave

IGAP allows user clients to connect to Network IGAP enabled gateways for access-controlled multicast services. These gateways have the ability to authenticate the user client's authority to join or leave a multicast group. This new functionality will require insight to the IGAP protocol control plane to understand the health and status of an IGMP multicast connection. Either the client will be allowed to join a multicast service or will be denied due to authentication or network failure. Authentication failure can be a result of several factors listed in the IGAP protocol specification. Serviceability is in the context that IGAP information is presented in a consistent format for the purpose of monitoring and troubleshooting network connectivity. By this, the information becomes more portable for usage in accounting and billing type applications. It's understood that an IGAP MIB is being developed but is not yet posted on the IETF web sight at this time.

2.9 ERS 8000 & ERS 8300 - IGMPv3 Backward Compatibility

This feature allows two modes of operation, IGMPv3 only and IGMP compatibility mode.

In IGMPv3 only mode, the switch will ignore all v2 messages except Query messages.

In IGMPv3 compatibility mode, IGMPv1, v2, and v3 will be supported. The group address of the messages will be parsed. If the group address is out of SSM range and is an IGMPv3 message, it will be dropped. If it is an IGMP v1 or v2 message, it will be handled by PIM-SM or IGMP Snoop process. The following table illustrates each specific behavior.

Host	VLAN	SSM Range	Action
IGMPv2 host	IGMPv3 VLAN	In or Out of range	Drop report
IGMPv3 host	IGMPv2 VLAN	In or Out of range	Drop report
IGMPv2 host	IGMPv2 VLAN	In SSM range	If the report matches an existing static SSM channel entry, create (S,G). If the report does not match any existing Static SSM channel entry, drop it.
IGMPv2 host	IGMPv2 VLAN	Out of SSM range	Ignore the SSM channel table and process the report as if it is in PIM-SM mode.
IGMPv3 host	IGMPv3 VLAN	Out of SSM range	Invalid scenario hence. Drop report.
IGMPv3 host	IGMPv3 VLAN	In SSM range	Global Flag: Dynamic learning enabled. Create (S,G).
IGMPv3 host	IGMPv3 VLAN	In SSM range	Global Flag: Dynamic learning disabled and matches an Existing SSM channel entry. Create (S,G)
IGMPv3 host	IGMPv3 VLAN	In SSM range	Dynamic disabled and does not match an existing SSM channel entry. Drop it.
IGMPv2 host	IGMPv3 VLAN	In SSM range	If the report matches an existing static SSM channel entry, create (S,G). If the report does not match any existing Static SSM channel entry, drop it.
IGMPv2 host	IGMPv3 VLAN	Out of SSM range	Process the report as in PIM- SM mode.

3. PIM-SM Design Guidelines

The following are general rules that must be followed when enabling multicast within a campus LAN.

1. All routers that are participating in multicast routing need to have PIM-SM enabled. An upstream non-PIM router will not receive PIM Join/Prune messages from a downstream PIM router and vice versa. As a consequence this will reduce the robustness of multicast connectivity.
2. The ERS8000 or VSP 9000 can connect to a Cisco proprietary PIMv1 network using Auto-RP. The IP interface between the ERS8000 or VSP 9000 and Cisco router must be configured using PIMv2. All other interfaced on the Cisco router can be configured as PIMv1 with or without Auto-RP. The Cisco router connected to the ERS8000 or VSP 9000 should be configured as the BSR allowing the Cisco router to advertise any RP discovered via Auto-RP to be advertised to the ERS8000. A multicast source on a Cisco PIMv1 can use an RP configured on the ERS8000 or VSP 9000. A multicast source on an ERS8000 or VSP 9000 switch cannot use an RP configured on a Cisco router. As long as the source is connected to a Cisco router where AutoRP is used, the multicast receivers can be on a Cisco router or ERS8000/VSP9000 switch.
3. Within a multicast domain PIM-SM and PIM-SSM can be used together.
4. Multicast routing protocol must be congruent with the unicast routing paths. As a general rule, in a PIM domain, you need to enable PIM-SM on all interfaces in the network for multicast traffic to flow properly. In some situations, the Interior Gateway Protocol (IGP) may determine the best reverse path may occur thru a non-PIM enable interface resulting in a failure in multicast. In addition within a PIM domain if each PIM-SM router does not have a RPF neighbor to any other PIM neighbor then bootstrap messages may not reach all routers. As a result PIM routers will have inconsistent RP-sets leading to group partitions within the PIM domain.
5. A PIM interface can be configured as active or passive. All SMLT VLANs should be configured to be PIM-SM active mode. PIM active mode will transmit and receive PIM control traffic and provide faster failovers/recoveries. If the ERS 8000 or VSP 9000 is used as an edge switch and aggregating end users then PIM interface should be in passive mode. A passive interface drops all PIM control traffic, thereby reducing the load on the system.

Rendezvous Point and Bootstrap Design

1. A rendezvous point router is required in each PIM-SM domain. In networks where RPs are to be dynamically learned, a BSR will need to be configured. It is recommended that the BSRs and RPs be assigned to a circuitless IP address. The BSR and RP can be configured on the same CLIP/Loopback address. This will prevent a BSR or RP failure if a VLAN interface goes down. The CLIP/Loopback address must be reachable throughout the network. The CLIP/Loopback address needs to have OSPF enabled if the OSPF is used for the IGP as well as PIM enabled.
2. PIM-SM builds a shared multicast distribution tree within each domain, and the RP is at the root of this shared tree. Although the RP can be physically located anywhere on the network, it must be as close to the source as possible.
3. Within a PIM domain it is recommended to configure multiple candidate RPs and BSRs for redundancy. Multicast group communication will become disrupted if a single RP or BSR was configured and then became unreachable. Creating multiple candidate RPs not only increases the robustness of the multicast network but it also allows for load sharing of multicast traffic because each group will be mapped to different RPs. In a PIM domain only one BSR can be active and only one RP can be active for a given multicast group.
4. You can configure a static entry for a RP with static RP. Static RP-enabled switches cannot learn about RPs through the BSR because the switch loses all dynamically-learned BSR information

and ignores BSR messages. When you configure static RP entries, the switch adds them to the RP-set as if they were learned through the BSR.

5. Static and dynamic RP configurations are not supported on the same switch. However within a PIM domain static RP and dynamic RP defined switches can coexist. The design caveat is that the active RP for any multicast group should not be defined on the switch configured with static RPs. Since this switch does not participate in candidate-rp advertisements or receive bootstrap messages it cannot advertise its RP for a given multicast group; resulting in inconsistent RP-Sets being distributed throughout the PIM domain. All PIM routers must have the same RP-Sets to ensure that “group to RP mapping” is consistent within the PIM domain to avoid group partitioning.

4. PIM-SSM Design Guidelines

Use the following information when you design an SSM network:

- If you configure SSM, it affects SSM groups only. The switch handles other groups in sparse mode (SM) if a valid RP exists on the network.
- It is possible to configure PIM-SSM only on switches at the edge of the network while the Core switches use PIM-SM. This can allow PIM-SSM and PIM-SM to co-exist on the same network PIM-SSM nodes will only generate (S,G) joins which can be handled by the PIM-SM Core (which can handle both (S,G) & (*,G) joins. The reverse (PIM-SSM in the Core and PIM-SM at the edge) is not true and will not work.
- For networks where group addresses are already in use, you can change the SSM range to match the groups.
- One switch has a single SSM range.
- You can have different SSM ranges on different switches.
Configure the core switches that relay multicast traffic so that they cover all of these groups in their SSM range, or use PIM-SM.
- One group in the SSM range can have a single source for a given SSM group.
- With IGMPv2 and Static Channels, you can have different sources for the same group in the SSM range (different channels) if they are on different switches.
- Two different devices in a network want to receive data from a physically closer server for the same group. Hence, receivers listen to different channels (still same group).

4.1 SMLT Hashing Algorithm for Multicast

4.1.1 VSP 9000

MultiLink Trunking provides a mechanism to distribute multicast streams over a multilink trunk. This mechanism is based on source-subnet and group addresses. You can use it to choose the address and bytes in the address for the distribution algorithm.

The multicast flow distribution over MLT algorithm is the same multicast flow distribution algorithm used in IEEE 802.3ad based link aggregation. As a result, you can distribute the load on the MLT ports and achieve even stream distribution. In applications such as television (TV) distribution, multicast traffic distribution is important because bandwidth requirements are substantial after a large number of TV streams are employed.

Multicast distribution is done in the datapath and is always enabled.

Multicast distribution algorithm

To determine the port for a particular source-group (S,G) pair, the number of active ports of the multilink trunk is used to MOD the number generated by the XOR of each byte of the masked group address with the masked source address. By default, the group mask and source mask is 255.255.255.255. A byte with a value of 255 in the mask means that the corresponding byte in the group or source address is taken into account when the algorithm is applied.

For example, consider:

If the group address is G[0].G[1].G[2].G[3], the group mask is GM[0].GM[1].GM[2].GM[3], the source subnet address is S[0].S[1].S[2].S[3], and the source mask is SM[0].SM[1].SM[2].SM[3]

Then, the port equals:

$$(((((G[0] \text{ AND } GM[0]) \text{ xor } (S[0] \text{ AND } SM[0])) \text{ xor } (G[1] \text{ AND } GM[1]) \text{ xor } (S[1] \text{ AND } SM[1])) \text{ xor } (G[2] \text{ AND } GM[2]) \text{ xor } (S[2] \text{ AND } SM[2])) \text{ xor } (G[3] \text{ AND } GM[3]) \text{ xor } (S[3] \text{ AND } SM[3]))) \text{ MOD } (\text{active ports of the MLT})$$

The algorithm used for traffic distribution causes sequential distribution if the streams are similar to those in the example that follows. Assume that the multilink trunk ports are 3/1 to 3/4, that mask configuration is 0.0.0.0 for the source mask and 0.0.0.255 for the group mask, and that source A.B.C.D sends to the following groups:

X.Y.Z.1

X.Y.Z.2

X.Y.Z.3

.....

X.Y.Z.10

The algorithm chooses link 3/1 for group X.Y.Z.1, 3/2 for group X.Y.Z.2, 3/3 for group X.Y.Z.3, and continues for the remaining ports.

Multicast traffic distribution

The goal of traffic distribution is to achieve stream distribution on the MultiLink Trunking links after an MLT configuration change takes place. Traffic distribution is based on the IP multicast MLT distribution algorithm, which is the same for all modules.

Traffic distribution is enabled by default. The active streams redistribute according to the distribution algorithm on the links of the multilink trunk links.

To minimize the effect of multicast traffic distribution on the multilink trunks, the implementation does not move the streams to the appropriate links at one time. Instead, it redistributes a few streams at every time tick of the system. After an MLT port becomes inactive only affected streams are redistributed on the remaining active ports.

4.1.2 ERS 8800 (R/RS Modules) and ERS 8600 (E-modules only)

MLT provides a mechanism to distribute multicast streams over a MultiLink trunk. This mechanism is based on source-subnet and group addresses. You can use it to choose the address and bytes in the address for the distribution algorithm.

The multicast flow distribution over MLT algorithm is the same multicast flow distribution algorithm used in IEEE 802.3ad-based link aggregation. As a result, you can distribute the load on the MLT ports and achieve even stream distribution. In applications such as Television (TV) distribution, multicast traffic distribution is important because bandwidth requirements are substantial when a large number of TV streams are employed.

When you configure flow distribution over MLT, Avaya recommends that you choose source and group masks that result in even traffic distribution over the MultiLink trunk links. For example, if the group addresses change incrementally while few sources sending to different groups, use a source mask of 0.0.0.0 and a group mask of 255.255.255.255. In most cases, this provides a sequential distribution of traffic on the MultiLink trunk links.

When changing the state parameters of multicast flow distribution, minor traffic interruptions can occur.

Multicast distribution algorithm

To determine the port for a particular source, group (S, G) pair, use the number of active MLT ports to MOD. The number generated by the XOR (exclusive OR operation) for each byte of the masked group address, with the masked source address.

By default, the group mask and source mask is 255.255.255.255. A byte with a value of 255 in the mask indicates that the corresponding byte in the group or source address is taken into account when the algorithm is applied.

The following is an example:

group address G[0].G[1].G[2].G[3]

group mask GM[0].GM[1].GM[2].GM[3]

source subnet address S[0].S[1].S[2].S[3]

source mask SM[0].SM[1].SM[2].SM[3]

The port is calculated by using:

$$(((((G[0] \text{ AND } GM[0]) \text{ XOR } (S[0] \text{ AND } SM[0])) \text{ XOR } (G[1] \text{ AND } GM[1]) \text{ XOR } (S[1] \text{ AND } SM[1]))) \text{ XOR } (G[2] \text{ AND } GM[2]) \text{ XOR } (S[2] \text{ AND } SM[2]))) \text{ XOR } ((G[3] \text{ AND } GM[3]) \text{ XOR } (S[3] \text{ AND } SM[3]))) \text{ MOD (active ports of the MLT)}$$

Algorithm example

The traffic distribution algorithm causes sequential distribution if the streams are similar in the following example.

Assume that the MLT ports are 1/1 to 1/4, the source mask configuration is 0.0.0.0 and the group mask configuration is 255.255.255.255. The source A.B.C.D. is sent to the following groups:

X.Y.Z.1

X.Y.Z.2

X.Y.Z.3 to X.Y.Z.10

The algorithm chooses link 1/1 for group X.Y.Z.1, X.Y.Z.2 goes on port 1/2, X.Y.Z.3 goes on port 1/3, X.Y.Z.4 goes on port 1/4, X.Y.Z.5 goes on port 1/1, and so on.

Multicast traffic distribution

The goal of traffic distribution is to achieve stream distribution on the MultiLink trunk links when an MLT configuration change takes place. Traffic distribution is based on the IP multicast MLT distribution algorithm, which is the same for all modules.

Traffic distribution is disabled by default. When you add or remove a link from the MultiLink trunk, the active streams continue to flow on the original links. If distribution is enabled, the active streams redistribute according to the distribution algorithm on the links of the MultiLink trunk links.

When changing the state parameters of multicast traffic distribution, minor traffic interruptions can occur.

To minimize the effect of multicast traffic distribution on the MultiLink trunks, the implementation does not move the streams to the appropriate links at one time. Instead, it redistributes a few streams at every time tick of the system. When an MLT port becomes inactive and distribution is disabled, only affected streams are redistributed on the remaining active ports.

If you enable distribution, all streams redistribute on the MLT ports based on the distribution algorithm assignment.

If you disable distribution and a new port becomes active in a Multilink trunk, existing streams remain on the original links. Enable distribution to redistribute the streams dynamically and split the load on all the links of the MultiLink trunk. This redistributes a few streams at every system time tick.

Multicast traffic distribution provisioning

Multicast flow distribution over MultiLink Trunking (MLT) provides a mechanism for distributing multicast streams over a multilink trunk. With MLT, you can distribute the load on different ports of the multilink trunk and (whenever possible) achieve an even distribution of the streams.

To configure multicast flow distribution over MLT, you must enable it globally and for each multilink trunk.

Global Provisioning

Configure multicast flow distribution globally to distribute multicast streams over a multilink trunk.

All MLT distribution for unicast or multicast traffic occurs at the ingress port, and therefore the port style make-up of the MLT itself has no affect on this operation. If the ingress port is a R, RS, or 8800 module port and the egress MLT is in the same VLAN (Layer 2 flow) distribution occurs only if IGMP snoop is enabled.

For inter-VLAN or Layer 3 flows, distribution always occurs for ingress IPMC traffic. In this configuration, you must enable an IPMC Layer 3 routing protocol, or configure static IPMC routing. Distribution does not occur for a pure Layer 2 multicast traffic (multicast destination MAC only) that has no Layer 3 IPMC address. If IGMP snoop is enabled for a particular VLAN/Brouter port, the switch accepts Layer 3 multicast protocol configuration on that VLAN or brouter port.

Command	Parameter
CLI	
config sys mcast-mlt-distribution	info
	disable
	enable
	grp-mask <grp-mask>
	redistribution <enable disable>
	src-mask <src-mask>
config sys mcast-smlt	square-smlt <enable disable>
ACLI	
multicast mlt-distribution	grp-mask <grp-mask>
	Redistribution
	src-mask <src-mask>
multicast mlt-distribution	<enter command to enable multicast mlt-distribution>
multicast smlt-square	<enter command when mlt is used in either a square or full-mesh topology>



Enable multicast smlt-square configuration all all four switch when either a square or full mesh topology is used.



Please note the “multicast mlt-distribution” command is only valid for the ERS 8000. Multicast MLT distribution is done completely in the datapath and is always enabled on the VSP 9000.

Configuring multicast flow distribution for a multilink trunk

Enable multicast flow distribution for each multilink trunk to customize your configuration. Distribute the load on different ports of the multilink trunk.

Command	Parameter
CLI	
config mlt <mltid> mcastdistribution	enable
	disable
ACLI – Enter ACLI command <i>interface mlt <ID></i> followed by:	
multicast mlt-distribution	[grp-mask <grp-mask>] [redistribution] [src-mask <src-mask>]
	<enter command to enable multicast mlt-distribution>



Please note the “multicast mlt-distribution” command is only valid for the ERS 8000. Multicast MLT distribution is done completely in the datapath and is always enabled on the VSP 9000.

4.1.3 ERS 8300

Multicast streams are forwarded based on the following algorithm

For any registered multicast (source port, source device, VID, VIDX):

- $\text{Reg_V}[11:0] = \text{VID}[11:0] \text{ XOR } (\text{VIDX}[0:11] - (\text{This is VID}[11:0] \text{ XOR with VIDX}[11:0] \text{ flipped}))$
- $\text{V}[3:0] = (\text{Reg_V}[11:8]) \text{ XOR } (\text{Reg_V}[7:4]) \text{ XOR } (\text{Reg_V}[3:0])$
- $\text{Reg_Trunk_Dist_Index}[3:0] = (\text{Src_Port}[3:0]) \text{ XOR } (\text{Src_Dev}[3:0]) \text{ XOR } (\{\text{Src_Dev}[6:4]\}) \text{ XOR } (\{\text{Src_Port}[5:4], 2'd0\}) \text{ XOR } (\text{Unk_V}[3:0])$


4.1.4 ERS 5000, ERS 4000, and ERS 2500

Multicast is always hashed on the lowest SMLT port index. If a link failure occurs then multicast stream will be hashed on the next lowest SMLT port index.

4.2 Multicast Scaling Numbers

4.2.1 ERS 8000

Table 4: PIM-SM Multicast Scaling Numbers for ERS 8000

Feature	Maximum number supported using 8692SF with SuperMezz or 8895SF	Maximum number supported using E and M modules
PIM Instances	On 64 VRFs (including GRT)	On GRT
PIM active interfaces	200 (200 for all VRFs)	200
PIM passive interfaces	1972 (2000 for all VRFs)	1972
PIM neighbors	80 (200 for all VRFs)	80
MSDP peers	20	20
MSDP maximum SA messages	6144	6144
Multicast streams: with SMLT/without SMLT	2000/4000	500/1500
Multicast streams per port	1000	
Multicast streams on non-SPB VLANs when SPBM is enabled on the switch	1500	N/A
IGMP reports/sec	250	
 PIM interfaces also need to run a unicast routing protocol, which in combination can be taxing on the ERS 8000. If number of VLANs exceed 500 it is recommended that only 10 active PIM interface are configured per ERS 8000.		

4.2.2 VSP 9000

Table 5: PIM-SM Multicast Scaling Numbers for VSP 9000

Feature	Maximum number supported
PIM Instances	512 active, 4048 passive
Multicast source and group (S,G)	6,000
PIM neighbors	80 (200 for all VRFs)

4.3 Supported Multicast SMLT Topologies

4.3.1 SMLT Triangle – Layer 2 Cluster

Split multi-link trunk logically aggregates two ERS 8000s, ERS 8300s or VSP 9000s to form one logical switching cluster. These two switches are connected with an inter-switching trunk (IST) which exchanges forwarding databases between them. This is a scalable and high performance resilient solution in the core of the network. SMLT is a proven resilient technology; providing sub second failovers in the event of link or nodal failures. In this section multicast with SMLT topologies will be discussed.

IGMP snooping on the edge and core switches, as seen in Figure 6, are supported. If IGMP snooping is not enabled then multicast traffic will be forwarded to all ports on that switch belonging to the VLAN. Enabling IGMP snooping will prune ports that are not participating in multicast.

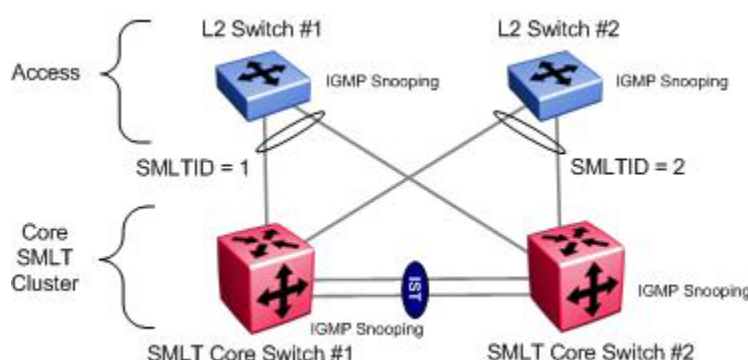


Figure 6: L2 IGMP SMLT Triangle Topology

Summary:

- Support with and without Q tagging
- A querier is required can be placed at the edge or in the core
- Queriers have to be placed on one switch/VLANs only
- One querier required per VLAN
- IGMP querier feature can be enabled to remove the requirement of an external IGMP querier – supported on ERS 8800, ERS 8300, ERS 5000, ERS 4000, and ERS 2500
- Senders and Receivers can be placed everywhere with the following exception
 - No senders and receivers on the SMLT VLANs on the core switches; they can be placed on other VLANs on the core switches

4.3.2 SMLT Triangle – Layer 3 Cluster, Layer 2 Access

The ERS 8000, ERS 8300, and the VSP 9000 each support rapid failover/recovery of multicast streams using PIM-SM on SMLT triangles, as shown in Figure 7. It is recommended that edge switches have IGMP snooping and proxy enabled. PIM-SM active mode should be enabled on all SMLT access VLANs and IST VLAN. Enabling PIM-SM on the ERS 8000 or VSP 9000 will automatically enable IGMP querier functionality. Redundant candidate RPs and BSRs should be configured on each SMLT peer and defined on a CLIP/Loopback address. For faster recoveries it is recommended to implement a design that uses static RPs.

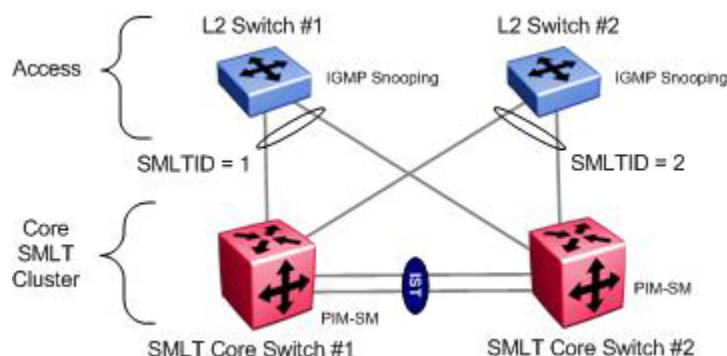


Figure 7: PIM-SM SMLT Triangle Topology

Summary:

- Support with and without Q tagging
- Enable PIM active more on the SMLT cluster switch; this will also enable IGMP querier
- ERS8000 and VSP9000 support PIM-SM and PIM-SSM in a SMLT Triangle topology
- Software release 4.x for the ERS 8300 supports PIM-SM in a SMLT Triangle topology
- Senders and Receivers can be placed everywhere with the following exception
- No senders and receivers on the SMLT VLANs on the core switches; they can be placed on other VLANs on the core switches.
- E or M modules are required for the ERS8600

4.3.3 SMLT Triangle – Layer 3 Cluster, Layer 3 Access

Designing a three tier network to support multicast with SMLT is fully supported. A L3 switch acting as the SMLT distribution switch can be running PIM-SM, as shown in Figure 8. PIM-SM builds its multicast forwarding table from the underlying unicast routing protocol and therefore an IGP must be configured within the SMLT core. The IGMP querier and the candidate RP should be configured as close as possible to the source of the multicast streams. It is also recommended that the active BSR is located in the core of the network to optimize bootstrap message flows and reduce the time duration during bootstrap elections.

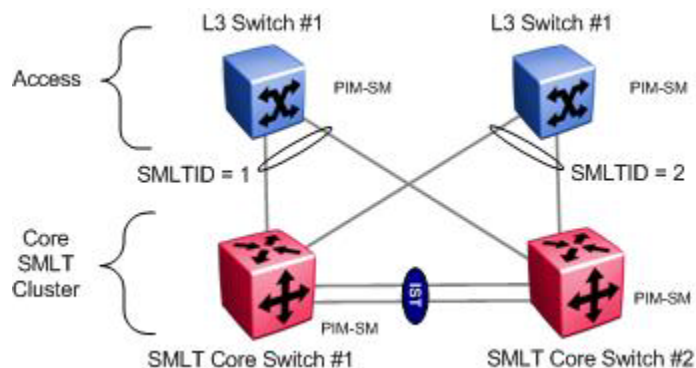


Figure 8: PIM-SM SMLT Distribution Edge Topology

Summary:

- Support with and without Q tagging
- Senders and receivers can be placed anywhere
- ERS8000 and VSP9000 support PIM-SM and PIM-SSM in a SMLT Triangle topology
- Software release 4.x for the ERS 8300 supports PIM-SM in a SMLT Triangle topology

4.3.4 SMLT Square – Layer 2 Cluster

Customers who wish to avoid implementing L3 multicast routing can implement L2 multicast forwarding in SMLT square configuration. As shown in Figure 9, IGMP snooping must be enabled on each VLAN participating in L2 multicast forwarding on each core switch. It is recommended that on the VLANs participating in multicast forwarding the IGMP snooping feature be enabled. An external router can serve as the IGMP querier for this network.

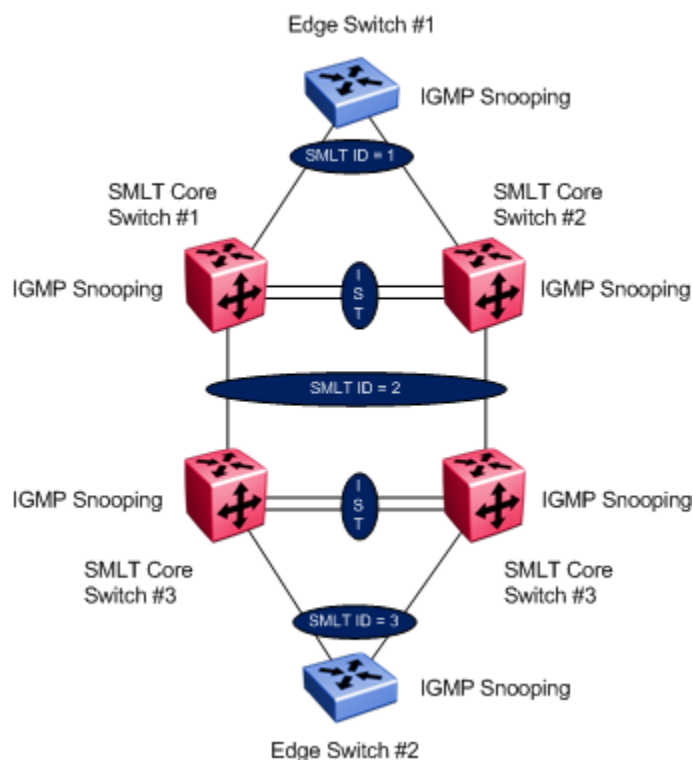


Figure 9: L2 IGMP SMLT Square Topology

Summary:

- Support with and without Q tagging
- Querier can be placed at the edge or in the core
- Queriers have to be placed on one switch/VLANs only
- One querier required per VLAN
- Senders and receivers can be placed anywhere
- Spanning Tree is not supported
- ERS8000, ERS8300, and VSP9000 support IGMPv1/v2/v3 in a SMLT Triangle topology
 - In reference the the ERS8300, in release 4.3, IGMPv3 is only supported where the ERS8300 SMLT cluster must connect to either an ERS8000 or VSP9000 SMTL cluster in a SMLT square topology

4.3.5 SMLT Square – Layer 3 Cluster

As illustrated in Figure 10, PIM multicast routing over SMLT square topology is supported. If PIM-SM is configured, Candidate RPs and BSRs can be configured on all four SMLT cluster switches for robustness and load sharing of a RP-tree for a given multicast group.

It is recommended all L2 Edge switches have IGMP snooping and proxy enabled. The IGMP querier should be located as close to the source and client of the multicast stream as possible.

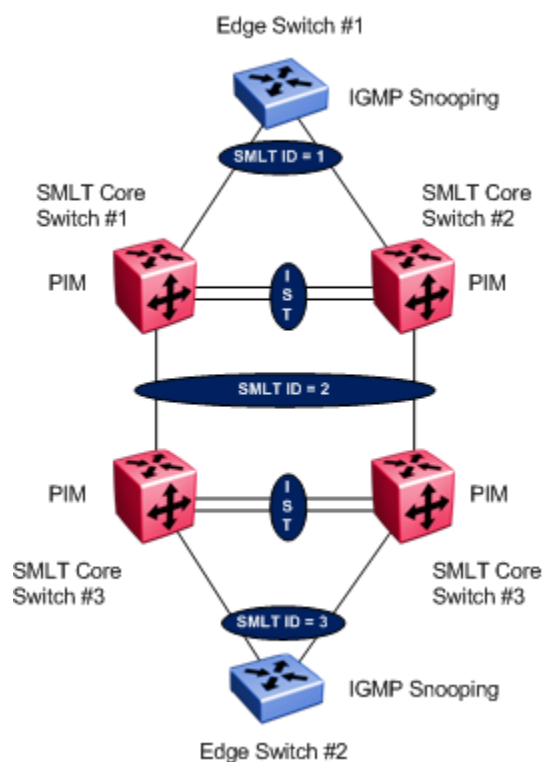


Figure 10: PIM SMLT Square Design

Summary:

- PIM-SM is supported on the ERS8300, ERS8000, and VSP9000
 - In reference the the ERS8300, in release 4.3, PIM-SM is only supported where the ERS8300 SMLT cluster must connect to either an ERS8000 or VSP9000 SMTL cluster in a SMLT square topology
- PIM-SSM is supported on the ERS8000 and VSP9000
- PIM-SM guidelines
 - It is recommended that candidate RP and BSRs are assigned to a CLIP/Loopback address.
 - If RIP is to be used as the IGP then static routes to each CLIP/Loopback address defined on each ERS 8000 should be created where the static route should be redistributed into RIP
 - Every VLAN participating in multicast routing must be PIM enabled.

4.3.6 SMLT Full Mesh – Layer 3 Cluster

As illustrated in Figure 11, PIM multicast routing over SMLT full mesh topology is supported. If PIM-SM is configured, Candidate RPs and BSRs can be configured on all four SMLT cluster switches for robustness and load sharing of a RP-tree for a given multicast group.

It is recommended all L2 Edge switches have IGMP snooping and proxy enabled. The IGMP querier should be located as close to the source and client of the multicast stream as possible.

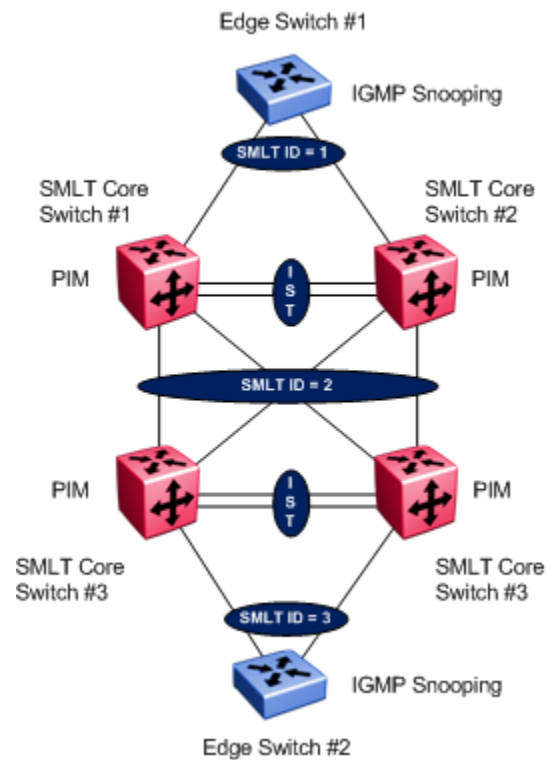


Figure 11: PIM-SM SMLT Full Mesh Topology

Summary:

- PIM-SM and PIM-SSM are supported on the ERS8000 and VSP9000

5. Configuring PIM using SMLT

Outlined below are the 10 basic steps for configuring PIM-SM over SMLT.

1. Configure an IGP within the SMLT core. PIM-SM builds its multicast forwarding table from the underlying unicast routing protocol. Static routes, RIP V1/2 and OSPF can be used
2. Configure SMLT to edge switches as per the Switch Cluster using SMLT TCG guide.
3. Configure IGMP snoop/proxy on edge switches that are participating in multicast on SMLT peer nodes.
4. If the network design is a SMLT square/mesh then a system flag for multicast over SMLT squares must be enabled. This applies to the VSP9000 and ERS8000 only using the CLI *config sys mcast-smlt square-smlt enable* command or ACLI *multicast smlt-square* command.
5. Enable PIM globally on the chassis
6. PIM-SM only. If dynamic PIM-SM is to be used then it is recommended that candidate RP and BSRs are assigned to a CLIP/Loopback address. The RP should be located as close as possible to the source of the multicast. It is recommended to use static RPs for faster recoveries.
7. PIM-SM only. Ensure that all the switches/routers as well as the sources and receivers can route to the RP. The CLIP/Loopback address needs to be OSPF and PIM-SM enabled. If RIP is to be used as the IGP then static routes to each CLIP/Loopback address defined on each switch should be created. Static routes should be distributed into RIP in order for downstream routers to learn how to route to the RPs.
8. Enable PIM active mode on each SMLT VLAN participating in multicast. PIM passive mode on all edge/access ports.
9. Enable PIM active mode on the IST VLAN for faster recoveries.
10. All VLANs on L2 Edge switches participating in IP multicast needs to have IGMP snooping and proxy enabled.

5.1 PIM-SM RSMLT Triangle Topology with L2 Edge

The following diagram is an example of the configuration of PIM-SM on RSMLT Triangle topology. Please refer to the Switch Clustering using Split Multi-Link Trunking (SMLT) Technical Configuration Guide for details on the best practices for SMLT.

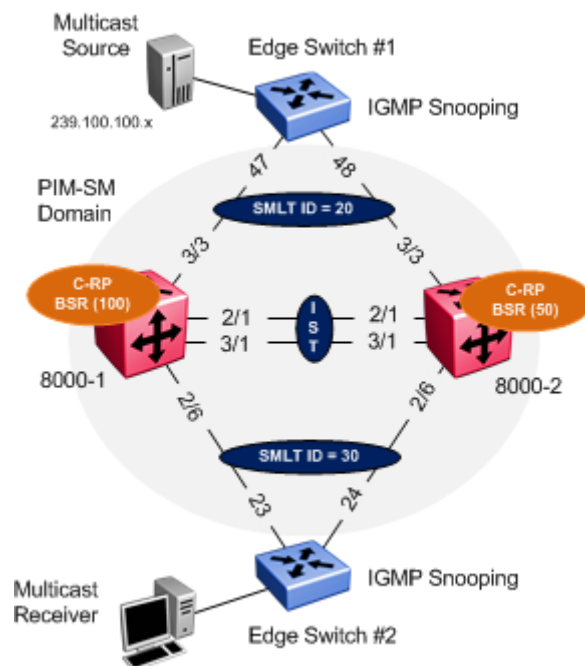


Figure 12: PIM-SM RSMLT Triangle Design

In this example the following will be configured as shown in Figure 12:

- IST
 - VLAN 2 is configured and associated to MLT# 1.
 - Tagging and auto negotiation are enabled on ports 2/1,3/1
- VLACP and SLPP settings are configured as defined in the Switch Clustering using SMLT TCG - NN48500-518
- Routed VLAN 100 (port 2/1, 3/1) is configured between ERS 8000-1 & 8000-2



It is good practice to avoid enabling OSPF on IST interfaces. In addition VLANs that extend to SMLT edge switch should be OSPF passive. As a result a “Routed VLAN” is configured and assigned to the IST ports in order for each SMLT peer to discover each others candidate RPs and BSRs. The Routed VLAN is configured with PIM and OSPF. The Routed VLAN is used to form OSPF neighbors and to exchange LSA’s between the SMLT peers.

- SMLT ID 20: VLAN 200 (port 3/3) to edge switch 1
- SMLT ID 30: VLAN 300 (port 2/6) to edge switch 2
- RSMLT Edge enabled on SMLT VLAN 200, 300



RSMLT Edge support for resilient default gateway designs. The RSMLT peer IP and MAC addresses and VLAN information are stored in the ERS 8000 configuration file.



RSMLT Edge holdup timer should be set to 9999 (infinity) to allow the RSMLT peer nodes to forward indefinitely on behalf of each other.



As an alternative to RSMLT Edge, VRRP Master and Backup-Master can be configured to serve as a resilient default gateway for VLAN 200, 300. Please refer to Switch Clustering using SMLT TCG on how to configure VRRP.

- CLIP/Loopback addresses are configured
- Dynamic PIM-SM is enabled
- PIM-SM active mode is enabled on VLAN 200 & 300
- PIM-SM active mode is enabled on IST VLAN 2



In order to achieve sub second failovers/recoveries with PIM-SM during node recovery, PIM needs to be enabled in active mode on the IST VLAN. All VLANs associated with a SMLT should be configured in PIM active mode so that one of the nodes in the SMLT cluster can be designated the PIM DR for that VLAN. All other VLANs not associated with any SMLT and where no PIM neighbours exist can be configured in passive mode.

- Candidate RP defined on each ERS 8000 for redundant RPs.
- Candidate BSR defined on each ERS 8000 for redundant BSR.



It is recommended that the BSR and RP are configured on a CLIP/Loopback address. This will prevent a BSR or RP failure if a VLAN interface goes down.

Recommended that the OSPF router ID is configured the same as the CLIP/Loopback address for management simplicity.

- OSPF Area 0.0.0.0
- OSPF passive mode enabled on VLAN 200, 300 and on the CLIP/Loopback addresses



The circuitless IP address must be reachable throughout the network. It is recommended that the CLIP/Loopback address is OSPF enabled. OSPF neighbors will learn the CLIP/Loopback address through OSPF on the Routed VLAN.



It is recommended to make OSPF interfaces passive on VLANs extending to a L2 SMLT access switch. This will prevent adjacencies from forming at the access switches. In addition this will reduce the amount of OSPF control messages to the edge switches.

On the Edge switches

- VLAN 200 and 300 are configured on Edge switch 1 and 2 respectively
- MLT is configured on Edge switch 1 and 2 respectively
- IGMP Snooping and proxy are enabled on VLAN 200 and 300



It is always recommended to enable IGMP snooping and proxy on edge switches. IGMP snooping will ensure that all ports are not flooded with IPMC while proxy consolidates all MHR and sends one MHR to the IGMP Querier.

Three IPMC streams (239.100.50.100, 239.100.50.101, 239.100.50.102) are generated from a multicast source using either MC Hammer or Winsend located on Edge switch #1. A multicast receiver for all three IPMC streams are located off Edge switch #2.

5.1.1 Configuration – ERS 8000 cluster

For this configuration example, 8000-1 is configured using the ACLI command interface while 8000-2 is configured using the CLI command interface.

5.1.1.1 IST Configuration

8000-1: Step 1 - Create IST using VLAN 2 and MLT 1

```
8000-1:5(config)#vlan create 2 name IST type port 1
8000-1:5(config-if)#interface vlan 2
8000-1:5(config-if)#ip address 10.50.2.1 255.255.255.252
8000-1:5(config-if)#exit
8000-1:5(config)#mlt 1
8000-1:5(config)#mlt 1 name IST
8000-1:5(config)#mlt 1 member 2/1,3/1
8000-1:5(config)#vlan mlt 2 1
8000-1:5(config)#mlt 1 encapsulation dot1q
8000-1:5(config)#interface mlt 1
8000-1:5(config-mlt)#ist peer-ip 10.50.2.2 vlan 2
8000-1:5(config-mlt)#ist enable
8000-1:5(config-mlt)#exit
```

8000-2: Step 1 - Create IST using VLAN 2 and MLT 1

```
8000-2:5# config vlan 2 create byport 1 name IST
8000-2:5# config vlan 2 ip create 10.50.2.2/30
8000-2:5# config mlt 1 create
8000-2:5# config mlt 1 add ports 2/1,3/1
8000-2:5# config vlan 2 add-mlt 1
8000-2:5# config mlt 1 name IST
8000-2:5# config mlt 1 perform-tagging enable
8000-2:5# config mlt 1 ist create ip 10.50.2.1 vlan-id 2
8000-2:5# config mlt 1 ist enable
```

8000-1: Step 2 – Enable VLACP globally and at interface level

```
8000-1:5(config)#interface gigabitEthernet 2/1,3/1
8000-1:5(config-if)#vlacp funcmac-addr 01:80:c2:00:00:0f
8000-1:5(config-if)#vlacp slow-periodic-time 10000
```

```
8000-1:5(config-if)#vlacp enable
8000-1:5(config-if)#exit
8000-1:5(config)#vlacp enable
```

8000-2: Step 2 - Enable VLACP globally and at interface level

```
8000-2:5# config ethernet 2/1,3/1 vlacp macaddress 01:80:c2:00:00:0f
8000-2:5# config ethernet 2/1,3/1 vlacp slow-periodic-time 10000
8000-2:5# config ethernet 2/1,3/1 vlacp enable
8000-2:5# config vlacp enable
```

5.1.1.2 Create Routed VLAN

8000-1: Step 1: Create VLAN 100

```
8000-1:5(config)#vlan create 100 name "Routed VLAN" type port 1
8000-1:5(config)#interface vlan 100
8000-1:5(config-if)#ip address 10.50.100.1 255.255.255.0
8000-1:5(config-if)#exit
8000-1:5(config)#vlan mlt 200 1
```

8000-2: Step 1: Create VLAN 100

```
8000-2:5# config vlan 100 create byport 1 name "Routed VLAN"
8000-2:5# config vlan 100 ip create 10.50.100.2/24
8000-2:5# config mlt 1 add vlan 100
```

5.1.1.3 Create Access VLANs

8000-1: Step 1: Create VLAN 200 using MLT/SMLT ID 20

```
8000-1:5(config)#vlan create 200 name Closet_Sw1 type port 1
8000-1:5(config)#interface vlan 200
8000-1:5(config-if)#ip address 10.50.200.1 255.255.255.0
8000-1:5(config-if)#exit
8000-1:5(config)#mlt 20
8000-1:5(config)#vlan mlt 200 20
8000-1:5(config)#mlt 20 name SMLT-20
8000-1:5(config)#mlt 20 encapsulation dot1q
8000-1:5(config)#mlt 20 member 3/3
8000-1:5(config)#interface mlt 20
8000-1:5(config-mlt)#smlt 20
8000-1:5(config-mlt)#exit
8000-1:5(config)#vlan mlt 200 1
```

8000-2: Step 1: Create VLAN 200 using MLT/SMLT ID 20

```
8000-2:5# config vlan 200 create byport 1 name "Closet_Sw1"
8000-2:5# config vlan 200 ip create 10.50.200.2/24
8000-2:5# config mlt 20 create
8000-2:5# config vlan 200 add-mlt 20
8000-2:5# config mlt 20 name SMLT-20
8000-2:5# config mlt 20 perform-tagging enable
8000-2:5# config mlt 20 add ports 3/3
8000-2:5# config mlt 20 smlt create smlt-id 20
8000-2:5# config mlt 1 add vlan 200
```

8000-1: Step 2: Create VLAN 300 using MLT/SMLT ID 30

```
8000-1:5(config)#vlan create 300 name Closet_Sw2 type port 1
8000-1:5(config)#interface vlan 300
8000-1:5(config-if)#ip address 10.50.30.1 255.255.255.0
8000-1:5(config-if)#exit
8000-1:5(config)#mlt 30
8000-1:5(config)#vlan mlt 300 30
8000-1:5(config)#mlt 30 name SMLT-30
8000-1:5(config)#mlt 30 encapsulation dot1q
8000-1:5(config)#mlt 30 member 2/6
8000-1:5(config)#interface mlt 30
8000-1:5(config-mlt)#smlt 30
8000-1:5(config-mlt)#exit
8000-1:5(config)#vlan mlt 300 1
```

8000-2: Step 2: Create VLAN 300 using MLT/SMLT ID 30

```
8000-2:5# config vlan 300 create byport 1 name Closet_Sw2
8000-2:5# config vlan 300 ip create 10.50.30.2/24
8000-2:5# config mlt 30 create
8000-2:5# config vlan 300 add-mlt 30
8000-2:5# config mlt 30 name SMLT-30
8000-2:5# config mlt 30 perform-tagging enable
8000-2:5# config mlt 30 add ports 2/6
8000-2:5# config mlt 30 smlt create smlt-id 30
8000-2:5# config mlt 1 add vlan 300
```


5.1.1.4 VLACP

As the access switches are an Avaya stackable switch, we will enable VLACP and use the short timeout option with the recommended fast-periodic-time of 500ms and time-out scale of 5. In addition, we will use the recommended VLACP reserved MAC address.

8000-1: Step 1 – Enable VLACP at port level

```
8000-1:5(config)#interface gigabitEthernet 2/6,3/3
8000-1:5(config-if)#vlacp fast-periodic-time 500
8000-1:5(config-if)#vlacp timeout short
8000-1:5(config-if)#vlacp timeout-scale 5
8000-1:5(config-if)#vlacp funcmac-addr 01:80:c2:00:00:0f
8000-1:5(config-if)#vlacp enable
8000-1:5(config-if)#exit
```

8000-2: Step 1 – Enable VLACP at port level

```
8000-2:5# config ethernet 2/6,3/3 vlacp fast-periodic-time 500
8000-2:5# config ethernet 2/6,3/3 vlacp timeout short
8000-2:5# config ethernet 2/6,3/3 vlacp timeout-scale 5
8000-2:5# config ethernet 2/6,3/3 vlacp macaddress 01:80:c2:00:00:0f
8000-2:5# config ethernet 2/6,3/3 vlacp enable
```



Do not enable VLACP on a port level until the VLACP MAC address has been changed.

5.1.1.5 Discard Untagged Frames

8000-1: Step 1 – Enable discard untagged frames

```
8000-1:5(config)#interface gigabitEthernet 2/1,2/6,3/1,3/3
8000-1:5(config-if)#untagged-frames-discard
8000-1:5(config-if)#exit
```

8000-2: Step 1 – Enable discard untagged frames

```
8000-2:5# config ethernet 2/1,2/6,3/1,3/3 untagged-frames-discard enable
```

5.1.1.6 SLPP

8000-1: Step 1 – Enable SLPP on VLANs 200 and 300 where 8000-1 is the primary switch

```
8000-1:5(config)#slpp vid 200,300
8000-1:5(config)#slpp enable
8000-1:5(config)#interface gigabitEthernet 2/6,3/3
8000-1:5(config-if)#slpp packet-rx-threshold 5
8000-1:5(config-if)#slpp packet-rx
8000-1:5(config-if)#exit
```

8000-2: Step 1 – Enable SLPP on VLANs 200 and 300 where 8000-2 is the secondary switch

```
8000-2:5# config slpp add 200,300
8000-2:5# config slpp operation enable
8000-2:5# config ethernet 2/6,3/3 slpp packet-rx enable
8000-2:5# config ethernet 2/6,3/3 slpp packet-rx-threshold 50
```

5.1.1.7 Enable RSMLT Edge

8000-1: Step 1: RSMLT Edge Configuration

```
8000-1:5(config)#ip rsmlt edge-support
8000-1:5(config)#interface vlan 200
8000-1:5(config-if)#ip rsmlt
8000-1:5(config-if)#ip rsmlt holdup-timer 9999
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 300
8000-1:5(config-if)#ip rsmlt
8000-1:5(config-if)#ip rsmlt holdup-timer 9999
8000-1:5(config-if)#exit
```

8000-2: Step 1: RSMLT Edge Configuration

```
8000-2:5# config ip rsmlt rsmlt-edge-support enable
8000-2:5# config vlan 200 ip rsmlt enable
8000-2:5# config vlan 200 ip rsmlt holdup-timer 9999
8000-2:5# config vlan 300 ip rsmlt enable
8000-2:5# config vlan 300 ip rsmlt holdup-timer 9999
```

5.1.1.8 Circuitless/Loopback IP address configuration

8000-1: Step 1 – Create loopback address

```
8000-1:5(config)#interface loopback 1
8000-1:5(config-if)#ip address 10.50.1.1/32
8000-1:5(config-if)#ip ospf
8000-1:5(config-if)#ip pim
8000-1:5(config-if)#exit
```

8000-1: Step 1 – Create CLIP address

```
8000-2:5# config ip circuitless-ip-int 1 create 10.50.1.2/32
8000-2:5# config ip circuitless-ip-int 1 ospf enable
8000-2:5# config ip circuitless-ip-int 1 pim enable
```

5.1.1.9 OSPF Configuration

8000-1: Step 1 – OSPF global configuration

```
8000-1:5(config)#router ospf enable
8000-1:5(config)#router ospf
8000-1:5(config-ospf)#router-id 10.50.1.1
8000-1:5(config-ospf)#exit
```

8000-2: Step 1 – OSPF global configuration

```
8000-2:5# config ip ospf admin-state enable
8000-2:5# config ip ospf router-id 10.50.1.2
8000-2:5# config ip ospf enable
```

8000-1: Step 2 – OSPF interface configuration

```
8000-1:5(config)#interface vlan 100
8000-1:5(config-if)#ip ospf enable
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 200
8000-1:5(config-if)#ip ospf network passive
8000-1:5(config-if)#ip ospf enable
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 300
8000-1:5(config-if)#ip ospf network passive
8000-1:5(config-if)#ip ospf enable
```

```
8000-1:5(config-if)#exit
```

8000-2: Step 2 – OSPF interface configuration

```
8000-2:5# config vlan 100 ip ospf enable
8000-2:5# config vlan 200 ip ospf interface-type passive
8000-2:5# config vlan 200 ip ospf enable
8000-2:5# config vlan 300 ip ospf interface-type passive
8000-2:5# config vlan 300 ip ospf enable
```

5.1.1.10 PIM Configuration

8000-1: Step 1 – PIM global configuration

```
8000-1:5(config)#ip pim enable
8000-1:5(config)#ip pim rp-candidate group 239.0.0.0 255.0.0.0 rp 10.50.1.1
8000-1:5(config)#interface loopback 1
8000-1:5(config-if)#ip pim bsr-candidate preference 100
8000-1:5(config-if)#exit
```

8000-2: Step 1 – PIM global configuration

```
8000-2:5# config ip pim enable
8000-2:5# config ip pim candrp add grp 239.0.0.0 mask 255.0.0.0 rp 10.50.1.2
8000-2:5# config ip pim candbsr interface 10.50.1.2 enable preference 50
```

8000-1: Step 2 – PIM interface configuration

```
8000-1:5(config)#interface vlan 2
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 100
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 200
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 300
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#exit
```

8000-2: Step 2 – PIM interface configuration

```
8000-2:5# config vlan 2 ip pim enable  
8000-2:5# config vlan 100 ip pim enable  
8000-2:5# config vlan 200 ip pim enable  
8000-2:5# config vlan 300 ip pim enable
```

5.1.2 Configuration – Edge Switch

5.1.2.1 Create VLAN

Edge Switch 1: Step 1 – VLAN 200

```
Edge-1(config)#vlan create 200 name Closet_Sw1 type port
Edge-1(config)#vlan configcontrol automatic
Edge-1(config)#vlan ports 47,48 tagging tagall
Edge-1(config)#vlan members add 200 3-11,47,48
Edge-1(config)#vlan members remove 1 47,48
```

Edge Switch 2: Step 1 – VLAN 300

```
Edge-2(config)#vlan create 300 name Closet_Sw2 type port
Edge-2(config)#vlan control automatic
Edge-2(config)#vlan port 23,24 tagging tagall
Edge-2(config)#vlan member add 300 3-11,23,24
Edge-2(config)#vlan members remove 1 23,24
```

5.1.2.1 Create MLT

Edge Switch 1: Step 1 – Create MLT

```
Edge-1(config)#mlt 1 enable member 47,48 learning disable
```

Edge Switch 2: Step 1 – Create MLT

```
Edge-2(config)#mlt 1 enable member 23,24 learning disable
```

5.1.2.1 VLACP

Edge Switch 1: Step 1 – Enable VLACP

```
Edge-1(config)#vlacp macaddress 180.c200.f
Edge-1(config)#vlacp enable
Edge-1(config)#interface fastEthernet 47,48
Edge-1(config-if)#vlacp timeout short
Edge-1(config-if)#vlacp timeout-scale 5
Edge-1(config-if)#vlacp enable
Edge-1(config-if)#exit
```

Edge Switch 2: Step 1 – Enable VLACP

```
Edge-2(config)#vlacp macaddress 180.c200.f
Edge-2(config)#vlacp enable
Edge-2(config)#interface fastEthernet 23,24
Edge-2(config-if)#vlacp timeout short
Edge-2(config-if)#vlacp timeout-scale 5
Edge-2(config-if)#vlacp enable
Edge-2(config-if)#exit
```

5.1.2.2 Enable Spanning Tree FastStart and BPDU filtering on all access ports

Edge Switch 1: Step 1 – Enable STP FastStart and BPDU Filtering

```
Edge-1(config)#interface fastEthernet 3-11
Edge-1(config-if)#spanning-tree learning fast
Edge-1(config-if)#spanning-tree bpdu-filtering timeout 0
Edge-1(config-if)#spanning-tree bpdu-filtering enable
Edge-1(config-if)#exit
```

Edge Switch 2: Step 1 – Enable STP FastStart and BPDU Filtering

```
Edge-2(config)#interface fastEthernet 3-11
Edge-2(config-if)#spanning-tree learning fast
Edge-2(config-if)#spanning-tree bpdu-filtering timeout 0
Edge-2(config-if)#spanning-tree bpdu-filtering enable
Edge-2(config-if)#exit
```

5.1.2.1 Discard Untagged Frames

Edge Switch 1: Step 1 – Enable Discard Untagged Frames

```
Edge-1(config)#vlan ports 47-48 filter-untagged-frame enable
```

Edge Switch 2: Step 1 – Enable Discard Untagged Frames

```
Edge-2(config)#vlan ports 23-24 filter-untagged-frame enable
```



Please note that with the ERS 5510 only, you cannot enable filter untagged frames when using VLACP. This does not apply to the ERS 5520 or ERS 5530.

5.1.2.1 Enable IGMP Snoop/Proxy

Edge Switch 1: Step 1 – Enable IGMP Snoop/Proxy

```
Edge-1(config)#vlan igmp 200 snooping enable  
Edge-1(config)#vlan igmp 200 proxy enable
```

Edge Switch 2: Step 1 – Enable IGMP Snoop/Proxy

```
Edge-2(config)#vlan igmp 300 snooping enable  
Edge-2(config)#vlan igmp 300 proxy enable
```


5.1.3 Verify Operations

5.1.3.1 IGMP

Step 1 – SMLT Cluster: Verifying IGMP Queriers

CLI/ACLI

show ip igmp interface

Results:

8000-1:

```
=====
                                IGMP Interface - GlobalRouter
=====
```

IF	QUERY		OPER		QUERY	WRONG	LASTMEM		
	INTVL	STATUS	VERS.	VERS	MAXRSPT	QUERY	JOINS	ROBUST	QUERY

V0	125	inact	2	2	0.0.0.0	100	0	0	2 10
V2	125	active	2	2	10.50.2.1	100	0	0	2 10
V200	125	active	2	2	10.50.200.1	100	0	101	2 10
V300	125	active	2	2	10.50.30.1	100	0	163	2 10
V100	125	active	2	2	10.50.100.1	100	0	0	2 10

8000-2:

```
=====
                                IGMP Interface - GlobalRouter
=====
```

IF	QUERY		OPER		QUERY	WRONG	LASTMEM		
	INTVL	STATUS	VERS.	VERS	MAXRSPT	QUERY	JOINS	ROBUST	QUERY

V0	125	inact	2	2	0.0.0.0	100	0	0	2 10
V2	125	active	2	2	10.50.2.1	100	0	0	2 10
V200	125	active	2	2	10.50.200.1	100	0	101	2 10
V300	125	active	2	2	10.50.30.1	100	0	163	2 10
V100	125	active	2	2	10.50.100.1	100	0	0	2 10

Step 1 – Edge Switch: Verifying IGMP Queriers

ACLI

```
show ip igmp interface
```

Results:

Edge-1:

Query		Oper			Query	Wrong			LastMbr	Send
VLAN	Intvl	Vers	Vers	Querier	MaxRspT	Query	Joins	Robust	Query	Query
----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
200	125	2	2	10.50.200.1	100	0	141	2	10	No

Edge-2:

Query		Oper			Query	Wrong			LastMbr	Send
VLAN	Intvl	Vers	Vers	Querier	MaxRspT	Query	Joins	Robust	Query	Query
----	----	----	----	-----	-----	-----	-----	-----	-----	-----
300	125	2	2	10.50.30.1	100	0	181	2	10	No

The ERS 8000 and the edge switches should all see the same IGMP Querier IP address. This should be the IGMP Querier with the lowest IP address on the subnet. Ensure that the correct IP interface is advertising as the IGMP querier.



On the ERS 8000, enabling any multicast routing protocol such as PIM-SM, PIM-SSM or DVMRP on an IP interface will enable the IGMP querier function.

Step 2 - SMLT Cluster: Verifying IGMP Groups

CLI/ACLI

show ip igmp group

Results:

8000-1:

```
=====
                                IGMP Group - GlobalRouter
=====
GRPADDR      INPORT      MEMBER      EXPIRATION TYPE
-----
239.100.100.100 V300-2/6    10.50.30.20  240      Dynamic
239.100.100.101 V300-2/6    10.50.30.20  240      Dynamic
239.100.100.102 V300-2/6    10.50.30.20  240      Dynamic
```

8000-2:

```
=====
                                IGMP Group - GlobalRouter
=====
GRPADDR      INPORT      MEMBER      EXPIRATION TYPE
-----
239.100.100.100 V300-2/6    10.50.30.20  251      Dynamic
239.100.100.101 V300-2/6    10.50.30.20  248      Dynamic
239.100.100.102 V300-2/6    10.50.30.20  254      Dynamic
```

Step 2 – Edge Switch: Verifying IGMP Groups

ACLI

show ip igmp group

Results: from Edge-2

Group	Address	VLAN	Member	Address	Expiration	Type	In Port
239.100.100.100	300	10.50.30.20	235	Dynamic	7		
239.100.100.101	300	10.50.30.20	240	Dynamic	7		
239.100.100.102	300	10.50.30.20	238	Dynamic	7		

Step 3 – SMLT Cluster: Verifying IGMP Senders

CLI/ACLI

show ip igmp sender

Results: from 8000-1

```
=====
                        IGMP Sender - GlobalRouter
=====
                        PORT/
GRPADDR      IFINDEX  MEMBER      MLT      STATE
-----
239.100.100.100 Vlan 200   10.50.200.10 MLT-20   NOTFILTERED
239.100.100.101 Vlan 200   10.50.200.10 MLT-20   NOTFILTERED
239.100.100.102 Vlan 200   10.50.200.10 MLT-20   NOTFILTERED
```

5.1.3.2 PIM

Step 1: Verify PIM neighbors

CLI/ACLI

show ip pim neighbor

Results: from 8000-1 and 8000-2

8000-1:

```
=====
                                PIM Neighbor - GlobalRouter
=====
INTERFACE ADDRESS          UPTIME                      EXPIRE
-----
Vlan2      10.50.2.2                0 day(s), 00:43:29          0 day(s), 00:01:16
Vlan100    10.50.100.2              0 day(s), 00:20:22          0 day(s), 00:01:23
```

8000-2:

```
=====
                                PIM Neighbor - GlobalRouter
=====
INTERFACE ADDRESS          UPTIME                      EXPIRE
-----
Vlan2      10.50.2.1                0 day(s), 00:43:54          0 day(s), 00:01:20
Vlan100    10.50.100.1              0 day(s), 00:20:47          0 day(s), 00:01:28
```

Step 2: Verify that the BSR are identical on 8000-1 and 8000-2

CLI

```
show ip pim bsr
```

Results: from 8000-1

8000-1:

```
=====
                        BootStrap Router Info - GlobalRouter
=====
```

```
Current BSR address: 10.50.1.1
Current BSR priority: 100
Current BSR HashMask: 255.255.255.252
Current BSR Fragment Tag: 60
Pim Bootstrap Timer : 46
```

8000-2:

```
=====
                        BootStrap Router Info - GlobalRouter
=====
```

```
Current BSR address: 10.50.1.1
Current BSR priority: 100
Current BSR HashMask: 255.255.255.252
Current BSR Fragment Tag: 60
Pim Bootstrap Timer : 106
```

Step 3: Verify RP Candidate

CLI/ACLI

show ip pim rp-candidate

Results: Should display local CLIP/Loopback address

8000-1:

```
=====
                        PIM Candidate RP Table - GlobalRouter
=====
GRPADDR      GRPMASK      RPADDR
-----
239.0.0.0    255.0.0.0    10.50.1.1
```

8000-2:

```
=====
                        PIM Candidate RP Table - GlobalRouter
=====
GRPADDR      GRPMASK      RPADDR
-----
239.0.0.0    255.0.0.0    10.50.1.2
```

Step 4: Verify that the Active RP are identical on 8000-1 and 8000-2

CLI/ACLI

show ip pim active-rp

Results:

8000-1:

```
=====
                        PIM Grp->RP Active RP Table - GlobalRouter
=====
GRPADDR          RP-ADDR          RP-PRIORITY
-----
239.100.100.100   10.50.1.1          0
239.100.100.101   10.50.1.1          0
239.100.100.102   10.50.1.1          0
```

8000-2:

```
=====
                        PIM Grp->RP Active RP Table - GlobalRouter
=====
GRPADDR          RP-ADDR          RP-PRIORITY
-----
239.100.100.100   10.50.1.1          0
239.100.100.101   10.50.1.1          0
239.100.100.102   10.50.1.1          0
```



The RP-Set, a collection of candidate RPs, is distributed by the BSR. Each PIM-SM router uses the BSR hash Mask and the RP set to determine the active RP for a given multicast group. The active RP for a given multicast group should be the same for each PIM-SM router within the PIM-SM domain.

5.1.3.3 Verify multicast routing table

Step 1: Verify multicast routing table on 8000-1 and 8000-2

CLI/ACLI

show ip pim mroute

Results:

8000-1:

```
=====
                          PIM Multicast Route - Global Router
=====
```

Src: 0.0.0.0 Grp: 239.100.100.100 RP: 10.50.1.1 Upstream: NULL

Flags: WC RP CACHE

Incoming Port: Vlan0-cpp,

Outgoing Ports: Vlan100-2/1, Vlan300-2/6,

Joined Ports: Vlan100-2/1,

Pruned Ports:

Leaf Ports: Vlan300-2/6,

Asserted Ports:

Prune Pending Ports:

Assert Winner Ifs:

Assert Loser Ifs:

TIMERS:

Entry	JP	RS	Assert
199	0	0	0

VLAN-Id: 2 100

Join-P: 0 199

Assert: 0 0

```
-----
Src: 10.50.200.10 Grp: 239.100.100.100 RP: 10.50.1.1 Upstream: NULL
```

Flags:

SPT CACHE SG

Incoming Port: Vlan200-MLT-20(3/3),

Outgoing Ports: Vlan300-2/6,

Joined Ports: Vlan100-2/1,

Pruned Ports:

Leaf Ports: Vlan300-2/6,

Asserted Ports:

Prune Pending Ports:

Assert Winner Ifs:			
Assert Loser Ifs:			
TIMERS:			
Entry	JP	RS	Assert
74	0	0	0
VLAN-Id:	2	100	
Join-P:	0	199	
Assert:	0	0	

Src: 0.0.0.0 Grp: 239.100.100.101 RP: 10.50.1.1 Upstream: NULL			
Flags: WC RP CACHE			
Incoming Port: Vlan0-cpp,			
Outgoing Ports: Vlan100-2/1, Vlan300-2/6,			
Joined Ports: Vlan100-2/1,			
Pruned Ports:			
Leaf Ports:			
Vlan300-2/6,			
Asserted Ports:			
Prune Pending Ports:			
Assert Winner Ifs:			
Assert Loser Ifs:			
TIMERS:			
Entry	JP	RS	Assert
197	0	0	0
VLAN-Id:	2	100	
Join-P:	0	197	
Assert:	0	0	

Src: 10.50.200.10 Grp: 239.100.100.102 RP: 10.50.1.1 Upstream: NULL			
Flags: SPT CACHE SG			
Incoming Port: Vlan200-MLT-20(3/3),			
Outgoing Ports: Vlan300-2/6,			
Joined Ports: Vlan100-2/1,			
Pruned Ports:			
Leaf Ports: Vlan300-2/6,			
Asserted Ports:			
Prune Pending Ports:			
Assert Winner Ifs:			
Assert Loser Ifs:			
TIMERS:			
Entry	JP	RS	Assert

199	0	0	0
VLAN-Id:	2	100	
Join-P:	0	174	
Assert:	0	0	

Src: 0.0.0.0	Grp: 239.255.255.250	RP: 10.50.1.1	Upstream: NULL
Flags:	WC RP CACHE		
Incoming Port:	Vlan0-cpp,		
Outgoing Ports:	Vlan100-2/1, Vlan200-3/3, Vlan300-2/6,		
Joined Ports:			
Vlan100-2/1,			
Pruned Ports:			
Leaf Ports:	Vlan200-3/3, Vlan300-2/6,		
Asserted Ports:			
Prune Pending Ports:			
Assert Winner Ifs:			
Assert Loser Ifs:			
TIMERS:			
Entry	JP	RS	Assert
174	0	0	0
VLAN-Id:	2	100	
Join-P:	0	174	
Assert:	0	0	

Src: 10.50.30.20	Grp: 239.255.255.250	RP: 10.50.1.1	Upstream: NULL
Flags:	SPT CACHE SG		
Incoming Port:	Vlan300-MLT-30(2/6),		
Outgoing Ports:	Vlan200-3/3, Vlan300-2/6,		
Joined Ports:	Vlan100-2/1,		
Pruned Ports:			
Leaf Ports:	Vlan200-3/3, Vlan300-2/6,		
Asserted Ports:			
Prune Pending Ports:			
Assert Winner Ifs:			
Assert Loser Ifs:			
TIMERS:			
Entry	JP	RS	Assert
204	0	0	0
VLAN-Id:	2	100	
Join-P:	0	173	

Assert: 0 0

Total Num of Entries Displayed 8/8

Flags Legend:

SPT = Shortest path tree, WC=(*,Grp) entry, RP=Rendezvous Point tree, CACHE=Kernel Cache, ASSERTED=Asserted, SG=(Src,Grp) entry, PMBR=(*,*,RP) entry, FWD_TO_RP=Forwarding to RP, FWD_TO_DR=Forwarding to DR, SG_NODATA=SG Due to Join, A=SG Advertised to MSDP, M=SG Created by MSDP, CP_TO_CPU=Copy to CPU, STATIC_MROUTE=Static Mroute, MRTF_SMLT_PEER_SG=Peer SG On Non-DR For SMLT

8000-2:

=====

PIM Multicast Route - Global Router

=====

Src: 0.0.0.0 Grp: 239.100.100.100 RP: 10.50.1.1 Upstream: 10.50.100.1

Flags: WC RP

Incoming Port: Vlan100-MLT-1(2/1),

Outgoing Ports: Vlan300-2/6,

Joined Ports:

Pruned Ports:

Leaf Ports: Vlan300-2/6,

Asserted Ports:

Prune Pending Ports:

Assert Winner Ifs:

Assert Loser Ifs:

TIMERS:

Entry	JP	RS	Assert
79	29	0	0

VLAN-Id: 2 100

Join-P: 0 0

Assert: 0 0

Src: 0.0.0.0 Grp: 239.100.100.101 RP: 10.50.1.1 Upstream: 10.50.100.1

Flags:

WC RP

Incoming Port: Vlan100-MLT-1(2/1),

Outgoing Ports: Vlan300-2/6,

Joined Ports:

Pruned Ports:

Leaf Ports: Vlan300-2/6,

Asserted Ports:

Prune Pending Ports:			
Assert Winner Ifs:			
Assert Loser Ifs:			
TIMERS:			
Entry	JP	RS	Assert
79	29	0	0
VLAN-Id:	2	100	
Join-P:	0	0	
Assert:	0	0	

Src: 0.0.0.0 Grp: 239.100.100.102 RP: 10.50.1.1 Upstream: 10.50.100.1			
Flags: WC RP			
Incoming Port: Vlan100-MLT-1(2/1),			
Outgoing Ports: Vlan300-2/6,			
Joined Ports:			
Pruned Ports:			
Leaf Ports:			
Vlan300-2/6,			
Asserted Ports:			
Prune Pending Ports:			
Assert Winner Ifs:			
Assert Loser Ifs:			
TIMERS:			
Entry	JP	RS	Assert
77	27	0	0
VLAN-Id:	2	100	
Join-P:	0	0	
Assert:	0	0	

Src: 0.0.0.0 Grp: 239.255.255.250 RP: 10.50.1.1 Upstream: 10.50.100.1			
Flags: WC RP			
Incoming Port: Vlan100-MLT-1(2/1),			
Outgoing Ports: Vlan200-3/3, Vlan300-2/6,			
Joined Ports:			
Pruned Ports:			
Leaf Ports: Vlan200-3/3, Vlan300-2/6,			
Asserted Ports:			
Prune Pending Ports:			
Assert Winner Ifs:			
Assert Loser Ifs:			
TIMERS:			

Entry	JP	RS	Assert
77	27	0	0
VLAN-Id:	2	100	
Join-P:	0	0	
Assert:	0	0	

Total Num of Entries Displayed 4/4			
Flags Legend:			
SPT = Shortest path tree, WC=(*,Grp) entry, RP=Rendezvous Point tree, CACHE=Kernel Cache, ASSERTED=Asserted, SG=(Src,Grp) entry, PMBR=(*,*,RP) entry, FWD_TO_RP=Forwarding to RP, FWD_TO_DR=Forwarding to DR, SG_NODATA=SG Due to Join, A=SG Advertised to MSDP, M=SG Created by MSDP, CP_TO_CPU=Copy to CPU, STATIC_MROUTE=Static Mroute, MRTF_SMLT_PEER_SG=Peer SG On Non-DR For SMLT			



For each multicast group there needs to be two entries in the multicast route table, a wildcard entry (*,G) and a SPT entry (S,G). Without these entries a DR will not be able to join a Rendezvous Point Tree and subsequently the DR will not learn the source of the IPMC. Consequently an (S,G) entry will never occur and a SP-Tree will never be formed.



The incoming ports (IIF) and outgoing ports (OIF) are determined by the RPF to either the RP or to the source.



The same information can also be viewed by using show ip mroute route and show ip mroute next-hop to indicate the upstream multicast neighbor to either RP-Tree or SP-Tree; as determined by the RPF algorithm.

5.2 PIM-SM Anycast-RP Triangle Topology with L2 Edge – VSP9000

The following diagram is an example of the configuration of PIM-SM Anycast-RP on RSMLT Triangle topology using the VSP-9000. Please refer to the Switch Clustering using Split Multi-Link Trunking (SMLT) Technical Configuration Guide for details on the best practices for SMLT.

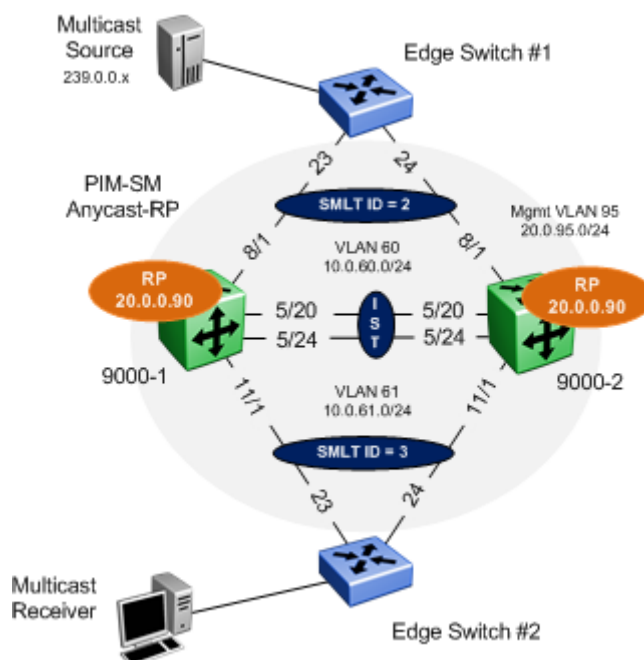


Figure 13: PIM-SM anycast-RP Triangle Design

In this example the following will be configured as shown in Figure 13:

- IST
 - VLAN 4000 is configured and associated to MLT# 512.
 - Tagging is enabled on ports 5/20,5/24
- VLACP and SLPP settings are configured as defined in the Switch Clustering using SMLT TCG - NN48500-518
- SMLT ID 2: VLAN 60 (port 8/1) and VLAN 95 (mgmt) to edge switch 1
- SMLT ID 3: VLAN 61 (port 11/1) and VLAN 95 (mgmt) to edge switch 2
- RSMLT Edge enabled on SMLT VLAN 60 and 61



RSMLT Edge support for resilient default gateway designs. The RSMLT peer IP and MAC addresses and VLAN information are stored in the VSP 9000 configuration file.



RSMLT Edge holdup timer should be set to 9999 (infinity) to allow the RSMLT peer nodes to forward indefinitely on behalf of each other.



As an alternative to RSMLT Edge, VRRP Master and Backup-Master can be configured to serve as a resilient default gateway for VLAN 10, 61, and 95. Please refer to Switch Clustering using SMLT TCG on how to configure VRRP.

- Loopback addresses are configured
- Dynamic PIM-SM is enabled
- PIM-SM active mode is enabled on VLAN 60 & 61
- PIM-SM active mode is enabled on IST VLAN 4000



In order to achieve sub second failovers/recoveries with PIM-SM the IST VLAN and all VLANs associated with a SMLT should be configured in PIM active mode. All other VLANs not associated with either a SMLT or PIM adjacencies should be configured in passive mode.

- We are not using an IGP protocol as all forwarding is done via the cluster switch only
- We will also use a loopback address instead of an interface address as the loopback interface is not dependant on the up/down state of an interface

On the Edge switches

- VLAN 60 and 61 are configured on Edge switch 1 and 2 respectively
- MLT is configured on Edge switch 1 and 2 respectively
- IGMP Snooping and proxy are enabled on VLAN 60 and 61



It is always recommended to enable IGMP snooping and proxy on edge switches. IGMP snooping will ensure that all ports are not flooded with IPMC while proxy consolidates all MHR and sends one MHR to the IGMP Querier.

5.2.1 Configuration – VSP 9000 cluster

5.2.1.1 IST Configuration

9000-1: Step 1 - Create IST using VLAN 4000 and MLT 512

```
9000-1:1(config)#vlan create 512 name IST port-mstprstp 0
9000-1:1(config)#interface vlan 4000
9000-1:1(config-if)#ip address 192.168.255.1 255.255.255.252
9000-1:1(config-if)#exit
9000-1:1(config)#mlt 512 enable name IST
9000-1:1(config)#mlt 512 member 5/20,5/24
9000-1:1(config)#mlt 1 encapsulation dot1q
9000-1:1(config)#vlan mlt 4000 512
9000-1:1(config)#interface mlt 512
9000-1:1(config-mlt)#ist 192.168.255.2 vlan 4000
9000-1:1(config-mlt)#ist enable
9000-1:1(config-mlt)#exit
```

9000-2: Step 1 - Create IST using VLAN 4000 and MLT 512

```
9000-2:1(config)#vlan create 512 name IST port-mstprstp 0
9000-2:1(config)#interface vlan 4000
9000-2:1(config-if)#ip address 192.168.255.2 255.255.255.252
9000-2:1(config-if)#exit
9000-2:1(config)#mlt 512 enable name IST
9000-2:1(config)#mlt 512 member 5/20,5/24
9000-2:1(config)#mlt 1 encapsulation dot1q
9000-2:1(config)#vlan mlt 4000 512
9000-2:1(config)#interface mlt 512
9000-2:1(config-mlt)#ist 192.168.255.1 vlan 4000
9000-2:1(config-mlt)#ist enable
9000-2:1(config-mlt)#exit
```

9000-1: Step 2 – Enable VLACP globally and at interface level

```
9000-1:1(config)#interface gigabitEthernet 5/20,5/24
9000-1:1(config)#no shutdown
9000-1:1(config-if)#vlacp slow-periodic-time 10000 timeout long funcmac-addr
01:80:c2:00:00:0f
9000-1:1(config-if)#vlacp enable
9000-1:1(config-if)#exit
9000-1:1(config)#vlacp enable
```

9000-2: Step 2 - Enable VLACP globally and at interface level

```
9000-2:1(config)#interface gigabitEthernet 5/20,5/24
9000-2:1(config)#no shutdown
9000-2:1(config-if)#vlacp slow-periodic-time 10000 timeout long funcmac-addr
01:80:c2:00:00:0f
9000-2:1(config-if)#vlacp enable
9000-2:1(config-if)#exit
9000-2:1(config)#vlacp enable
```

5.2.1.2 Create Access VLANs

9000-1: Step 1: Create VLAN 60 using MLT/SMLT ID 2

```
9000-1:1(config)# vlan create 60 name "User-60" type port-mstprstp 0
9000-1:1(config)# interface vlan 60
9000-1:1(config-if)# ip address 20.0.60.1 255.255.255.0
9000-1:1(config-if)# exit
9000-1:1(config)# mlt 2 enable name "Edge-1"
9000-1:1(config)# mlt 2 member 8/1
9000-1:1(config)# mlt 2 encapsulation dot1q
9000-1:1(config)# vlan mlt 60 2
9000-1:1(config)# interface mlt 2
9000-1:1(config-mlt)# smlt
9000-1:1(config-mlt)# exit
9000-1:1(config)# vlan mlt 60 512
```

9000-2: Step 1: Create VLAN 60 using MLT/SMLT ID 2

```
9000-2:1(config)# vlan create 60 name "User-60" type port-mstprstp 0
9000-2:1(config)# interface vlan 60
9000-2:1(config-if)# ip address 20.0.60.2 255.255.255.0
9000-2:1(config-if)# exit
9000-2:1(config)# mlt 2 enable name "Edge-1"
9000-2:1(config)# mlt 2 member 8/1
9000-2:1(config)# mlt 2 encapsulation dot1q
9000-2:1(config)# vlan mlt 60 2
9000-2:1(config)# interface mlt 2
9000-2:1(config-mlt)# smlt
9000-2:1(config-mlt)# exit
9000-2:1(config)# vlan mlt 60 512
```

9000-1: Step 2: Create VLAN 61 using MLT/SMLT ID 3

```
9000-1:1(config)# vlan create 61 name "User-61" type port-mstprstp 0
9000-1:1(config)#interface vlan 61
9000-1:1(config-if)#ip address 20.0.61.1 255.255.255.0
9000-1:1(config-if)#exit
9000-1:1(config)#mlt 3 enable name "Edge-2"
9000-1:1(config)#mlt 3 member 11/1
9000-1:1(config)#mlt 3 encapsulation dot1q
9000-1:1(config)#vlan mlt 61 3
9000-1:1(config)#interface mlt 3
9000-1:1(config-mlt)#smlt
9000-1:1(config-mlt)#exit
9000-1:1(config)#vlan mlt 61 512
```

9000-2: Step 2: Create VLAN 61 using MLT/SMLT ID 3

```
9000-2:1(config)# vlan create 61 name "User-61" type port-mstprstp 0
9000-2:1(config)#interface vlan 61
9000-2:1(config-if)#ip address 20.0.61.2 255.255.255.0
9000-2:1(config-if)#exit
9000-2:1(config)#mlt 3 enable name "Edge-2"
9000-2:1(config)#mlt 3 member 11/1
9000-2:1(config)#mlt 3 encapsulation dot1q
9000-2:1(config)#vlan mlt 61 3
9000-2:1(config)#interface mlt 3
9000-2:1(config-mlt)#smlt
9000-2:1(config-mlt)#exit
9000-2:1(config)#vlan mlt 61 512
```

5.2.1.3 Create Mgmt VLAN

9000-1: Step 1: Create management VLAN 95 for edge switches

```
9000-1:1(config)#vlan create 95 name "VSP-Edge-Mgmt" type port-mstprstp 0
9000-1:1(config)#interface vlan 95
9000-1:1(config-if)#ip address 20.0.95.1 255.255.255.0
9000-1:1(config-if)#exit
9000-1:1(config)#vlan mlt 95 2
9000-1:1(config)#vlan mlt 95 3
9000-1:1(config)#vlan mlt 95 512
```

9000-2: Step 1: Create management VLAN 95 for edge switches

```
9000-2:1(config)#vlan create 95 name "VSP-Edge-Mgmt" type port-mstprstp 0
9000-2:1(config)#interface vlan 95
9000-2:1(config-if)#ip address 20.0.95.1 255.255.255.0
9000-2:1(config-if)#exit
9000-2:1(config)#vlan mlt 95 2
9000-2:1(config)#vlan mlt 95 3
9000-2:1(config)#vlan mlt 95 512
```

5.2.1.4 VLACP – To Edge Switch

As the access switches are an Avaya stackable switch, we will enable VLACP and use the short timeout option with the recommended fast-periodic-time of 500ms and time-out scale of 5. In addition, we will use the recommended VLACP reserved MAC address.

9000-1: Step 1 – Enable VLACP at port level

```
9000-1:1(config)#interface gigabitEthernet 8/1,11/1
9000-1:1(config)#no shutdown
9000-1:1(config-if)#vlacp fast-periodic-time 500 timeout short timeout-scale 5
funcmac-addr 01:80:c2:00:00:0f
9000-1:1(config-if)#vlacp enable
9000-1:1(config-if)#exit
```

9000-2: Step 1 – Enable VLACP at port level

```
9000-2:1(config)#interface gigabitEthernet 8/1,11/1
9000-2:1(config)#no shutdown
9000-2:1(config-if)#vlacp fast-periodic-time 500 timeout short timeout-scale 5
funcmac-addr 01:80:c2:00:00:0f
9000-2:1(config-if)#vlacp enable
9000-2:1(config-if)#exit
```



Do not enable VLACP on a port level until the VLACP MAC address has been changed.

5.2.1.5 Discard Untagged Frames

9000-1: Step 1 – Enable discard untagged frames

```
9000-1:1(config)#interface gigabitEthernet 5/20,5/24,8/1,11/1
9000-1:1(config-if)#untagged-frames-discard
9000-1:1(config-if)#exit
```

9000-2: Step 1 – Enable discard untagged frames

```
9000-2:1(config)#interface gigabitEthernet 5/20,5/24,8/1,11/1
9000-2:1(config-if)#untagged-frames-discard
9000-2:1(config-if)#exit
```

5.2.1.6 SLPP

9000-1: Step 1 – Enable SLPP on VLANs 60, 61, and 95 where 9000-1 is the primary switch

```
9000-1:1(config)#slpp vid 60,61,95
9000-1:1(config)#slpp enable
9000-1:1(config)#interface gigabitEthernet 8/1,11/1
9000-1:1(config-if)#slpp packet-rx-threshold 5
9000-1:1(config-if)#slpp packet-rx
9000-1:1(config-if)#exit
```

9000-2: Step 1 – Enable SLPP on VLANs 200 and 300 where 9000-2 is the secondary switch

```
9000-2:1(config)#slpp vid 60,61,95
9000-2:1(config)#slpp enable
9000-2:1(config)#interface gigabitEthernet 8/1,11/1
9000-2:1(config-if)#slpp packet-rx-threshold 50
9000-2:1(config-if)#slpp packet-rx
9000-2:1(config-if)#exit
```

5.2.1.7 Enable RSMLT Edge

9000-1: Step 1: RSMLT Edge Configuration

```
9000-1:1(config)#ip rsmlt edge-support
9000-1:1(config)#interface vlan 60
9000-1:1(config-if)#ip rsmlt
9000-1:1(config-if)#ip rsmlt holdup-timer 9999
9000-1:1(config-if)#exit
9000-1:1(config)#interface vlan 91
9000-1:1(config-if)#ip rsmlt
9000-1:1(config-if)#ip rsmlt holdup-timer 9999
9000-1:1(config-if)#exit
9000-1:1(config)#interface vlan 95
9000-1:1(config-if)#ip rsmlt
9000-1:1(config-if)#ip rsmlt holdup-timer 9999
9000-1:1(config-if)#exit
```

9000-2: Step 1: RSMLT Edge Configuration

```
9000-2:1(config)#ip rsmlt edge-support
9000-2:1(config)#interface vlan 60
9000-2:1(config-if)#ip rsmlt
9000-2:1(config-if)#ip rsmlt holdup-timer 9999
9000-2:1(config-if)#exit
9000-2:1(config)#interface vlan 91
9000-2:1(config-if)#ip rsmlt
9000-2:1(config-if)#ip rsmlt holdup-timer 9999
9000-2:1(config-if)#exit
9000-2:1(config)#interface vlan 95
9000-2:1(config-if)#ip rsmlt
9000-2:1(config-if)#ip rsmlt holdup-timer 9999
9000-2:1(config-if)#exit
```

5.2.1.8 Loopback IP address configuration

9000-1: Step 1 – Create loopback addresses. Loopback 2 will be used for for the Anycast RP address

```
9000-1:1(config)#interface loopback 1
9000-1:1(config-if)#ip address 1 20.0.0.91/255.255.255.255
9000-1:1(config-if)#ip pim
9000-1:1(config-if)#exit
9000-1:1(config)#interface loopback 2
9000-1:1(config-if)#ip address 1 20.0.0.90/255.255.255.255
9000-1:1(config-if)#ip pim
9000-1:1(config-if)#exit
```

9000-2: Step 1 – Create Loopback address. Loopback 2 will be used for for the Anycast RP address

```
9000-2:1(config)#interface loopback 1
9000-2:1(config-if)#ip address 1 20.0.0.92/255.255.255.255
9000-2:1(config-if)#ip pim
9000-2:1(config-if)#exit
9000-2:1(config)#interface loopback 2
9000-2:1(config-if)#ip address 1 20.0.0.90/255.255.255.255
9000-2:1(config-if)#ip pim
9000-2:1(config-if)#exit
```


5.2.1.9 IP Route Configuration

9000-1: Step 1 – Static route configuration

```
9000-1:1(config)#ip route 20.0.0.92 255.255.255.255 192.168.255.2 weight 1
```

9000-2: Step 1 – Static route configuration

```
9000-2:1(config)#ip route 20.0.0.91 255.255.255.255 192.168.255.1 weight 1
```

5.2.1.10 PIM Configuration

9000-1: Step 1 – PIM global & static-rp configuration

```
9000-1:1(config)#ip pim enable
9000-1:1(config)#ip pim static-rp
9000-1:1(config)#ip pim static-rp 239.0.0.0/255.0.0.0 20.0.0.90
```

9000-2: Step 1 – PIM global & static-rp configuration

```
9000-2:1(config)#ip pim enable
9000-2:1(config)#ip pim static-rp
9000-2:1(config)#ip pim static-rp 239.0.0.0/255.0.0.0 20.0.0.90
```

9000-1: Step 2 – PIM interface configuration

```
9000-1:1(config)#interface vlan 60
9000-1:1(config-if)#ip pim enable
9000-1:1(config-if)#exit
9000-1:1(config)#interface vlan 61
9000-1:1(config-if)#ip pim enable
9000-1:1(config-if)#ip pim immediate-leave
9000-1:1(config-if)#exit
9000-1:1(config)#interface vlan 4000
9000-1:1(config-if)#ip pim enable
9000-1:1(config-if)#exit
```

9000-2: Step 2 – PIM interface configuration

```
9000-2:1(config)#interface vlan 60
9000-2:1(config-if)#ip pim enable
9000-2:1(config-if)#exit
9000-2:1(config)#interface vlan 61
```

```
9000-2:1(config-if)#ip pim enable  
9000-2:1(config-if)#ip pim immediate-leave  
9000-2:1(config-if)#exit  
9000-2:1(config)#interface vlan 4000  
9000-2:1(config-if)#ip pim enable  
9000-2:1(config-if)#exit
```

5.2.2 Configuration – Edge Switch

5.2.2.1 Create Management VLAN

Edge Switch 1: Step 1 – VLAN mgmt 95 and add IP address/mask/default gateway

```
Edge-1(config)#vlan create 95 name mgmt type port
Edge-1(config)#vlan mgmt 95
Edge-1(config)#ip address 20.0.95.11 netmask 255.0.0.0 default-gateway 20.0.95.1
Edge-1(config)#vlan configcontrol automatic
Edge-1(config)#vlan ports 23,24 tagging tagall
Edge-1(config)#vlan members add 95 23,24
Edge-1(config)#vlan members remove 1 23,24
```

Edge Switch 2: Step 1 – VLAN 95 and add IP address/mask/default gateway

```
Edge-2(config)#vlan create 95 name mgmt type port
Edge-2(config)#vlan mgmt 95
Edge-2(config)#ip address 20.0.95.12 netmask 255.0.0.0 default-gateway 20.0.95.1
Edge-2(config)#vlan control automatic
Edge-2(config)#vlan port 23,24 tagging tagall
Edge-2(config)#vlan member add 95 23,24
Edge-2(config)#vlan members remove 1 23,24
```

5.2.2.2 Create User Traffic VLAN

Edge Switch 1: Step 1 – VLAN 60

```
Edge-1(config)#vlan create 60 name User-60 type port
Edge-1(config)#vlan members 60 1-12,47,48
```

Edge Switch 2: Step 1 – VLAN 61

```
Edge-2(config)#vlan create 61 name User-61 type port
Edge-2(config)#vlan member add 61 1-12,23,24
```

5.2.2.3 Create MLT

Edge Switch 1: Step 1 – Create MLT

```
Edge-1(config)#mlt 1 enable member 47,48 learning disable
Edge-1(config)#mlt 1 loadbalance advance
```

Edge Switch 2: Step 1 – Create MLT

```
Edge-2(config)#mlt 1 enable member 23,24 learning disable
Edge-2(config)#mlt 1 loadbalance advance
```

5.2.2.4 VLACP

Edge Switch 1: Step 1 – Enable VLACP

```
Edge-1(config)#vlacp macaddress 180.c200.f
Edge-1(config)#vlacp enable
Edge-1(config)#interface fastEthernet 23,24
Edge-1(config-if)#vlacp timeout short
Edge-1(config-if)#vlacp timeout-scale 5
Edge-1(config-if)#vlacp enable
Edge-1(config-if)#exit
```

Edge Switch 2: Step 1 – Enable VLACP

```
Edge-2(config)#vlacp macaddress 180.c200.f
Edge-2(config)#vlacp enable
Edge-2(config)#interface fastEthernet 23,24
Edge-2(config-if)#vlacp timeout short
Edge-2(config-if)#vlacp timeout-scale 5
Edge-2(config-if)#vlacp enable
Edge-2(config-if)#exit
```

5.2.2.5 Enable Spanning Tree FastStart and BPDU filtering on all access ports

Edge Switch 1: Step 1 – Enable STP FastStart and BPDU Filtering

```
Edge-1(config)#interface fastEthernet 1-12
Edge-1(config-if)#spanning-tree learning fast
Edge-1(config-if)#spanning-tree bpdu-filtering timeout 0
Edge-1(config-if)#spanning-tree bpdu-filtering enable
Edge-1(config-if)#exit
```

Edge Switch 2: Step 1 – Enable STP FastStart and BPDU Filtering

```
Edge-2(config)#interface fastEthernet 1-12
Edge-2(config-if)#spanning-tree learning fast
Edge-2(config-if)#spanning-tree bpdu-filtering timeout 0
Edge-2(config-if)#spanning-tree bpdu-filtering enable
Edge-2(config-if)#exit
```

5.2.2.6 Discard Untagged Frames

Edge Switch 1: Step 1 – Enable Discard Untagged Frames

```
Edge-1(config)#vlan ports 23,24 filter-untagged-frame enable
```

Edge Switch 2: Step 1 – Enable Discard Untagged Frames

```
Edge-2(config)#vlan ports 23,24 filter-untagged-frame enable
```



Please note that with the ERS 5510 only, you cannot enable filter untagged frames when using VLACP. This does not apply to the ERS 5520 or ERS 5530.

5.2.2.7 Enable IGMP Snoop/Proxy

Edge Switch 1: Step 1 – Enable IGMP Snoop/Proxy

```
Edge-1(config)#vlan igmp 60 snooping enable
Edge-1(config)#vlan igmp 60 proxy enable
```

Edge Switch 2: Step 1 – Enable IGMP Snoop/Proxy

```
Edge-2(config)#vlan igmp 61 snooping enable
Edge-2(config)#vlan igmp 61 proxy enable
```

5.2.3 Verify Operations

5.2.3.1 IGMP

Step 1 – SMLT Cluster: Verifying IGMP Queriers

ACLI

show ip igmp interface

Results:

9000-1:

Igmp Interface										
	QUERY		OPER			QUERY	WRONG		LASTMEM	
IF	INTVL	STATUS	VERS.	VERS	QUERIER	MAXRSPT	QUERY	JOINS	ROBUST	QUERY
V60	125	active	2	2	20.0.60.1	100	0	0	2	10
V61	125	active	2	2	20.0.61.1	100	0	30	2	10
V95	125	inact	2	2	0.0.0.0	100	0	0	2	10
V4000	125	active	2	2	192.168.255.1	100	0	0	2	10

9000-2:

Igmp Interface										
	QUERY			OPER			QUERY	WRONG		LASTMEM
IF	INTVL	STATUS	VERS.	VERS	QUERIER	MAXRSPT	QUERY	JOINS	ROBUST	QUERY
V60	125	active	2	2	20.0.60.1	100	0	0	2	10
V61	125	active	2	2	20.0.61.1	100	0	30	2	10
V95	125	inact	2	2	0.0.0.0	100	0	0	2	10
V4000	125	active	2	2	192.168.255.1	100	0	0	2	10

Step 2 – SMLT Cluster: Verifying IGMP Groups

ACLI

show ip igmp group

Results: from 9000-2

9000-2:

```
=====
```

Igmp Group				
=====				
GRPADDR	INPORT	MEMBER	EXPIRATION	TYPE

239.0.0.1	V61-11/1	20.0.61.144	177	Dynamic
239.0.0.2	V61-11/1	20.0.61.144	176	Dynamic
239.0.0.3	V61-11/1	20.0.61.144	177	Dynamic
239.0.0.4	V61-11/1	20.0.61.144	179	Dynamic
239.0.0.5	V61-11/1	20.0.61.144	180	Dynamic
239.255.255.250	V61-11/1	20.0.61.144	176	Dynamic

6 out of 6 group Receivers displayed

Step 2 – SMLT Cluster: Verifying IGMP Senders

ACLI

show ip igmp sender

Results: from 9000-2

9000-2:

=====				
Igmp Sender				
=====				
		PORT/		
GRPADDR	IFINDEX	MEMBER	MLT	STATE

239.0.0.1	Vlan 60	20.0.60.105	MLT-2	NOTFILTERED
239.0.0.2	Vlan 60	20.0.60.105	MLT-2	NOTFILTERED
239.0.0.3	Vlan 60	20.0.60.105	MLT-2	NOTFILTERED
239.0.0.4	Vlan 60	20.0.60.105	MLT-2	NOTFILTERED
239.0.0.5	Vlan 60	20.0.60.105	MLT-2	NOTFILTERED

5.2.3.2 PIM

Step 1 – SMLT Cluster: Static RP

ACLI

```
show ip pim static-rp
```

Results: from 9000-2

9000-2:

```
=====
                                Pim Static RP Table
=====
GRPADDR          GRPMASK          RPADDR          STATUS
-----
239.0.0.0        255.0.0.0        20.0.0.90       valid
```

Step 2 – SMLT Cluster: Active RP

ACLI

```
show ip pim active-rp
```

Results: from 9000-2

9000-2:

```
=====
                                Pim Grp->RP Active RP Table
=====
GRPADDR          RP-ADDR          RP-PRIORITY
-----
239.0.0.1        20.0.0.90        0
239.0.0.2        20.0.0.90        0
239.0.0.3        20.0.0.90        0
239.0.0.4        20.0.0.90        0
239.0.0.5        20.0.0.90        0
239.255.255.250  20.0.0.90        0
```

Step 3 – SMLT Cluster: PIM Interface

ACLI

show ip pim interface

Results:

9000-1:

Pim Interface								
IF TYPE	ADDR	MASK	MODE	DR	HLINT	JPINT	CBSPR	OPSTAT INTF
Clip1 passive	20.0.0.91	255.255.255.255	sparse	20.0.0.91	30	60	-1 (disabled)	up
Clip2 passive	20.0.0.90	255.255.255.255	sparse	20.0.0.90	30	60	-1 (disabled)	up
Vlan60 active	20.0.60.1	255.255.255.0	sparse	20.0.60.2	30	60	-1 (disabled)	up
Vlan61 active	20.0.61.1	255.255.255.0	sparse	20.0.61.2	30	60	-1 (disabled)	up
Vlan95 active	20.0.95.1	255.255.255.0	sparse	0.0.0.0	30	60	-1 (disabled)	down
Vlan4000 active	192.168.255.1	255.255.255.252	sparse	192.168.255.2	30	60	-1 (disabled)	up

9000-2:

Pim Interface								
IF TYPE	ADDR	MASK	MODE	DR	HLINT	JPINT	CBSPR	OPSTAT INTF
Clip1 passive	20.0.0.92	255.255.255.255	sparse	20.0.0.92	30	60	-1 (disabled)	up
Clip2 passive	20.0.0.90	255.255.255.255	sparse	20.0.0.90	30	60	-1 (disabled)	up
Vlan60 active	20.0.60.2	255.255.255.0	sparse	20.0.60.2	30	60	-1 (disabled)	up
Vlan61 active	20.0.61.2	255.255.255.0	sparse	20.0.61.2	30	60	-1 (disabled)	up
Vlan95 active	20.0.95.2	255.255.255.0	sparse	0.0.0.0	30	60	-1 (disabled)	down
Vlan4000 active	192.168.255.2	255.255.255.252	sparse	192.168.255.2	30	60	-1 (disabled)	up

5.3 PIM-SM SMLT Triangle Topology Design with L3 Edge

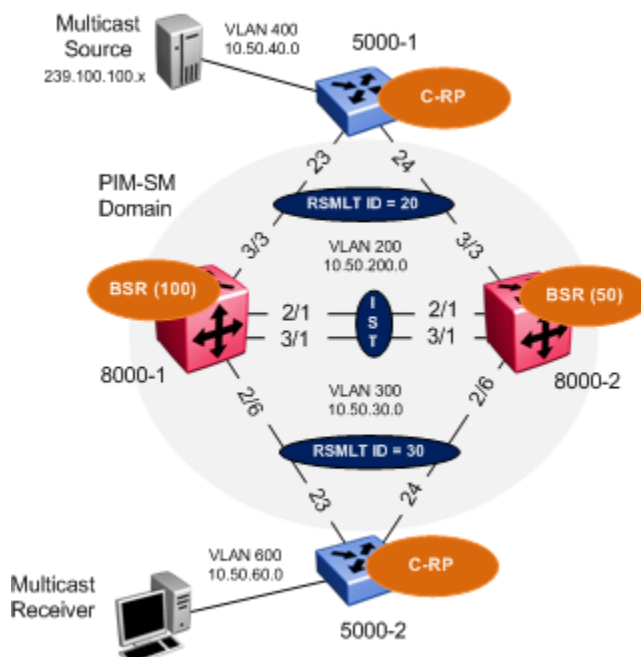


Figure 14: PIM-SM SMLT ERS5000 Distribution Edge

In this example the following is configured on the ERS8000 as per Figure 14:

- IST
 - VLAN 2 is configured and associated to MLT# 1.
 - Tagging is enabled on ports 2/1, 3/1
- VLACP and SLPP settings are configured as defined in the Switch Clustering using SMLT TCG
- SMLT ID 20: VLAN 200 (port 3/3) to 5000-1
- SMLT ID 30: VLAN 300 (port 2/6) to 5000-2
- RSMLT enable on VLAN 200 and 300
- CLIP/Loopback address is configured
- Dynamic PIM-SM is enabled
- PIM-SM active mode is enabled on VLAN 200 & 300
- PIM-SM active mode is enabled on the IST VLAN 2



In order to achieve sub second failovers/recoveries with PIM-SM the IST VLAN all VLANs associated with a SMLT should be configured in PIM active mode. All other VLANs not associated with either a SMLT or PIM adjacencies should be configured in passive mode.

- Candidate BSR is defined on each ERS8000 for redundant BSR.



It is recommended that the BSR is configured on a CLIP/Loopback address. This will prevent a BSR failure if a VLAN interface goes down.

Recommended that the OSPF router ID is configured the same as the CLIP/Loopback address for management simplicity.

- RSMILT is enabled on VLAN 200 and 300
- OSPF Area 0.0.0.0
- OSPF broadcast mode is enabled on VLAN 200 & 300. OSPF passive mode is enabled on CLIP/Loopback addresses
- VLANs 200, 400 and VLANs 300, 600 are configured on 5000-1 and 5000-2 respectively
- MLT is configured on each ERS5000 to the ERS8000 core
- Dynamic PIM-SM is enabled
- Candidate RPs are defined on each ERS5000 for redundant RPs.



It is recommended that the RP is configured on a CLIP/Loopback address. This will prevent a RP failure if a VLAN interface goes down.



The location of the RPs should be as close as possible to the source of the multicast streams. In this example the Source of the IPMC is a server located off the 5000-2. BSRs should be in a central location in the network to optimize flow of bootstrap messages.

- PIM-SM passive mode is configured on VLANs 400 and 600 on 5000-1 and 5000-2 respectively
- PIM-SM active mode is configured on VLANs 200 and 300 on 5000-1 and 5000-2 respectively.
- OSPF passive is configured on VLANs 400 and 600 on 5000-1 and 5000-2 respectively

5.3.1 8000 SMLT Cluster

5.3.1.1 IST Configuration

For this configuration example, 8000-1 is configured using the ACLI command interface while 8000-2 is configured using the CLI command interface

8000-1: Step 1 - Create IST using VLAN 2 and MLT 1

```
8000-1:5(config)#vlan create 2 name IST type port 1
8000-1:5(config-if)#ip address 10.50.2.1 255.255.255.252
8000-1:5(config-if)#exit
8000-1:5(config)#mlt 1
8000-1:5(config)#mlt 1 name IST
8000-1:5(config)#mlt 1 member 2/1,3/1
8000-1:5(config)#vlan mlt 2 1
8000-1:5(config)#mlt 1 encapsulation dot1q
8000-1:5(config)#interface mlt 1
8000-1:5(config-mlt)#ist peer-ip 10.50.2.2 vlan 2
8000-1:5(config-mlt)#ist enable
8000-1:5(config-mlt)#exit
```

8000-2: Step 1 - Create IST using VLAN 2 and MLT 1

```
8000-2:5# config vlan 2 create byport 1 name "IST"
8000-2:5# config vlan 2 ip create 10.50.2.2/255.255.255.252
8000-2:5# config mlt 1 create
8000-2:5# config mlt 1 add ports 2/1,2/30
8000-2:5# config vlan 2 add-mlt 1
8000-2:5# config mlt 1 name "IST"
8000-2:5# config mlt 1 perform-tagging enable
8000-2:5# config mlt 1 ist create ip 10.50.2.1 vlan-id 2
8000-2:5# config mlt 1 ist enable
```

5.3.1.2 SMLT Configuration

8000-1: Step 1: Create VLAN 200 using MLT/SMLT ID 20

```
8000-1:5(config)#vlan create 200 name Vlan-200 type port 1
8000-1:5(config)#interface vlan 200
8000-1:5(config-if)#ip address 10.50.200.1 255.255.255.0
8000-1:5(config-if)#exit
8000-1:5(config)#mlt 20
8000-1:5(config)#vlan mlt 200 20
8000-1:5(config)#mlt 20 name SMLT-20
8000-1:5(config)#mlt 20 encapsulation dot1q
8000-1:5(config)#mlt 20 member 3/3
8000-1:5(config)#interface mlt 20
8000-1:5(config-mlt)#smlt 20
8000-1:5(config-mlt)#exit
8000-1:5(config)#vlan mlt 200 1
```

8000-2: Step 1: Create VLAN 200 using MLT/SMLT ID 20

```
8000-2:5# config vlan 200 create byport 1 name "Vlan-200"
8000-2:5# config vlan 200 ip create 10.50.200.3/255.255.255.0
8000-2:5# config mlt 20 create
8000-2:5# config mlt 20 add ports 2/3
8000-2:5# config vlan 200 add-mlt 20
8000-2:5# config mlt 20 name "SMLT-20"
8000-2:5# config mlt 20 perform-tagging enable
8000-2:5# config mlt 20 smlt create smlt-id 20
8000-2:5# config mlt 1 add vlan 200
```

8000-1: Step 2: Create VLAN 300 using MLT/SMLT ID 30

```
8000-1:5(config)#vlan create 300 name Closet_Sw2 type port 1
8000-1:5(config)#interface vlan 300
8000-1:5(config-if)#ip address 10.50.30.1 255.255.255.0
8000-1:5(config-if)#exit
8000-1:5(config)#mlt 30
8000-1:5(config)#vlan mlt 300 30
8000-1:5(config)#mlt 30 name SMLT-30
8000-1:5(config)#mlt 30 encapsulation dot1q
8000-1:5(config)#mlt 30 member 2/6
```

```
8000-1:5(config)#interface mlt 30
8000-1:5(config-mlt)#smlt 30
8000-1:5(config-mlt)#exit
8000-1:5(config)#vlan mlt 300 1
```

8000-2: Step 2: Create VLAN 300 using MLT/SMLT ID 30

```
8000-2:5# config vlan 300 create byport 1 name Closet_Sw2
8000-2:5# config vlan 300 ip create 10.50.30.2/24
8000-2:5# config mlt 30 create
8000-2:5# config vlan 300 add-mlt 30
8000-2:5# config mlt 30 name SMLT-30
8000-2:5# config mlt 30 perform-tagging enable
8000-2:5# config mlt 30 add ports 2/6
8000-2:5# config mlt 30 smlt create smlt-id 30
8000-2:5# config mlt 1 add vlan 300
```

5.3.1.3 Enable RSMLT

8000-1: Step 1: RSMLT Configuration

```
8000-1:5(config)#interface vlan 200
8000-1:5(config-if)#ip rsmlt
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 300
8000-1:5(config-if)#ip rsmlt
8000-1:5(config-if)#exit
```

8000-2: Step 1: RSMLT Configuration

```
8000-2:5# config vlan 200 ip rsmlt enable
8000-2:5# config vlan 300 ip rsmlt enable
```

5.3.1.4 VLACP

As the access switches are an Avaya stackable switch, we will enable VLACP and use the short timeout option with the recommended fast-periodic-time of 500ms and time-out scale of 5. In addition, we will use the recommended VLACP reserved MAC address.

8000-1: Step 1 – Enable VLACP at port level and globally

```
8000-1:5(config)#vlacp enable
8000-1:5(config)#interface gigabitEthernet 2/6,3/3
8000-1:5(config-if)#vlacp fast-periodic-time 500
8000-1:5(config-if)#vlacp timeout short
8000-1:5(config-if)#vlacp timeout-scale 5
8000-1:5(config-if)#vlacp funcmac-addr 01:80:c2:00:00:0f
8000-1:5(config-if)#vlacp enable
8000-1:5(config-if)#exit
```

8000-2: Step 1 – Enable VLACP at port level and globally

```
8000-2:5# config vlacp enable
8000-2:5# config ethernet 2/6,3/3 vlacp fast-periodic-time 500
8000-2:5# config ethernet 2/6,3/3 vlacp timeout short
8000-2:5# config ethernet 2/6,3/3 vlacp timeout-scale 5
8000-2:5# config ethernet 2/6,3/3 vlacp macaddress 01:80:c2:00:00:0f
8000-2:5# config ethernet 2/6,3/3 vlacp enable
```



Do not enable VLACP on a port level until the VLACP MAC address has been changed.

5.3.1.5 Discard Untagged Frames

8000-1: Step 1 – Enable discard untagged frames

```
8000-1:5(config)#interface gigabitEthernet 2/1,2/6,3/1,3/3
8000-1:5(config-if)#untagged-frames-discard
8000-1:5(config-if)#exit
```

8000-2: Step 1 – Enable discard untagged frames

```
8000-2:5# config ethernet 2/1,2/6,3/1,3/3 untagged-frames-discard enable
```


5.3.1.6 SLPP

8000-1: Step 1 – Enable SLPP on VLANs 200 and 300 where 8000-1 is the primary switch

```
8000-10:5(config)#slpp vid 200,300
8000-10:5(config)#slpp enable
8000-10:5(config)#interface gig
8000-10:5(config)#interface gigabitEthernet 2/6,3/3
8000-10:5(config-if)#slpp packet-rx-threshold 5
8000-10:5(config-if)#slpp packet-rx
8000-10:5(config-if)#exit
```

8000-2: Step 1 – Enable SLPP on VLANs 200 and 300 where 8000-2 is the secondary switch

```
8000-2:5# config slpp add 200,300
8000-2:5# config slpp operation enable
8000-2:5# config ethernet 2/6,3/3 slpp packet-rx enable
8000-2:5# config ethernet 2/6,3/3 slpp packet-rx-threshold 50
```

5.3.1.7 Circuitless/Loopback IP address configuration

8000-1: Step 1 – Create Loopback address

```
8000-1:5(config)#interface loopback 1
8000-1:5(config-if)#ip address 10.50.1.1/32
8000-1:5(config-if)#ip ospf
8000-1:5(config-if)#ip pim
8000-1:5(config-if)#exit
```

8000-2: Step 1 – Create CLIP address

```
8000-2:5# config ip circuitless-ip-int 1 create 10.50.1.2/32
8000-2:5# config ip circuitless-ip-int 1 ospf enable
8000-2:5# config ip circuitless-ip-int 1 pim enable
```

5.3.1.8 OSPF Configuration

8000-1: Step 1 – OSPF global configuration

```
8000-1:5(config)#router ospf enable
8000-1:5(config)#router ospf
8000-1:5(config-ospf)#router-id 10.50.1.1
8000-1:5(config-ospf)#exit
```

8000-2: Step 1 – OSPF global configuration

```
8000-2:5# config ip ospf admin-state enable
8000-2:5# config ip ospf router-id 10.50.1.2
8000-2:5# config ip ospf enable
```

8000-1: Step 2 – OSPF interface configuration

```
8000-1:5(config)#interface vlan 200
8000-1:5(config-if)#ip ospf enable
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 300
8000-1:5(config-if)#ip ospf enable
8000-1:5(config-if)#exit
```

8000-2: Step 2 – OSPF interface configuration

```
8000-2:5# config vlan 200 ip ospf enable
8000-2:5# config vlan 300 ip ospf enable
```

5.3.1.9 PIM Configuration

8000-1: Step 1 – PIM global configuration

```
8000-1:5(config)#ip pim enable
8000-1:5(config)#interface loopback 1
8000-1:5(config-if)#ip pim bsr-candidate preference 100
8000-1:5(config-if)#exit
```

8000-2: Step 1 – PIM global configuration

```
8000-2:5# config ip pim enable
8000-2:5# config ip pim candbsr interface 10.50.1.2 enable preference 50
```

8000-1: Step 2 – PIM interface configuration

```
8000-1:5(config)#interface vlan 2
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 200
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 300
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#exit
```

8000-2: Step 2 – PIM interface configuration

```
8000-2:5# config vlan 2 ip pim enable
8000-2:5# config vlan 200 ip pim enable
8000-2:5# config vlan 300 ip pim enable
```

5.3.2 ERS5000 Configuration

5.3.2.1 Create VLANs

5000-1: Step 1: Create VLAN 200 and 400

```
5000-1(config)#vlan create 200 name type port
5000-1(config)#vlan create 400 name type port
5000-1(config)#vlan configcontrol automatic
5000-1(config)#vlan ports 23,24 tagging tagall
5000-1(config)#vlan members add 200 23,24
5000-1(config)#vlan members add 400 3-11
5000-1(config)#vlan members remove 1 23,24
5000-1(config)#interface vlan 200
5000-1(config-if)#ip address 10.50.200.3 255.255.255.0
5000-1(config-if)#exit
5000-1(config)#interface vlan 400
5000-1(config-if)#ip address 10.50.40.1 255.255.255.0
5000-1(config-if)#exit
```

5000-2: Step 1: Create VLAN 300 and 600

```
5000-2(config)#vlan create 300 type port
5000-2(config)#vlan create 600 type port
5000-2(config)#vlan configcontrol automatic
5000-2(config)#vlan ports 23,24 tagging tagall
5000-2(config)#vlan members add 300 23,24
5000-2(config)#vlan members add 600 3-11
5000-2(config)#vlan members remove 1 23,24
5000-2(config)#interface vlan 300
5000-2(config-if)#ip address 10.40.30.3 255.255.255.0
5000-2(config-if)#exit
5000-2(config)#interface vlan 600
5000-2(config-if)#ip address 10.50.60.1 255.255.255.0
5000-2(config-if)#exit
```

5.3.2.2 Create MLT to 8000 SMLT Cluster

5000-1: Step 1: Create MLT using MLT 1 with load balance of advance (IP)

```
5000-1(config)#mlt 1 enable member 23,24 learning disable
5000-1(config)#mlt 1 loadbalance advance
```

5000-2: Step 1: Create MLT using MLT 1 with load balance of advance (IP)

```
5000-2(config)#mlt 1 enable member 23,24 learning disable
5000-2(config)#mlt 1 loadbalance advance
```

5.3.2.3 VLACP

5000- 1: Step 1 – Enable VLACP

```
5000-1(config)#vlacp macaddress 180.c200.f
5000-1(config)#vlacp enable
5000-1(config)#interface fastEthernet 23,24
5000-1(config-if)#vlacp timeout short
5000-1(config-if)#vlacp timeout-scale 5
5000-1(config-if)#vlacp enable
5000-1(config-if)#exit
```

5000-2: Step 1 – Enable VLACP

```
5000-2(config)#vlacp macaddress 180.c200.f
5000-2(config)#vlacp enable
5000-2(config)#interface fastEthernet 23,24
5000-2(config-if)#vlacp timeout short
5000-2(config-if)#vlacp timeout-scale 5
5000-2(config-if)#vlacp enable
5000-2(config-if)#exit
```

5.3.2.4 Enable Spanning Tree FastStart and BPDU filtering on all access ports

5000-1: Step 1 – Enable STP FastStart and BPDU Filtering on all access ports

```
5000-1(config)#interface fastEthernet 3-11
5000-1(config-if)#spanning-tree learning fast
5000-1(config-if)#spanning-tree bpdu-filtering timeout 0
5000-1(config-if)#spanning-tree bpdu-filtering enable
5000-1(config-if)#exit
```

5000-2: Step 1 – Enable STP FastStart and BPDU Filtering on all access ports

```
5000-2(config)#interface fastEthernet 3-11
5000-2(config-if)#spanning-tree learning fast
5000-2(config-if)#spanning-tree bpdu-filtering timeout 0
5000-2(config-if)#spanning-tree bpdu-filtering enable
5000-2(config-if)#exit
```

5.3.2.5 OSPF Configuration

5000-1: Step 1 – Enable IP Routing and enable OSPF globally

```
5000-1(config)#ip routing
5000-1(config)#router ospf enable
```

5000-2: Step 1 – Enable IP Routing and enable OSPF globally

```
5000-2(config)#ip routing
5000-2(config)#router ospf enable
```

5000-1: Step 2 – OSPF interface configuration

```
5000-1(config)#interface vlan 200
5000-1(config-if)#ip ospf enable
5000-1(config-if)#exit
5000-1(config)#interface vlan 400
5000-1(config-if)#ip ospf network passive
5000-1(config-if)#ip ospf enable
5000-1(config-if)#exit
```

5000-2: Step 2 – OSPF interface configuration

```
5000-2(config)#interface vlan 300
5000-2(config-if)#ip ospf enable
5000-2(config-if)#exit
5000-2(config)#interface vlan 600
5000-2(config-if)#ip ospf network passive
5000-2(config-if)#ip ospf enable
5000-2(config-if)#exit
```

5.3.2.6 PIM Configuration

5000-1: Step 1 – PIM global configuration

```
5000-1:5(config)#ip pim enable
```

5000-2: Step 1 – PIM global configuration

```
5000-2:5(config)#ip pim enable
```

5000-1: Step 2 – PIM interface configuration

```
5000-1(config)#interface vlan 200
5000-1(config-if)#ip pim enable
5000-1(config-if)#exit
5000-1(config)#interface vlan 400
5000-1(config-if)#ip pim interface-type passive
5000-1(config-if)#ip pim enable
5000-1(config-if)#exit
```

5000-2: Step 2 – PIM interface configuration

```
5000-2(config)#interface vlan 300
5000-2(config-if)#ip pim enable
5000-2(config-if)#exit
5000-2(config)#interface vlan 600
5000-2(config-if)#ip pim interface-type passive
5000-2(config-if)#ip pim enable
5000-2(config-if)#exit
```

5000-1: Step 3 – PIM PIM Candidate RP. For this example, we will use VLAN 400 IP address

```
5000-1:5(config)#ip pim rp-candidate group 239.0.0.0 255.0.0.0 rp 10.50.40.1
```

5000-2: Step 1 – PIM PIM Candidate RP. For this example, we will use VLAN 600 IP address

```
5000-2:5(config)#ip pim rp-candidate group 239.0.0.0 255.0.0.0 rp 10.50.60.1
```


5.3.3 Verify Operation

5.3.3.1 IGMP

Step 1 – SMLT Cluster: Verifying IGMP Queriers. For VLAN 200 and 300, the lowest IP (8000-1) should be the querier for VLAN 200 and 300

CLI/ACLI

show ip igmp interface

Results:

8000-1:

=====										
IGMP Interface - GlobalRouter										
=====										
IF	QUERY INTVL	STATUS	VERS.	OPER VERS	QUERIER	QUERY MAXRSPT	WRONG QUERY	JOINS	ROBUST	LASTMEM QUERY

V0	125	inact	2	2	0.0.0.0	100	0	0	2	10
V2	125	active	2	2	10.50.2.1	100	0	0	2	10
V200	125	active	2	2	10.50.200.1	100	0	0	2	10
V300	125	active	2	2	10.50.30.1	100	0	0	2	10

8000-2:

=====										
IGMP Interface - GlobalRouter										
=====										
IF	QUERY INTVL	STATUS	VERS.	OPER VERS	QUERIER	QUERY MAXRSPT	WRONG QUERY	JOINS	ROBUST	LASTMEM QUERY

V0	125	inact	2	2	0.0.0.0	100	0	0	2	10
V2	125	active	2	2	10.50.2.1	100	0	0	2	10
V200	125	active	2	2	10.50.200.1	100	0	0	2	10
V300	125	active	2	2	10.50.30.1	100	0	0	2	10

Step 1 – ERS5000: Verifying IGMP Queriers

ACLI

```
show ip igmp interface
```

Results:

5000-1:

Query	Oper	Query	Wrong	LastMbr	Send
VLAN Intvl Vers Vers Querier	MaxRspT	Query	Joins	Robust	Query
-----	-----	-----	-----	-----	-----
200 125 2 2 10.50.200.1	100	0	0	2	10
400 125 2 2 10.50.40.1	100	0	5	2	10

5000-2:

Query	Oper	Query	Wrong	LastMbr	Send
VLAN Intvl Vers Vers Querier	MaxRspT	Query	Joins	Robust	Query
-----	-----	-----	-----	-----	-----
300 125 2 2 10.50.30.1	100	0	0	2	10
600 125 2 2 10.50.60.1	100	0	110	2	10



On the ERS 8000, enabling any multicast routing protocol such as PIM-SM, PIM-SSM or DVMRP on an IP interface will enable the IGMP querier and snoop function. You cannot disable or enable IGMP snoop while PIM-SM is enabled on the same interface.



Try and localize the IGMP queriers to the first and last hop routers in the PIM domain. This will prevent excessive IGMP queries and MHR from spanning the core of the network.

Step 2 – ERS8000: Verifying IGMP Groups – should not be any via both 8000-1 & 8000-2

CLI/ACLI

```
show ip igmp group
```

Results:

```
=====
                        Igmp Group
=====
GRPADDR          INPORT          MEMBER          EXPIRATION TYPE
-----
Total number of groups 0
Total number of unique groups 0
```

Step 2 – ERS5000 Verifying IGMP Groups – assuming receivers via 5000-2 on ports 7 and 9

CLI

```
show ip igmp group
```

Results:

5000-1:

Group Address	VLAN	Member Address	Expiration	Type	In Port
239.255.255.250	400	10.50.40.10	221	Dynamic	5

5000-2:

Group Address	VLAN	Member Address	Expiration	Type	In Port
239.100.100.100	600	10.50.60.10	224	Dynamic	9
239.100.100.100	600	10.50.60.20	232	Dynamic	7
239.100.100.101	600	10.50.60.10	233	Dynamic	9
239.100.100.101	600	10.50.60.20	232	Dynamic	7
239.100.100.102	600	10.50.60.10	225	Dynamic	9
239.100.100.102	600	10.50.60.20	225	Dynamic	7
239.255.255.250	600	10.50.60.20	229	Dynamic	7

Step 3 – ERS8000: Verifying IGMP sender

CLI/ACLI

```
show ip igmp sender
```

Results:

8000-1:

=====				
IGMP Sender - GlobalRouter				
=====				
		PORT/		
GRPADDR	IFINDEX	MEMBER	MLT	STATE

239.100.100.100	Vlan 200	10.50.40.10	MLT-20	NOTFILTERED
239.100.100.101	Vlan 200	10.50.40.10	MLT-20	NOTFILTERED
239.100.100.102	Vlan 200	10.50.40.10	MLT-20	NOTFILTERED

8000-2:

=====				
IGMP Sender - GlobalRouter				
=====				
		PORT/		
GRPADDR	IFINDEX	MEMBER	MLT	STATE

239.100.100.100	Vlan 200	10.50.40.10	MLT-20	NOTFILTERED
239.100.100.101	Vlan 200	10.50.40.10	MLT-20	NOTFILTERED
239.100.100.102	Vlan 200	10.50.40.10	MLT-20	NOTFILTERED



Only the IGMP groups are displayed on 5000-2. No IGMP groups are display on the ERS 8000 because there are no MHR being generated on VLANs 200 and 300. The multicast address 239.255.255.250 shown in the IGMP table for 5000-1 & 5000-2 is being generated by Microsoft OS. The multicast group 239.255.255.250 is used for SSDP Discovery service used request for UPnP services.

5.3.3.2 PIM

Step 1: ERS8000 - Verify PIM neighbors

CLI/ACLI

show ip pim neighbor

Results:

8000-1:

```
=====
                                PIM Neighbor - GlobalRouter
=====
INTERFACE ADDRESS          UPTIME                      EXPIRE
-----
Vlan2      10.50.2.2              1 day(s), 02:22:25         0 day(s), 00:01:24
Vlan300    10.50.30.2              0 day(s), 01:09:45         0 day(s), 00:01:30
Vlan300    10.50.30.3              0 day(s), 01:14:55         0 day(s), 00:01:29
Vlan200    10.50.200.2             0 day(s), 23:15:28         0 day(s), 00:01:37
Vlan200    10.50.200.3             0 day(s), 00:30:08         0 day(s), 00:01:37

Total PIM Neighbors = 5
```

8000-2:

```
=====
                                PIM Neighbor - GlobalRouter
=====
INTERFACE ADDRESS          UPTIME                      EXPIRE
-----
Vlan2      10.50.2.1              1 day(s), 02:22:21         0 day(s), 00:01:20
Vlan300    10.50.30.1              0 day(s), 01:09:45         0 day(s), 00:01:30
Vlan300    10.50.30.3              0 day(s), 01:09:45         0 day(s), 00:01:29
Vlan200    10.50.200.1             0 day(s), 23:15:24         0 day(s), 00:01:38
Vlan200    10.50.200.3             0 day(s), 00:30:08         0 day(s), 00:01:37

Total PIM Neighbors = 5
```

Step 1: ERS5000 - Verify PIM neighbors

ACLI

show ip pim neighbor

Results:

5000-1:

Address	Vlan	Uptime	Expiry Time
-----	-----	-----	-----
10.50.200.1	200	0d 00:29:01	0d 00:01:15
10.50.200.2	200	0d 00:29:01	0d 00:01:15

Total PIM Neighbors: 2

5000-2:

Address	Vlan	Uptime	Expiry Time
-----	-----	-----	-----
10.50.30.1	300	0d 01:16:19	0d 00:01:37
10.50.30.2	300	0d 01:08:39	0d 00:01:38

Total PIM Neighbors: 2

Step 2: ERS8000 - Verify that the BSR are identical on 8000-1 and 8000-2 which should be loopback address from 8000-1

CLI/ACLI

show ip pim bsr

Results:

8000-1:

```
=====
                        BootStrap Router Info - GlobalRouter
=====
```

```
Current BSR address: 10.50.1.1
Current BSR priority: 100
Current BSR HashMask: 255.255.255.252
Current BSR Fragment Tag: 1602
Pim Bootstrap Timer : 4
```

8000-2:

```
=====
                        BootStrap Router Info - GlobalRouter
=====
```

```
Current BSR address: 10.50.1.1
Current BSR priority: 100
Current BSR HashMask: 255.255.255.252
Current BSR Fragment Tag: 1602
Pim Bootstrap Timer : 74
```

Step 2: ERS5000 - Verify that the BSR are identical on 5000-1 and 5000-2 which should be loopback address from 8000-1

ACLI

show ip pim bsr

Results:

5000-1:

Current BSR Address: 10.50.1.1
 Current BSR Priority: 100
 Current BSR Hash Mask: 255.255.255.252
 Current BSR Fragment Tag: 1606
 Current BSR Boot Strap Timer: 120

5000-2:

Current BSR Address: 10.50.1.1
 Current BSR Priority: 100
 Current BSR Hash Mask: 255.255.255.252
 Current BSR Fragment Tag: 1606
 Current BSR Boot Strap Timer: 119

Step 3: ERS8000 - Verify that the RP sets are identical on 8000-1 and 8000-2 where in this example, is the VLAN 400 IP address from 5000-1 and VLAN 600 IP address from 5000-2 – 10.50.40.1 and 10.50.60.1 respectively

CLI

show ip pim rp-set

ACLI

show ip pim rp-hash

Results:

8000-1:

```
=====
                        PIM RPSet - GlobalRouter
=====
GRPADDRESS      GRPMASK      ADDRESS      HOLDTIME    EXPTIME
-----
239.0.0.0       255.0.0.0       10.50.40.1   150         104
239.0.0.0       255.0.0.0       10.50.60.1   150         131
```

8000-2:

```
=====
                        PIM RPSet - GlobalRouter
=====
GRPADDRESS      GRPMASK      ADDRESS      HOLDTIME    EXPTIME
-----
239.0.0.0       255.0.0.0       10.50.40.1   0           0
239.0.0.0       255.0.0.0       10.50.60.1   0           0
```

Step 3: ERS5000 - Verify that the RP Sets are identical on 5000-1 and 5000-2 where in this example, is the VLAN 400 IP address from 5000-1 and VLAN 600 IP address from 5000-2 – 10.50.40.1 and 10.50.60.1 respectively

CLI

```
show ip pim rp-hash
```

Results:

5000-1:

Group Address	Group Mask	Address	Hold Time	Expiry Time
239.0.0.0	255.0.0.0	10.50.40.1	0	0d 00:00:00
239.0.0.0	255.0.0.0	10.50.60.1	0	0d 00:00:00

Total RP sets: 2

5000-2:

Group Address	Group Mask	Address	Hold Time	Expiry Time
239.0.0.0	255.0.0.0	10.50.40.1	0	0d 00:00:00
239.0.0.0	255.0.0.0	10.50.60.1	0	0d 00:00:00

Total RP sets: 2

Step 4: ERS8000 - Verify that the Active RP are identical on 8000-1 and 8000-2

CLI/ACLI

show ip pim active-rp

Results:

8000-1:

```
=====
PIM Grp->RP Active RP Table - GlobalRouter
=====
GRPADDR          RP-ADDR          RP-PRIORITY
-----
239.100.100.100   10.50.60.1       0
239.100.100.101   10.50.60.1       0
239.100.100.102   10.50.60.1       0
239.255.255.250   10.50.60.1       0
```

8000-2:

```
=====
PIM Grp->RP Active RP Table - GlobalRouter
=====
GRPADDR          RP-ADDR          RP-PRIORITY
-----
239.100.100.100   10.50.60.1       0
239.100.100.101   10.50.60.1       0
239.100.100.102   10.50.60.1       0
239.255.255.250   10.50.60.1       0
```

Step 4: ERS5000 - Verify that the Active RP are identical on 5000-1 and 5000-2

ACLI

show ip pim active-rp

Results:

5000-1:

Group Address	Group Mask	Active RP	Priority
-----	-----	-----	-----
239.100.100.100	255.0.0.0	10.50.60.1	0
239.100.100.101	255.0.0.0	10.50.60.1	0
239.100.100.102	255.0.0.0	10.50.60.1	0
239.255.255.250	255.0.0.0	10.50.60.1	0

Total active RP flows: 4

5000-2:

Group Address	Group Mask	Active RP	Priority
-----	-----	-----	-----
239.100.100.100	255.0.0.0	10.50.60.1	0
239.100.100.101	255.0.0.0	10.50.60.1	0
239.100.100.102	255.0.0.0	10.50.60.1	0
239.255.255.250	255.0.0.0	10.50.60.1	0

Total active RP flows: 4



The RP-Set, a collection of candidate RPs, is distributed by the BSR. Each PIM-SM router uses the BSR hash Mask and the RP set to determine the active RP for a given multicast group. The active RP for a given multicast group should be the same for each PIM-SM router within the PIM-SM domain.

5.3.3.3 Verify Multicast Routing Table

Step 1: ERS8000 - Verify multicast routing table on 8000-1 and 8000-2

CLI/ACLI

show ip pim mroute

Results:

8000-1:

```
=====
                        PIM Multicast Route - GlobalRouter
=====
Src: 10.50.40.10   Grp: 239.100.100.100 RP: 10.50.60.1   Upstream: 10.50.200.3
Flags: CACHE SG
Incoming  Port: Vlan200-MLT-20(3/3),
Outgoing Ports: Vlan200-2/1, Vlan300-2/6,
Joined   Ports: Vlan200-2/1, Vlan300-2/6,
Pruned   Ports:
Leaf     Ports:
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
  Entry   JP   RS   Assert
    172   21    0        0
VLAN-Id:    2   200   300
Join-P:     0   171   172
Assert:     0    0    0
-----
-
Src: 10.50.40.10   Grp: 239.100.100.101 RP: 10.50.60.1   Upstream: 10.50.200.3
Flags:
CACHE SG
Incoming  Port: Vlan200-MLT-20(3/3),
Outgoing Ports: Vlan200-2/1, Vlan300-2/6,
Joined   Ports: Vlan200-2/1, Vlan300-2/6,
Pruned   Ports:
```

Leaf	Ports:				
Asserted Ports:					
Prune Pending Ports:					
Assert Winner Ifs:					
Assert Loser Ifs:					
TIMERS:					
Entry	JP	RS	Assert		
172	21	0	0		
VLAN-Id:	2	200	300		
Join-P:	0	171	172		
Assert:	0	0	0		

-					
Src:	10.50.40.10	Grp:	239.100.100.102	RP:	10.50.60.1 Upstream: 10.50.200.3
Flags:	CACHE SG				
Incoming Port:	Vlan200-MLT-20(3/3),				
Outgoing Ports:	Vlan200-2/1, Vlan300-2/6,				
Joined Ports:	Vlan200-2/1, Vlan300-2/6,				
Pruned Ports:					
Leaf	Ports:				
Asserted Ports:					
Prune Pending Ports:					
Assert Winner Ifs:					
Assert Loser Ifs:					
TIMERS:					
Entry	JP	RS	Assert		
171	20	0	0		
VLAN-Id:	2	200	300		
Join-P:	0	170	171		
Assert:	0	0	0		

-					
Src:	0.0.0.0	Grp:	239.255.255.250	RP:	10.50.60.1 Upstream: 10.50.30.3
Flags:	WC RP CACHE				
Incoming Port:	Vlan300-MLT-30(2/6),				
Outgoing Ports:	Vlan200-3/3, Vlan300-2/1,				
Joined Ports:	Vlan200-3/3, Vlan300-2/1,				

```

Pruned   Ports:
Leaf     Ports:
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
  Entry   JP    RS   Assert
      173   23    0      0
VLAN-Id:      2   200   300
Join-P:       0   173   173
Assert:       0    0    0
-----
-
Src: 10.50.40.10   Grp: 239.255.255.250 RP: 10.50.60.1   Upstream: 10.50.200.3
Flags: SPT CACHE SG
Incoming  Port: Vlan200-MLT-20(3/3),
Outgoing Ports: Vlan200-2/1,3/3, Vlan300-2/6,
Joined   Ports: Vlan200-2/1, Vlan200-3/3, Vlan300-2/6,
Pruned   Ports: Vlan300-2/1,
Leaf     Ports:
Asserted Ports:
Prune Pending Ports: Vlan200-3/3,
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
  Entry   JP    RS   Assert
      173   27    0      0
VLAN-Id:      2   200   300
Join-P:       0   177   173
Assert:       0    0    0
-----

Total Num of Entries Displayed 5/5
Flags Legend:
SPT = Shortest path tree, WC=(*,Grp) entry, RP=Rendezvous Point tree, CACHE=Kern

```

el Cache, ASSERTED=Asserted, SG=(Src,Grp) entry, PMBR=(*,*,RP) entry, FWD_TO_RP=Forwarding to RP, FWD_TO_DR=Forwarding to DR, SG_NODATA=SG Due to Join, A=SG Advertised to MSDP, M=SG Created by MSDP, CP_TO_CPU=Copy to CPU, STATIC_MROUTE=Static Mroute, MRTF_SMLT_PEER_SG=Peer SG On Non-DR For SMLT

8000-2:

PIM Multicast Route - GlobalRouter

Src: 10.50.40.10 Grp: 239.100.100.100 RP: 10.50.60.1 Upstream: 10.50.200.3

Flags: CACHE SG

Incoming Port: Vlan200-MLT-20(3/3),

Outgoing Ports: Vlan200-2/1, Vlan300-2/6,

Joined Ports: Vlan200-2/1, Vlan300-2/6,

Pruned Ports:

Leaf Ports:

Asserted Ports:

Prune Pending Ports:

Assert Winner Ifs:

Assert Loser Ifs:

TIMERS:

Entry	JP	RS	Assert
207	56	0	0
VLAN-Id:	2	200	300
Join-P:	0	207	207
Assert:	0	0	0

Src: 10.50.40.10 Grp: 239.100.100.101 RP: 10.50.60.1 Upstream: 10.50.200.3

Flags: CACHE SG

Incoming Port: Vlan200-MLT-20(3/3),

Outgoing Ports: Vlan200-2/1, Vlan300-2/6,

Joined Ports: Vlan200-2/1, Vlan300-2/6,

Pruned Ports:

Leaf Ports:

Asserted Ports:

Prune Pending Ports:

Assert Winner Ifs:			
Assert Loser Ifs:			
TIMERS:			
Entry	JP	RS	Assert
207	56	0	0
VLAN-Id:	2	200	300
Join-P:	0	207	207
Assert:	0	0	0

Src: 10.50.40.10 Grp: 239.100.100.102 RP: 10.50.60.1 Upstream: 10.50.200.3			
Flags: CACHE SG			
Incoming Port: Vlan200-MLT-20(3/3),			
Outgoing Ports: Vlan200-2/1, Vlan300-2/6,			
Joined Ports: Vlan200-2/1, Vlan300-2/6,			
Pruned Ports:			
Leaf Ports:			
Asserted Ports:			
Prune Pending Ports:			
Assert Winner Ifs:			
Assert Loser Ifs:			
TIMERS:			
Entry	JP	RS	Assert
207	56	0	0
VLAN-Id:	2	200	300
Join-P:	0	207	207
Assert:	0	0	0

Src: 0.0.0.0 Grp: 239.255.255.250 RP: 10.50.60.1 Upstream: 10.50.30.3			
Flags: WC RP CACHE			
Incoming Port: Vlan300-MLT-30(2/6),			
Outgoing Ports: Vlan200-3/3, Vlan300-2/1,			
Joined Ports: Vlan200-3/3, Vlan300-2/1,			
Pruned Ports:			
Leaf Ports:			
Asserted Ports:			
Prune Pending Ports:			
Assert Winner Ifs:			
Assert Loser Ifs:			

TIMERS:

Entry	JP	RS	Assert
210	0	0	0
VLAN-Id:	2	200	300
Join-P:	0	210	151
Assert:	0	0	0

Src: 10.50.40.10 Grp: 239.255.255.250 RP: 10.50.60.1 Upstream: 10.50.200.3

Flags: SPT CACHE SG

Incoming Port: Vlan200-MLT-20(3/3),

Outgoing Ports: Vlan200-2/1,3/3, Vlan300-2/6,

Joined Ports: Vlan200-2/1, Vlan200-3/3, Vlan300-2/6,

Pruned Ports: Vlan300-2/1,

Leaf Ports:

Asserted Ports:

Prune Pending Ports: Vlan200-3/3,

Assert Winner Ifs:

Assert Loser Ifs:

TIMERS:

Entry	JP	RS	Assert
151	5	0	0
VLAN-Id:	2	200	300
Join-P:	0	156	151
Assert:	0	0	0

Total Num of Entries Displayed 5/5

Flags Legend:

SPT = Shortest path tree, WC=(*,Grp) entry, RP=Rendezvous Point tree, CACHE=Kernel Cache, ASSERTED=Asserted, SG=(Src,Grp) en

try, PMBR=(*,*,RP) entry, FWD_TO_RP=Forwarding to RP, FWD_TO_DR=Forwarding to DR, SG_NODATA=SG Due to Join, A=SG Advertised

to MSDP, M=SG Created by MSDP, CP_TO_CPU=Copy to CPU, STATIC_MROUTE=Static Mroute, MRTF_SMLT_PEER_SG=Peer SG On Non-DR For S

MLT

Step 1: ERS5000 - Verify multicast routing table on 5000-1 and 5000-2

ACLI

show ip pim mroute

Results:

5000-1:

Src: 10.50.40.10 Grp: 239.100.100.100 RP: 10.50.60.1 Upstream: NULL

Flags: CACHE SG

Incoming Port: Vlan400-5,

Outgoing Ports: Vlan200-T#1,

Joined Ports: Vlan200-T#1,

Pruned Ports:

Leaf Ports:

Asserted Ports:

Prune Pending Ports:

Assert Winner Ifs:

Assert Loser Ifs:

TIMERS:

Entry	JP	RS	Assert
207	0	2	0

VLAN-Id: 200

Join-P: 202

Assert: 0

Src: 10.50.40.10 Grp: 239.100.100.101 RP: 10.50.60.1 Upstream: NULL

Flags: CACHE SG

Incoming Port: Vlan400-5,

Outgoing Ports: Vlan200-T#1,

Joined Ports: Vlan200-T#1,

Pruned Ports:

Leaf Ports:

Asserted Ports:

Prune Pending Ports:

Assert Winner Ifs:

Assert Loser Ifs:

TIMERS:

Entry	JP	RS	Assert
207	0	2	0

```

VLAN-Id: 200
Join-P: 202
Assert: 0
Src: 10.50.40.10 Grp: 239.100.100.102 RP: 10.50.60.1 Upstream: NULL
Flags: CACHE SG
Incoming Port: Vlan400-5,
Outgoing Ports: Vlan200-T#1,
Joined Ports: Vlan200-T#1,
Pruned Ports:
Leaf Ports:
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
Entry JP RS Assert
207 0 2 0
VLAN-Id: 200
Join-P: 202
Assert: 0
Src: 0.0.0.0 Grp: 239.255.255.250 RP: 10.50.60.1 Upstream: 10.50.200.1

Flags: WC RP CACHE
Incoming Port: Vlan200-T#1,
Outgoing Ports: Vlan400-5,
Joined Ports:
Pruned Ports:
Leaf Ports: Vlan400-5,
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
Entry JP RS Assert
122 55 0 0
VLAN-Id: 200
Join-P: 0
Assert: 0

```

```

Src: 10.50.40.10   Grp: 239.255.255.250 RP: 10.50.60.1 Upstream: NULL
Flags: SPT CACHE SG
Incoming Port: Vlan400-5,
Outgoing Ports: Vlan200-T#1, Vlan400-5,
Joined Ports: Vlan200-T#1,
Pruned Ports:
Leaf Ports: Vlan400-5,
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
Entry   JP   RS   Assert
  151    0    5      0
VLAN-Id:  200
Join-P:   151
Assert:   0

```

Total Num of Entries Displayed 5

Flags Legend:

```

SPT = Shortest path tree
WC = (*,Grp) entry
RP = Rendezvous Point tree
CACHE = Kernel Cache
ASSERTED = Asserted
SG = (Src,Grp) entry
FWD_TO_RP = Forwarding to RP
FWD_TO_DR = Forwarding to DR
SG_NODATA = SG Due to Join
IPMC_ERR = IPMC Add Failed

```

5000-2:

```

Src: 0.0.0.0       Grp: 239.100.100.100 RP: 10.50.60.1 Upstream: NULL
Flags: WC RP CACHE
Incoming Port: Vlan0-cpp,
Outgoing Ports: Vlan600-7, Vlan600-9
Joined Ports:
Pruned Ports:

```

```

Leaf      Ports: Vlan600-7, Vlan600-9
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
  Entry   JP   RS   Assert
    209    0    0        0
VLAN-Id:   300
Join-P:    0
Assert:    0
Src: 10.50.40.10   Grp: 239.100.100.100 RP: 10.50.60.1   Upstream: 10.50.30.1

Flags: SPT CACHE SG
Incoming Port: Vlan300-T#1,
Outgoing Ports: Vlan600-7, Vlan600-9
Joined Ports:
Pruned Ports:
Leaf      Ports: Vlan600-7, Vlan600-9
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
  Entry   JP   RS   Assert
    210    24    0        0
VLAN-Id:   300
Join-P:    0
Assert:    0
Src: 0.0.0.0       Grp: 239.100.100.101 RP: 10.50.60.1   Upstream: NULL
Flags: WC RP CACHE
Incoming Port: Vlan0-cpp,
Outgoing Ports: Vlan600-7, Vlan600-9
Joined Ports:
Pruned Ports:
Leaf      Ports: Vlan600-7, Vlan600-9
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:

```

Entry	JP	RS	Assert
202	0	0	0

VLAN-Id: 300

Join-P: 0

Assert: 0

Src: 10.50.40.10 Grp: 239.100.100.101 RP: 10.50.60.1 Upstream: 10.50.30.1

Flags: SPT CACHE SG

Incoming Port: Vlan300-T#1,

Outgoing Ports: Vlan600-7, Vlan600-9

Joined Ports:

Pruned Ports:

Leaf Ports: Vlan600-7, Vlan600-9

Asserted Ports:

Prune Pending Ports:

Assert Winner Ifs:

Assert Loser Ifs:

TIMERS:

Entry	JP	RS	Assert
206	20	0	0

VLAN-Id: 300

Join-P: 0

Assert: 0

Src: 0.0.0.0 Grp: 239.100.100.102 RP: 10.50.60.1 Upstream: NULL

Flags: WC RP CACHE

Incoming Port: Vlan0-cpp,

Outgoing Ports: Vlan600-7, Vlan600-9

Joined Ports:

Pruned Ports:

Leaf Ports: Vlan600-7, Vlan600-9

Asserted Ports:

Prune Pending Ports:

Assert Winner Ifs:

Assert Loser Ifs:

TIMERS:

Entry	JP	RS	Assert
197	0	0	0

VLAN-Id: 300

Join-P: 0

Assert: 0

Src: 10.50.40.10 Grp: 239.100.100.102 RP: 10.50.60.1 Upstream: 10.50.30.1

Flags: SPT CACHE SG

Incoming Port: Vlan300-T#1,

Outgoing Ports: Vlan600-7, Vlan600-9

Joined Ports:

Pruned Ports:

Leaf Ports: Vlan600-7, Vlan600-9

Asserted Ports:

Prune Pending Ports:

Assert Winner Ifs:

Assert Loser Ifs:

TIMERS:

Entry	JP	RS	Assert
206	20	0	0

VLAN-Id: 300

Join-P: 0

Assert: 0

Src: 0.0.0.0 Grp: 239.255.255.250 RP: 10.50.60.1 Upstream: NULL

Flags: WC RP CACHE

Incoming Port: Vlan0-cpp,

Outgoing Ports: Vlan300-T#1, Vlan600-7

Joined Ports: Vlan300-T#1

Pruned Ports:

Leaf Ports: Vlan600-7

Asserted Ports:

Prune Pending Ports:

Assert Winner Ifs:

Assert Loser Ifs:

TIMERS:

Entry	JP	RS	Assert
201	0	0	0

VLAN-Id: 300

Join-P: 174

Assert: 0

Src: 10.50.40.10 Grp: 239.255.255.250 RP: 10.50.60.1 Upstream: 10.50.30.1

Flags: SPT CACHE SG

Incoming Port: Vlan300-T#1,

Outgoing Ports: Vlan600-7

Joined Ports:

Pruned Ports: Vlan300-T#1

Leaf Ports: Vlan600-7

Asserted Ports:

Prune Pending Ports:

Assert Winner Ifs:

Assert Loser Ifs:

TIMERS:

Entry	JP	RS	Assert
173	23	0	0

VLAN-Id: 300

Join-P: 0

Assert: 0

Total Num of Entries Displayed 8

Flags Legend:

SPT = Shortest path tree

WC = (*, Grp) entry

RP = Rendezvous Point tree

CACHE = Kernel Cache

ASSERTED = Asserted

SG = (Src, Grp) entry

FWD_TO_RP = Forwarding to RP

FWD_TO_DR = Forwarding to DR

SG_NODATA = SG Due to Join

IPMC_ERR = IPMC Add Failed



For each multicast group there needs to be two entries in the multicast route table, a wildcard entry (*,G) and a SPT entry (S,G). Without these entries a DR will not be able to join a Rendezvous Point Tree and subsequently the DR will not learn the source of the IPMC. Consequently a (S,G) entry will never occur and a SP-Tree will never be formed.



The incoming ports (IIF) and outgoing ports (OIF) are determined by the RPF to either the RP or to the source.



The same information can also be viewed by using *show ip mroute route* and *show ip mroute next-hop* to indicate upstream multicast neighbor to either RPT or SPT; as determined by the RPF algorithm.

5.4 PIM-SSM SMLT Triangle Topology Design with L3 Edge

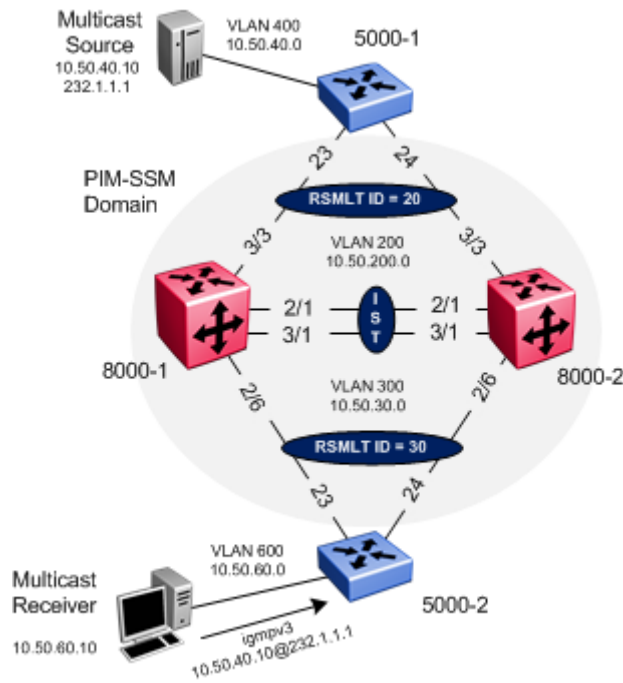


Figure 15: PIM-SSM SMLT ERS5000 Distribution Edge

Continuing from example from section 5.3, instead of providing PIM-SM, this example will show how to setup PIM-SSM on the SMLT cluster and edge routers.

5.4.1 8000 SMLT Cluster

Please follow all the configuration steps from section 5.3.1.1 to 5.3.1.4. The only change is the PIM configuration to setup PIM-SSM.

5.4.1.1 PIM Configuration

8000-1: Step 1 – PIM global configuration

```
8000-1:5(config)#ip pim enable
8000-1:5(config)#ip pim mode ssm
```

8000-2: Step 1 – PIM global configuration

```
8000-2:5# config ip pim enable
8000-2:5# config ip pim mode ssm
```

8000-1: Step 2 – PIM interface configuration

```
8000-1:5(config)#interface vlan 2
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#ip igmp version 3
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 200
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#ip igmp version 3
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 300
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#ip igmp version 3
8000-1:5(config-if)#exit
```

8000-2: Step 2 – PIM interface configuration

```
8000-2:5# config vlan 2 ip igmp version 3
8000-2:5# config vlan 2 ip pim enable
8000-2:5# config vlan 200 ip igmp version 3
8000-2:5# config vlan 200 ip pim enable
8000-2:5# config vlan 300 ip igmp version 3
8000-2:5# config vlan 300 ip pim enable
```

5.4.1.1 ERS5000 Configuration

Please follow all the configuration steps from section 5.2.2.1 to 5.2.2.7. The only change is the PIM configuration to setup PIM-SSM.

5000-1: Step 1 – PIM global configuration

```
5000-1(config)#ip pim enable
5000-1(config)#ip pim mode ssm
```

5000-2: Step 1 – PIM global configuration

```
5000-2(config)#ip pim enable
5000-2(config)#ip pim mode ssm
```

5000-1: Step 2 – PIM interface configuration

```
5000-1(config)#interface vlan 200
5000-1(config-if)#ip pim enable
5000-1(config-if)#exit
5000-1(config)#interface vlan 400
5000-1(config-if)#ip pim interface-type passive
5000-1(config-if)#ip pim enable
5000-1(config-if)#ip igmp version 3
5000-1(config-if)#exit
```

5000-2: Step 2 – PIM interface configuration

```
5000-2(config)#interface vlan 300
5000-2(config-if)#ip pim enable
5000-2(config-if)#exit
5000-2(config)#interface vlan 600
5000-2(config-if)#ip pim interface-type passive
5000-2(config-if)#ip pim enable
5000-2(config-if)#ip igmp version 3
5000-2(config-if)#exit
```

5.4.2 Verify Operations

5.4.2.1 IGMP

Step 1 – SMLT Cluster: Verifying IGMP Queriers. For VLAN 200 and 300, the lowest IP (8000-1) should be the querier for VLAN 200 and 300. IGMP version should display 3 for igmpv3.

CLI/ACLI

```
show ip igmp interface
```

Results:

8000-1:

=====										
IGMP Interface - GlobalRouter										
=====										
IF	QUERY INTVL	STATUS	VERS.	OPER VERS	QUERIER	QUERY MAXRSPT	WRONG QUERY	JOINS	ROBUST	LASTMEM QUERY

V0	125	inact	2	2	0.0.0.0	100	0	0	2	10
V2	125	active	3	3	10.50.2.1	100	0	0	2	10
V200	125	active	3	3	10.50.200.1	100	0	0	2	10
V300	125	active	3	3	10.50.30.1	100	0	0	2	10

8000-2:

=====										
IGMP Interface - GlobalRouter										
=====										
IF	QUERY INTVL	STATUS	VERS.	OPER VERS	QUERIER	QUERY MAXRSPT	WRONG QUERY	JOINS	ROBUST	LASTMEM QUERY

V0	125	inact	2	2	0.0.0.0	100	0	0	2	10
V2	125	active	3	3	10.50.2.1	100	0	0	2	10
V200	125	active	3	3	10.50.200.1	100	0	0	2	10
V300	125	active	3	3	10.50.30.1	100	0	0	2	10

Step 1 – ERS500 : Verifying IGMP Queriers

ACLI

```
show ip igmp interface
```

Results:

5000-1:

Query	Oper				Query	Wrong				LastMbr	Send
VLAN	Intvl	Vers	Vers	Querier	MaxRspT	Query	Joins	Robust		Query	Query
200	125	3	3	10.50.200.1	100	0	0	2		10	No
400	125	3	3	10.50.40.1	100	0	119	2		10	No

5000-2:

Query	Oper				Query	Wrong				LastMbr	Send
VLAN	Intvl	Vers	Vers	Querier	MaxRspT	Query	Joins	Robust		Query	Query
300	125	3	3	10.50.30.1	100	0	0	2		10	No
600	125	3	3	10.50.60.1	100	0	122	2		10	No

Step 2 – ERS8000: Verifying IGMP Groups – should not be any via both 8000-1 & 8000-2

CLI/ACLI

```
show ip igmp group
```

Results:

```
=====
                        Igmp Group
=====
GRPADDR          INPORT          MEMBER          EXPIRATION TYPE
-----
Total number of groups 0
Total number of unique groups 0
```

Step 2 – ERS5000 Verifying IGMP Groups – assuming receiver (10.50.60.10) via 5000-2 on ports 9 requesting stream 10.50.40.10@232.1.1.1

CLI

```
show ip igmp group
```

Results:

5000-2:

Group Address	VLAN	Member Address	Expiration	Type	In Port
232.1.1.1	600	10.50.60.10	259	Dynamic	9

Step 3 – ERS8000: Verifying IGMP sender - assuming receiver (10.50.60.10) via 5000-2 on ports 9 requesting stream 10.50.40.10@232.1.1.1

CLI/ACLI

show ip igmp sender

Results:

8000-1:

=====				
IGMP Sender - GlobalRouter				
=====				
			PORT/	
GRPADDR	IFINDEX	MEMBER	MLT	STATE

232.1.1.1	Vlan 200	10.50.40.10	MLT-20	NOTFILTERED

8000-2:

=====				
IGMP Sender - GlobalRouter				
=====				
			PORT/	
GRPADDR	IFINDEX	MEMBER	MLT	STATE

232.1.1.1	Vlan 200	10.50.40.10	MLT-20	NOTFILTERED

Step 3 – ERS5000: Verifying IGMP sender - assuming receiver (10.50.60.10) via 5000-2 on ports 9 requesting stream 10.50.40.10@232.1.1.1

CLI/ACLI

show ip igmp sender

Results:

5000-1:

Multicast Address	Source Address	Learning Mode	Activity	Admin State

Number of Entries: 0

5000-2:

Multicast Address	Source Address	Learning Mode	Activity	Admin State

232.1.1.1	10.50.40.10	Dynamic	Yes	Enabled

Number of Entries: 1

5.4.2.1 Verify Multicast Routing Table

Step 1: ERS8000 - Verify multicast routing table on 8000-1 and 8000-2

CLI/ACLI

show ip pim mroute

Results:

8000-1:

```
=====
                        PIM Multicast Route - GlobalRouter
=====
Src: 10.50.40.10   Grp: 232.1.1.1   RP: 0.0.0.0   Upstream: 10.50.200.3
Flags: SPT CACHE SG
Incoming Port: Vlan200-MLT-20(3/3),
Outgoing Ports: Vlan200-2/1, Vlan300-2/6,
Joined Ports: Vlan200-2/1, Vlan300-2/6,
Pruned Ports:
Leaf Ports:
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
  Entry   JP   RS   Assert
    152    3    0      0
VLAN-Id:    2   200   300
Join-P:     0   154   152
Assert:     0    0    0
-----
```

Total Num of Entries Displayed 1/1

Flags Legend:

SPT = Shortest path tree, WC=(*,Grp) entry, RP=Rendezvous Point tree, CACHE=Kernel Cache, ASSERTED=Asserted, SG=(Src,Grp) entry, PMBR=(*,*,RP) entry, FWD_TO_RP=Forwarding to RP, FWD_TO_DR=Forwarding to DR, SG_NODATA=SG Due to Join, A=SG Advertised to MSDP, M=SG Created by MSDP, CP_TO_CPU=Copy to CPU, STATIC_MROUTE=Static Mroute, MRTF_SMLT_P
EER_SG=Peer SG On Non-DR For SMLT

8000-2:

PIM Multicast Route - GlobalRouter

Src: 10.50.40.10 Grp: 232.1.1.1 RP: 0.0.0.0 Upstream: 10.50.200.3

Flags: SPT CACHE SG

Incoming Port: Vlan200-MLT-20(3/3),

Outgoing Ports: Vlan200-2/1, Vlan300-2/6,

Joined Ports: Vlan200-2/1, Vlan300-2/6,

Pruned Ports:

Leaf Ports:

Asserted Ports:

Prune Pending Ports:

Assert Winner Ifs:

Assert Loser Ifs:

TIMERS:

Entry	JP	RS	Assert
210	1	0	0
VLAN-Id:	2	200	300
Join-P:	0	151	210
Assert:	0	0	0

Total Num of Entries Displayed 1/1

Flags Legend:

SPT = Shortest path tree, WC=(*,Grp) entry, RP=Rendezvous Point tree, CACHE=Kernel Cache, ASSERTED=Asserted, SG=(S

rc,Grp) entry, PMBR=(*,*,RP) entry, FWD_TO_RP=Forwarding to RP, FWD_TO_DR=Forwarding to DR, SG_NODATA=SG Due to Jo

in, A=SG Advertised to MSDP, M=SG Created by MSDP, CP_TO_CPU=Copy to CPU, STATIC_MROUTE=Static Mroute, MRTF_SMLT_P

EER_SG=Peer SG On Non-DR For SMLT

Step 1: ERS5000 - Verify multicast routing table on 5000-1 and 5000-2

ACLI

show ip pim mroute

Results:

5000-1:

Src: 10.50.40.10 Grp: 232.1.1.1 RP: 0.0.0.0 Upstream: NULL

Flags: SPT CACHE SG

Incoming Port: Vlan400-5,

Outgoing Ports: Vlan200-T#1

Joined Ports: Vlan200-T#1

Pruned Ports:

Leaf Ports:

Asserted Ports:

Prune Pending Ports:

Assert Winner Ifs:

Assert Loser Ifs:

TIMERS:

Entry	JP	RS	Assert
204	0	0	0

VLAN-Id: 200

Join-P: 204

Assert: 0

Total Num of Entries Displayed 1

Flags Legend:

SPT = Shortest path tree

WC = (*,Grp) entry

RP = Rendezvous Point tree

CACHE = Kernel Cache

ASSERTED = Asserted

SG = (Src,Grp) entry

FWD_TO_RP = Forwarding to RP

FWD_TO_DR = Forwarding to DR

SG_NODATA = SG Due to Join

IPMC_ERR = IPMC Add Failed

5000-2:

Src: 10.50.40.10 Grp: 232.1.1.1 RP: 0.0.0.0 Upstream: 10.50.30.1

Flags: SPT CACHE SG

Incoming Port: Vlan300-T#1,

Outgoing Ports: Vlan600-9

Joined Ports:

Pruned Ports:

Leaf Ports: Vlan600-9

Asserted Ports:

Prune Pending Ports:

Assert Winner Ifs:

Assert Loser Ifs:

TIMERS:

Entry	JP	RS	Assert
97	52	0	0

VLAN-Id: 300

Join-P: 0

Assert: 0

Total Num of Entries Displayed 1

Flags Legend:

SPT = Shortest path tree
 WC = (*,Grp) entry
 RP = Rendezvous Point tree
 CACHE = Kernel Cache
 ASSERTED = Asserted
 SG = (Src,Grp) entry
 FWD_TO_RP = Forwarding to RP
 FWD_TO_DR = Forwarding to DR
 SG_NODATA = SG Due to Join
 IPMC_ERR = IPMC Add Failed

5.5 PIM-SM RSMLT Square/Mesh Topology

The following diagram is an example of the configuration of PIM-SM on RSMLT Squares or Full Mesh Topologies. Please refer to the Switch Clustering using Split Multi-Link Trunking (SMLT) Technical Configuration Guide for the details on the best practices for SMLT.

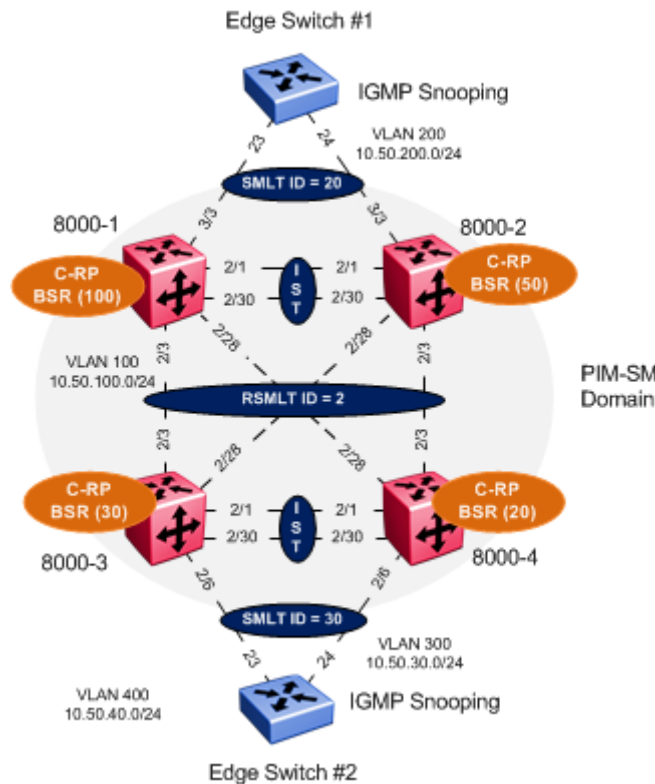


Figure 16: PIM-SM RSMLT Mesh Topology

In this example the following will be configured as per Figure 16.

- IST
 - VLAN 2 is configured and associated to MLT# 1.
 - Tagging is enabled on ports 2/1,2/30
- VLACP and SLPP settings are configured as defined in the Switch Clustering using SMLT TCG
- SMLT ID 20: VLAN 200 (port 3/3) on switch Cluster #1
- SMLT ID 30: VLAN 300 (port 2/6) on Switch Cluster #2
- Core SMLT ID 2: VLAN 100 (ports 2/3 and 2/28)
- RSMLT Edge is enabled on SMLT VLAN 200, 300
- RSMLT is enabled on Core SMLT VLAN



RSMLT Edge support for resilient default gateway designs. The RSMLT peer IP and MAC address and VLAN information are stored in the ERS 8000 configuration files.



The RSMLT hold-down timer should be set to 1.5x the IGP convergence time. With OSPF typical hold-down time is 90 seconds. RSMLT Edge holdup timer should be set to 9999 (infinity) to allow the RSMLT peer nodes to forward indefinitely on behalf of each other.

- CLIP/Loopback address are configured
- Dynamic PIM-SM is enabled
- PIM-SM active mode is enabled on VLANs 200, 300 and 100
- PIM-SM active mode is enabled on IST VLAN 100



In order to achieve sub second failovers/recoveries with PIM-SM the IST VLAN all VLANs associated with a SMLT should be configured in PIM active mode. All other VLANs not associated with either a SMLT or PIM adjacencies should be configured in passive mode.

- Mcast-smlt square-smlt flag is enabled



In a square/mesh design the smlt-square flag must be enabled on all four switches in the SMLT square. This flag provides faster recoveries when a switch fails. A static route to the source, RP and BSR is created and used until the IGP converges and the recovered switch dynamic learns routes via IGP.

- Candidate RPs are defined on each ERS 8000 for redundant RPs.
- Candidate BSRs are defined on each ERS 8000 for redundant BSR.



It is recommended that the BSR and RP are configured on a CLIP/Loopback address. This will prevent a BSR or RP failure if a VLAN interface goes down.

Recommended that the OSPF router ID is configured the same as the CLIP/Loopback address for management simplicity.

- OSPF Area 0.0.0.0
- OSPF active mode is enabled on VLAN 100
- OSPF passive mode is enabled on VLAN 200, 300 and on the CLIP/Loopback address



The CLIP/Loopback IP address must be reachable throughout the network. It is recommended that the CLIP/Loopback address is OSPF enabled. OSPF neighbors will learn the CLIP/Loopback address through OSPF on through the core SMLT VLAN 100.



It is recommended to make OSPF interfaces passive on VLANs extending to a L2 SMLT access switch. This will prevent adjacencies from forming at the access switches. In addition this will reduce the amount of OSPF control messages to the edge switches.

- On the Edge switches
- VLAN 200 and 300 are configured on Edge switch 1 and 2 respectively
- MLT is configured on switch 1 and 2 respectively
- IGMP Snooping and proxy are configured on VLAN 200 and 300



It is always recommended to enable IGMP snooping and proxy on edge switches. IGMP snooping will ensure that all ports are not flooded with IPMC while proxy consolidates all MHR and sends one MHR to the IGMP Querier.

Three IPMC streams (239.100.100.100, 239.100.100.101, 239.100.100.102) are generated from a multicast source using either MC Hammer or Winsend located on edge switch #2. A multicast receiver for all three IPMC streams are located off edge switch #1.

5.5.1 Configuration – ERS 8000 cluster

For this configuration example SMLT cluster 1 (8000-1 & 8000-2) are provisioned using ACLI while cluster 2 (8000-3 & 8000-4) are provisioned using CLI.

5.5.1.1 IST Configuration

Cluster 1

8000-1: Step 1 - Create IST using VLAN 2 and MLT 1

```
8000-1:5(config)#vlan create 2 name IST type port 1
8000-1:5(config-if)#interface vlan 2
8000-1:5(config-if)#ip address 10.50.2.1 255.255.255.252
8000-1:5(config-if)#exit
8000-1:5(config)#mlt 1
8000-1:5(config)#mlt 1 name IST
8000-1:5(config)#mlt 1 member 2/1,2/30
8000-1:5(config)#vlan mlt 2 1
8000-1:5(config)#mlt 1 encapsulation dot1q
8000-1:5(config)#interface mlt 1
8000-1:5(config-mlt)#ist peer-ip 10.50.2.2 vlan 2
8000-1:5(config-mlt)#ist enable
8000-1:5(config-mlt)#exit
```

8000-2: Step 1 - Create IST using VLAN 2 and MLT 1

```
8000-2:5(config)#vlan create 2 name IST type port 1
8000-2:5(config-if)#interface vlan 2
8000-2:5(config-if)#ip address 10.50.2.2 255.255.255.252
8000-2:5(config-if)#exit
8000-2:5(config)#mlt 1
8000-2:5(config)#mlt 1 name IST
8000-2:5(config)#mlt 1 member 2/1,2/30
8000-2:5(config)#vlan mlt 2 1
8000-2:5(config)#mlt 1 encapsulation dot1q
8000-2:5(config)#interface mlt 1
8000-2:5(config-mlt)#ist peer-ip 10.50.2.1 vlan 2
8000-2:5(config-mlt)#ist enable
```



```
8000-2:5(config-mlt)#exit
```

Cluster 2

8000-3: Step 1 - Create IST using VLAN 2 and MLT 1

```
8000-3:5# config vlan 2 create byport 1 name IST
8000-3:5# config vlan 2 ip create 10.50.3.1/255.255.255.252
8000-3:5# config mlt 1 create
8000-3:5# config mlt 1 add ports 2/1,2/30
8000-3:5# config vlan 2 add-mlt 1
8000-3:5# config mlt 1 name IST
8000-3:5# config mlt 1 perform-tagging enable
8000-3:5# config mlt 1 ist create ip 10.50.3.2 vlan-id 2
8000-3:5# config mlt 1 ist enable
```

8000-4: Step 1 - Create IST using VLAN 2 and MLT 1

```
8000-4:5# config vlan 2 create byport 1 name IST
8000-4:5# config vlan 2 ip create 10.50.3.2/255.255.255.252
8000-4:5# config mlt 1 create
8000-4:5# config mlt 1 add ports 2/1,2/30
8000-4:5# config vlan 2 add-mlt 1
8000-4:5# config mlt 1 name IST
8000-4:5# config mlt 1 perform-tagging enable
8000-4:5# config mlt 1 ist create ip 10.50.3.1 vlan-id 2
8000-4:5# config mlt 1 ist enable
```

5.5.1.2 SMLT Configuration

Cluster 1

8000-1: Step 1: Create VLAN 100 using MLT/SMLT ID 2

```
8000-1:5(config)#vlan create 100 name Core_VLAN type port 1
8000-1:5(config)#interface vlan 100
8000-1:5(config-if)#ip address 10.50.100.1 255.255.255.0
8000-1:5(config-if)#exit
8000-1:5(config)#mlt 2
8000-1:5(config)#vlan mlt 100 2
8000-1:5(config)#mlt 2 name Core_SMLT
8000-1:5(config)#mlt 2 encapsulation dot1q
8000-1:5(config)#mlt 2 member 2/3,2/28
8000-1:5(config)#interface mlt 2
8000-1:5(config-mlt)#smlt 2
8000-1:5(config-mlt)#exit
8000-1:5(config)#vlan mlt 100 1
```

8000-2: Step 1: Create VLAN 100 using MLT/SMLT ID 2

```
8000-2:5(config)#vlan create 100 name Core_VLAN type port 1
8000-2:5(config)#interface vlan 100
8000-2:5(config-if)#ip address 10.50.100.2 255.255.255.0
8000-2:5(config-if)#exit
8000-2:5(config)#mlt 2
8000-2:5(config)#vlan mlt 100 2
8000-2:5(config)#mlt 2 name Core_SMLT
8000-2:5(config)#mlt 2 encapsulation dot1q
8000-2:5(config)#mlt 2 member 2/3,2/28
8000-2:5(config)#interface mlt 2
8000-2:5(config-mlt)#smlt 2
8000-2:5(config-mlt)#exit
8000-2:5(config)#vlan mlt 100 1
```

8000-1: Step 2: Create VLAN 200 using MLT/SMLT ID 20

```
8000-1:5(config)#vlan create 200 name Closet_Sw1 type port 1
8000-1:5(config)#interface vlan 200
8000-1:5(config-if)#ip address 10.50.200.1 255.255.255.0
8000-1:5(config-if)#exit
8000-1:5(config)#mlt 20
8000-1:5(config)#vlan mlt 200 20
8000-1:5(config)#mlt 20 name SMLT-20
8000-1:5(config)#mlt 20 encapsulation dot1q
8000-1:5(config)#mlt 20 member 3/3
8000-1:5(config)#interface mlt 20
8000-1:5(config-mlt)#smlt 20
8000-1:5(config-mlt)#exit
8000-1:5(config)#vlan mlt 200 1
```

8000-2: Step 2: Create VLAN 200 using MLT/SMLT ID 20

```
8000-1:5(config)#vlan create 200 name Closet_Sw1 type port 1
8000-1:5(config)#interface vlan 200
8000-1:5(config-if)#ip address 10.50.200.2 255.255.255.0
8000-1:5(config-if)#exit
8000-1:5(config)#mlt 20
8000-1:5(config)#vlan mlt 200 20
8000-1:5(config)#mlt 20 name SMLT-20
8000-1:5(config)#mlt 20 encapsulation dot1q
8000-1:5(config)#mlt 20 member 3/3
8000-1:5(config)#interface mlt 20
8000-1:5(config-mlt)#smlt 20
8000-1:5(config-mlt)#exit
8000-1:5(config)#vlan mlt 200 1
```

Cluster 2

8000-3: Step 1: Create VLAN 100 using MLT/SMLT ID 2

```
8000-3:5# config vlan 100 create byport 1 name Core_VLAN
8000-3:5# config vlan 100 ip create 10.50.100.3/255.255.255.0
8000-3:5# config mlt 2 create
8000-3:5# config mlt 2 add ports 2/3,2/28
8000-3:5# config vlan 100 add-mlt 2
8000-3:5# config mlt 2 name Core_SMLT
8000-3:5# config mlt 2 perform-tagging enable
8000-3:5# config mlt 2 smlt create smlt-id 2
8000-3:5# config mlt 1 add vlan 100
```

8000-4: Step 1: Create VLAN 100 using MLT/SMLT ID 2

```
8000-4:5# config vlan 100 create byport 1 name Core_VLAN
8000-4:5# config vlan 100 ip create 10.50.100.4/255.255.255.0
8000-4:5# config mlt 2 create
8000-4:5# config mlt 2 add ports 2/3,2/28
8000-4:5# config vlan 100 add-mlt 2
8000-4:5# config mlt 2 name Core_SMLT
8000-4:5# config mlt 2 perform-tagging enable
8000-4:5# config mlt 2 smlt create smlt-id 2
8000-4:5# config mlt 1 add vlan 100
```

8000-3: Step 2: Create VLAN 300 using MLT/SMLT ID 30

```
8000-3:5# config vlan 300 create byport 1 name Closet_Sw2
8000-3:5# config vlan 300 ip create 10.50.30.1/255.255.255.0
8000-3:5# config mlt 30 create
8000-3:5# config mlt 30 add ports 2/6
8000-3:5# config vlan 300 add-mlt 30
8000-3:5# config mlt 30 name SMLT-30
8000-3:5# config mlt 30 perform-tagging enable
8000-3:5# config mlt 30 smlt create smlt-id 30
8000-3:5# config mlt 1 add vlan 300
```

8000-4: Step 2: Create VLAN 300 using MLT/SMLT ID 30

```
8000-4:5# config vlan 300 create byport 1 name Closet_Sw2
8000-4 5# config vlan 300 ip create 10.50.30.2/255.255.255.0
8000-4:5# config mlt 30 create
8000-4:5# config mlt 30 add ports 2/6
8000-4:5# config vlan 300 add-mlt 30
8000-4:5# config mlt 30 name SMLT-30
8000-4:5# config mlt 30 perform-tagging enable
8000-4:5# config mlt 30 smlt create smlt-id 30
8000-4:5# config mlt 1 add vlan 300
```

5.5.1.3 Enable RSMLT

Cluster 1

8000-1: Step 1: RSMLT Configuration

```
8000-1:5(config)#ip rsmlt edge-support
8000-1:5(config)#interface vlan 200
8000-1:5(config-if)#ip rsmlt
8000-1:5(config-if)#ip rsmlt holdup-timer 9999
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 100
8000-1:5(config-if)#ip rsmlt
8000-1:5(config-if)#exit
```

8000-2: Step 1: RSMLT Configuration

```
8000-2:5(config)#ip rsmlt edge-support
8000-2:5(config)#interface vlan 200
8000-2:5(config-if)#ip rsmlt
8000-2:5(config-if)#ip rsmlt holdup-timer 9999
8000-2:5(config-if)#exit
8000-2:5(config)#interface vlan 100
8000-2:5(config-if)#ip rsmlt
8000-2:5(config-if)#exit
```

Cluster 2

8000-3: Step 1: RSMLT Configuration

```
8000-3:5# config ip rsmlt rsmlt-edge-support enable
8000-3:5# config vlan 300 ip rsmlt enable
8000-3:5# config vlan 300 ip rsmlt holdup-timer 9999
8000-3:5# config vlan 100 ip rsmlt enable
```

8000-4: Step 1: RSMLT Configuration

```
8000-4:5# config ip rsmlt rsmlt-edge-support enable
8000-4:5# config vlan 300 ip rsmlt enable
8000-4:5# config vlan 300 ip rsmlt holdup-timer 9999
8000-4:5# config vlan 100 ip rsmlt enable
```

5.5.1.4 Circuitless/Loopback IP address configuration

Cluster 1

8000-1: Step 1 – Create loopback address

```
8000-1:5(config)#interface loopback 1
8000-1:5(config-if)#ip address 1.1.1.1/32
8000-1:5(config-if)#ip ospf
8000-1:5(config-if)#ip pim
8000-1:5(config-if)#exit
```

8000-2: Step 1 – Create loopback address

```
8000-2:5(config)#interface loopback 1
8000-2:5(config-if)#ip address 2.2.2.2/32
8000-2:5(config-if)#ip ospf
8000-2:5(config-if)#ip pim
8000-2:5(config-if)#exit
```

Cluster 2

8000-3: Step 1 – Create CLIP address

```
8000-3:5# config ip circuitless-ip-int 1 create 3.3.3.3/255.255.255.255
8000-3:5# config ip circuitless-ip-int 1 ospf enable
8000-3:5# config ip circuitless-ip-int 1 pim enable
```

8000-4: Step 1 – Create CLIP address

```
8000-4:5# config ip circuitless-ip-int 1 create 4.4.4.4/255.255.255.255
8000-4:5# config ip circuitless-ip-int 1 ospf enable
8000-4:5# config ip circuitless-ip-int 1 pim enable
```

5.5.1.5 OSPF Configuration

Cluster 1

8000-1: Step 1 – OSPF global configuration

```
8000-1:5(config)#router ospf enable
8000-1:5(config)#router ospf
8000-1:5(config-ospf)#router-id 1.1.1.1
8000-1:5(config-ospf)#exit
```

8000-2: Step 1 – OSPF global configuration

```
8000-2:5(config)#router ospf enable
8000-2:5(config)#router ospf
8000-2:5(config-ospf)#router-id 2.2.2.2
8000-2:5(config-ospf)#exit
```

8000-1: Step 2 – OSPF interface configuration

```
8000-1:5(config)#interface vlan 100
8000-1:5(config-if)#ip ospf enable
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 200
8000-1:5(config-if)#ip ospf network passive
8000-1:5(config-if)#ip ospf enable
8000-1:5(config-if)#exit
```

8000-2: Step 2 – OSPF interface configuration

```
8000-2:5(config)#interface vlan 100
8000-2:5(config-if)#ip ospf enable
8000-2:5(config-if)#exit
8000-2:5(config)#interface vlan 200
8000-2:5(config-if)#ip ospf network passive
8000-2:5(config-if)#ip ospf enable
8000-2:5(config-if)#exit
```

Cluster 2

8000-3: Step 1 – OSPF global configuration

```
8000-3:5# config ip ospf admin-state enable
8000-3:5# config ip ospf router-id 3.3.3.3
8000-3:5# config ip ospf enable
```

8000-4: Step 1 – OSPF global configuration

```
8000-4:5# config ip ospf admin-state enable
8000-4:5# config ip ospf router-id 4.4.4.4
8000-4:5# config ip ospf enable
```

8000-3: Step 2 – OSPF interface configuration

```
8000-3:5# config vlan 100 ip ospf enable
8000-3:5# config vlan 300 ip ospf interface-type passive
8000-3:5# config vlan 300 ip ospf enable
```

8000-4: Step 2 – OSPF interface configuration

```
8000-4:5# config vlan 100 ip ospf enable
8000-4:5# config vlan 300 ip ospf interface-type passive
8000-4:5# config vlan 300 ip ospf enable
```


5.5.1.6 PIM Configuration

Cluster 1

8000-1: Step 1 – PIM global configuration

```
8000-1:5(config)#ip pim enable
8000-1:5(config)#ip pim rp-candidate group 239.0.0.0 255.0.0.0 rp 1.1.1.1
8000-1:5(config)#interface loopback 1
8000-1:5(config-if)#ip pim bsr-candidate preference 100
8000-1:5(config-if)#exit
```

8000-2: Step 1 – PIM global configuration

```
8000-2:5(config)#ip pim enable
8000-2:5(config)#ip pim rp-candidate group 239.0.0.0 255.0.0.0 rp 2.2.2.2
8000-2:5(config)#interface loopback 1
8000-2:5(config-if)#ip pim bsr-candidate preference 50
8000-2:5(config-if)#exit
```

8000-1: Step 2 – PIM interface configuration

```
8000-1:5(config)#interface vlan 2
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 100
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 200
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#exit
```

8000-2: Step 2 – PIM interface configuration

```
8000-2:5(config)#interface vlan 2
8000-2:5(config-if)#ip pim enable
8000-2:5(config-if)#exit
8000-2:5(config)#interface vlan 100
8000-2:5(config-if)#ip pim enable
8000-2:5(config-if)#exit
8000-2:5(config)#interface vlan 200
8000-2:5(config-if)#ip pim enable
8000-2:5(config-if)#exit
```

Cluster 2

8000-3: Step 1 – PIM global configuration

```
8000-3:5# config ip pim enable
8000-3:5# config ip circuitless-ip-int 1 pim enable
8000-3:5# config ip pim candrp add grp 239.0.0.0 mask 255.0.0.0 rp 3.3.3.3
8000-3:5# config ip pim interface 3.3.3.3 cbsrpreference 30 enable
```

8000-4: Step 1 – PIM global configuration

```
8000-4:5# config ip pim enable
8000-4:5# config ip circuitless-ip-int 1 pim enable
8000-4:5# config ip pim candrp add grp 239.0.0.0 mask 255.0.0.0 rp 4.4.4.4
8000-4:5# config ip pim interface 4.4.4.4 cbsrpreference 20 enable
```

8000-3: Step 2 – PIM interface configuration

```
8000-3:5# config vlan 2 ip pim enable
8000-3:5# config vlan 100 ip pim enable
8000-3:5# config vlan 300 ip pim enable
```

8000-4: Step 2 – PIM interface configuration

```
8000-2:5# config vlan 2 ip pim enable
8000-4:5# config vlan 100 ip pim enable
8000-4:5# config vlan 300 ip pim enable
```

5.5.2 Verify Operations

5.5.2.1 IGMP

Step 1 – Verify IGMP interface on both SMLT clusters

CLI/ACLI

show ip igmp interface

Results:

8000-1:

```
=====
                                Igmp Interface
=====
```

IF	QUERY INTVL	STATUS	OPER VERS.	OPER VERS	QUERIER	QUERY MAXRSPT	WRONG QUERY	JOINS	ROBUST	LASTMEM QUERY
V2	125	active	2	2	10.50.2.1	100	0	0	2	10
V100	125	active	2	2	10.50.100.1	100	0	0	2	10
V200	125	active	2	2	10.50.200.1	100	0	575	2	10

3 out of 3 entries displayed

8000-2:

```
=====
                                Igmp Interface
=====
```

IF	QUERY INTVL	STATUS	OPER VERS.	OPER VERS	QUERIER	QUERY MAXRSPT	WRONG QUERY	JOINS	ROBUST	LASTMEM QUERY
V2	125	active	2	2	10.50.2.1	100	0	0	2	10
V100	125	active	2	2	10.50.100.1	100	0	0	2	10
V200	125	active	2	2	10.50.200.1	100	0	562	2	10

3 out of 3 entries displayed

8000-3:

```
=====
```

Igmp Interface

=====										
	QUERY		OPER			QUERY	WRONG		LASTMEM	
IF	INTVL	STATUS	VERS.	VERS	QUERIER	MAXRSPT	QUERY	JOINS	ROBUST	QUERY

V2	125	active	2	2	10.50.3.1	100	0	0	2	10
V100	125	active	2	2	10.50.100.1	100	0	0	2	10
V300	125	active	2	2	10.50.30.1	100	0	6	2	10
3 out of 3 entries displayed										

8000-4:

Igmp Interface

=====										
	QUERY		OPER			QUERY	WRONG		LASTMEM	
IF	INTVL	STATUS	VERS.	VERS	QUERIER	MAXRSPT	QUERY	JOINS	ROBUST	QUERY

V2	125	active	2	2	10.50.3.1	100	0	0	2	10
V100	125	active	2	2	10.50.100.1	100	0	0	2	10
V300	125	active	2	2	10.50.30.1	100	0	6	2	10
3 out of 3 entries displayed										

Step 2 – Verify IGMP groups on both SMLT clusters

CLI/ACLI

show ip igmp group

Results:

8000-1:

=====				
Igmp Group				
=====				
GRPADDR	INPORT	MEMBER	EXPIRATION	TYPE

239.100.100.100	V200-3/3	10.50.200.20	198	Dynamic
239.100.100.101	V200-3/3	10.50.200.20	198	Dynamic
239.100.100.102	V200-3/3	10.50.200.20	204	Dynamic

239.255.255.250 V200-3/3 10.50.200.20 206 Dynamic

8000-2:

=====

Igmp Group

=====

GRPADDR	INPORT	MEMBER	EXPIRATION	TYPE
---------	--------	--------	------------	------

239.100.100.100	V200-3/3	10.50.200.20	229	Dynamic
-----------------	----------	--------------	-----	---------

239.100.100.101	V200-3/3	10.50.200.20	229	Dynamic
-----------------	----------	--------------	-----	---------

239.100.100.102	V200-3/3	10.50.200.20	229	Dynamic
-----------------	----------	--------------	-----	---------

239.255.255.250	V200-3/3	10.50.200.20	229	Dynamic
-----------------	----------	--------------	-----	---------

8000-3:

=====

Igmp Group

=====

GRPADDR	INPORT	MEMBER	EXPIRATION	TYPE
---------	--------	--------	------------	------

239.255.255.250	V300-2/6	10.50.30.20	193	Dynamic
-----------------	----------	-------------	-----	---------

Total number of groups 1

8000-4:

=====

Igmp Group

=====

GRPADDR	INPORT	MEMBER	EXPIRATION	TYPE
---------	--------	--------	------------	------

239.255.255.250	V300-2/6	10.50.30.20	138	Dynamic
-----------------	----------	-------------	-----	---------

Total number of groups 1

Step 2 – Verify IGMP senders on both SMLT clusters

CLI/ACLI

show ip igmp sender

Results:

8000-1:

```
=====
                        Igmp Sender
=====
GRPADDR          IFINDEX    MEMBER          PORT          STATE
-----
239.100.100.100  Vlan 100    10.50.30.20     2/3           NOTFILTERED
239.100.100.101  Vlan 100    10.50.30.20     2/3           NOTFILTERED
239.100.100.102  Vlan 100    10.50.30.20     2/3           NOTFILTERED
239.100.100.100  Vlan 200    10.50.200.20     2/1           NOTFILTERED
239.100.100.101  Vlan 200    10.50.200.20     2/1           NOTFILTERED
239.100.100.102  Vlan 200    10.50.200.20     2/1           NOTFILTERED
```

8000-2:

```
=====
                        Igmp Sender
=====
GRPADDR          IFINDEX    MEMBER          PORT          STATE
-----
239.100.100.100  Vlan 100    10.50.30.20     2/3           NOTFILTERED
239.100.100.101  Vlan 100    10.50.30.20     2/3           NOTFILTERED
239.100.100.102  Vlan 100    10.50.30.20     2/3           NOTFILTERED
```

8000-3:

```
=====
                        Igmp Sender
=====
GRPADDR          IFINDEX    MEMBER          PORT          STATE
-----
```

239.100.100.100	Vlan 100	10.50.200.20	2/3	NOTFILTERED
239.100.100.101	Vlan 100	10.50.200.20	2/3	NOTFILTERED
239.100.100.102	Vlan 100	10.50.200.20	2/3	NOTFILTERED
239.100.100.100	Vlan 300	10.50.30.20	2/6	NOTFILTERED
239.100.100.101	Vlan 300	10.50.30.20	2/6	NOTFILTERED
239.100.100.102	Vlan 300	10.50.30.20	2/6	NOTFILTERED

8000-4:

```
=====
                                Igmp Sender
=====
GRPADDR          IFINDEX    MEMBER          PORT          STATE
-----
239.100.100.100  Vlan 100    10.50.200.20    2/28          NOTFILTERED
239.100.100.101  Vlan 100    10.50.200.20    2/28          NOTFILTERED
239.100.100.102  Vlan 100    10.50.200.20    2/28          NOTFILTERED
239.100.100.100  Vlan 300    10.50.30.20     2/1           NOTFILTERED
239.100.100.101  Vlan 300    10.50.30.20     2/1           NOTFILTERED
239.100.100.102  Vlan 300    10.50.30.20     2/1           NOTFILTERED
```

5.5.2.2 PIM

Step 1: ERS8000 - Verify PIM neighbors on both SMLT clusters

CLI/ACLI

show ip pim neighbor

Results:

8000-1:

```
=====
                        Pim Neighbor
=====
INTERFACE ADDRESS          UPTIME                      EXPIRE
-----
Vlan2      10.50.2.2         0 day(s), 02:39:00         0 day(s), 00:01:26
Vlan100    10.50.100.2         0 day(s), 02:32:37         0 day(s), 00:01:17
Vlan100    10.50.100.3         0 day(s), 02:40:47         0 day(s), 00:01:16
Vlan100    10.50.100.4         0 day(s), 02:40:48         0 day(s), 00:01:40
Vlan200    10.50.200.2         0 day(s), 02:40:07         0 day(s), 00:01:19
Total PIM Neighbors = 5
```

8000-2:

```
=====
                        Pim Neighbor
=====
INTERFACE ADDRESS          UPTIME                      EXPIRE
-----
Vlan2      10.50.2.1         0 day(s), 02:42:56         0 day(s), 00:01:33
Vlan100    10.50.100.1         0 day(s), 02:36:32         0 day(s), 00:01:23
Vlan100    10.50.100.3         0 day(s), 02:36:32         0 day(s), 00:01:23
Vlan100    10.50.100.4         0 day(s), 02:36:32         0 day(s), 00:01:16
Vlan200    10.50.200.1         0 day(s), 02:44:03         0 day(s), 00:01:26
Total PIM Neighbors = 5
```

8000-3:

```
=====
                        Pim Neighbor
```



```
=====
INTERFACE ADDRESS          UPTIME                      EXPIRE
-----
Vlan2      10.50.3.2            0 day(s), 04:58:06         0 day(s), 00:01:38
Vlan300    10.50.30.2             0 day(s), 04:58:06         0 day(s), 00:01:34
Vlan100    10.50.100.1             0 day(s), 02:46:17         0 day(s), 00:01:21
Vlan100    10.50.100.2             0 day(s), 02:38:36         0 day(s), 00:01:21
Vlan100    10.50.100.4             0 day(s), 04:58:06         0 day(s), 00:01:45
Total PIM Neighbors = 5
```

8000-4:

```
=====
                          Pim Neighbor
=====
INTERFACE ADDRESS          UPTIME                      EXPIRE
-----
Vlan2      10.50.3.1            0 day(s), 04:56:13         0 day(s), 00:01:17
Vlan300    10.50.30.1             0 day(s), 04:56:13         0 day(s), 00:01:16
Vlan100    10.50.100.1             0 day(s), 02:45:43         0 day(s), 00:01:44
Vlan100    10.50.100.2             0 day(s), 02:38:06         0 day(s), 00:01:15
Vlan100    10.50.100.3             0 day(s), 04:56:13         0 day(s), 00:01:44
Total PIM Neighbors = 5
```

Step 2: ERS8000 - Verify that the BSR are identical on 8000-1 and 8000-2

CLI/ACLI

show ip pim bsr

Results:

8000-1:

```
=====
                          Current BootStrap Router Info
=====

Current BSR address: 1.1.1.1
Current BSR priority: 100
Current BSR HashMask: 255.255.255.252
Current BSR Fragment Tag: 741
```

Pim Bootstrap Timer : 6

8000-2:

=====

Current BootStrap Router Info

=====

Current BSR address: 1.1.1.1

Current BSR priority: 100

Current BSR HashMask: 255.255.255.252

Current BSR Fragment Tag: 741

Pim Bootstrap Timer : 76

8000-3:

=====

Current BootStrap Router Info

=====

Current BSR address: 1.1.1.1

Current BSR priority: 100

Current BSR HashMask: 255.255.255.252

Current BSR Fragment Tag: 741

Pim Bootstrap Timer : 76

8000-4:

=====

Current BootStrap Router Info

=====

Current BSR address: 1.1.1.1

Current BSR priority: 100

Current BSR HashMask: 255.255.255.252

Current BSR Fragment Tag: 741

Pim Bootstrap Timer : 76

Step 3: ERS8000 - Verify that the RP Sets are identical on SMLT Clusters

CLI

show ip pim rp-set

ACLI

show ip pim rp-hash

Results:

8000-1:

=====

Pim RPSet

=====

GRPADDRESS	GRPMASK	ADDRESS	HOLDTIME	EXPTIME
-----	-----	-----	-----	-----
239.0.0.0	255.0.0.0	1.1.1.1	150	99
239.0.0.0	255.0.0.0	2.2.2.2	150	115
239.0.0.0	255.0.0.0	3.3.3.3	150	144
239.0.0.0	255.0.0.0	4.4.4.4	150	116

8000-2:

=====

Pim RPSet

=====

GRPADDRESS	GRPMASK	ADDRESS	HOLDTIME	EXPTIME
-----	-----	-----	-----	-----
239.0.0.0	255.0.0.0	1.1.1.1	0	0
239.0.0.0	255.0.0.0	2.2.2.2	0	0
239.0.0.0	255.0.0.0	3.3.3.3	0	0
239.0.0.0	255.0.0.0	4.4.4.4	0	0

8000-3:

=====

Pim RPSet

=====

GRPADDRESS	GRPMASK	ADDRESS	HOLDTIME	EXPTIME
-----	-----	-----	-----	-----

239.0.0.0	255.0.0.0	1.1.1.1	0	0
239.0.0.0	255.0.0.0	2.2.2.2	0	0
239.0.0.0	255.0.0.0	3.3.3.3	0	0
239.0.0.0	255.0.0.0	4.4.4.4	0	0

8000-4:

=====

Pim RPSet

=====

GRPADDRESS	GRPMASK	ADDRESS	HOLDTIME	EXPTIME
------------	---------	---------	----------	---------

239.0.0.0	255.0.0.0	1.1.1.1	0	0
239.0.0.0	255.0.0.0	2.2.2.2	0	0
239.0.0.0	255.0.0.0	3.3.3.3	0	0
239.0.0.0	255.0.0.0	4.4.4.4	0	0

Step 4: ERS8000 - Verify that the Active RP are identical on SMLT Clusters

CLI/ACLI

show ip pim active-rp

Results:

8000-1:

```
=====
                        Pim Grp->RP Active RP Table
=====
GRPADDR          RP-ADDR          RP-PRIORITY
-----
239.100.100.100   3.3.3.3              0
239.100.100.101   3.3.3.3              0
239.100.100.102   3.3.3.3              0
```

8000-2:

```
=====
                        Pim Grp->RP Active RP Table
=====
GRPADDR          RP-ADDR          RP-PRIORITY
-----
239.100.100.100   3.3.3.3              0
239.100.100.101   3.3.3.3              0
239.100.100.102   3.3.3.3              0
```

8000-3:

```
=====
                        Pim Grp->RP Active RP Table
=====
GRPADDR          RP-ADDR          RP-PRIORITY
-----
239.100.100.100   3.3.3.3              0
239.100.100.101   3.3.3.3              0
239.100.100.102   3.3.3.3              0
```

8000-4:

=====		
Pim Grp->RP Active RP Table		
=====		
GRPADDR	RP-ADDR	RP-PRIORITY

239.100.100.100	3.3.3.3	0
239.100.100.101	3.3.3.3	0
239.100.100.102	3.3.3.3	0

5.5.2.1 Verify multicast routing table

Step 1: ERS8000 - Verify multicast routing table on both SMLT clusters

CLI/ACLI

show ip pim mroute

Results:

8000-1:

```
=====
                          Pim Multicast Route
=====
Src: 0.0.0.0      Grp: 239.100.100.100 RP: 3.3.3.3      Upstream: 10.50.100.3
Flags: WC RP CACHE
Incoming Port: Vlan100-2/28,
Outgoing Ports: Vlan200-3/3, Vlan100-2/1,
Joined Ports: Vlan100-2/1,
Pruned Ports:
Leaf Ports: Vlan200-3/3,
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
  Entry   JP   RS  Assert
    164   13    0      0
VLAN-Id:   200   100
Join-P:     0   164
Assert:     0    0
-----
Src: 10.50.30.20  Grp: 239.100.100.100 RP: 3.3.3.3      Upstream: 10.50.100.3
Flags: SPT CACHE SG
Incoming Port: Vlan100-2/28,
Outgoing Ports: Vlan200-3/3, Vlan100-2/1,
Joined Ports: Vlan100-2/1,
Pruned Ports:
Leaf Ports: Vlan200-3/3,
Asserted Ports:
```

```

Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
  Entry   JP   RS   Assert
    165   14    0        0
VLAN-Id:   200   100
Join-P:     0   165
Assert:     0    0

8000-2:

=====
                          Pim Multicast Route
=====

Src: 0.0.0.0      Grp: 239.100.100.100 RP: 3.3.3.3      Upstream: 10.50.100.3
Flags: WC RP CACHE
Incoming Port: Vlan100-2/3,
Outgoing Ports: Vlan200-3/3, Vlan100-2/1,
Joined Ports: Vlan100-2/1,
Pruned Ports:
Leaf Ports: Vlan200-3/3,
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
  Entry   JP   RS   Assert
    163   13    0        0
VLAN-Id:   200   100
Join-P:     0   163
Assert:     0    0

-----

Src: 10.50.30.20  Grp: 239.100.100.100 RP: 3.3.3.3      Upstream: 10.50.100.3
Flags: SPT CACHE SG
Incoming Port: Vlan100-2/3,
Outgoing Ports: Vlan200-3/3, Vlan100-2/1,
Joined Ports: Vlan100-2/1,

```



```

Pruned   Ports:
Leaf     Ports: Vlan200-3/3,
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
  Entry   JP   RS   Assert
    164   14    0      0
VLAN-Id:   200   100
Join-P:     0   164
Assert:     0    0

8000-3:

=====
                          Pim Multicast Route
=====

Src: 0.0.0.0      Grp: 239.100.100.100 RP: 3.3.3.3      Upstream: NULL
Flags: WC RP CACHE
Incoming Port: Vlan0-2/1,
Outgoing Ports: Vlan100-2/1,2/28,
Joined   Ports: Vlan100-2/1, Vlan100-2/28,
Pruned   Ports:
Leaf     Ports:
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
  Entry   JP   RS   Assert
    163    0    0      0
VLAN-Id:   300   100
Join-P:     0   163
Assert:     0    0

-----
Src: 10.50.30.20  Grp: 239.100.100.100 RP: 3.3.3.3      Upstream: 10.50.30.2
Flags: SPT CACHE SG FWD_TO_DR

```

Incoming Port:	Vlan300-2/6,
Outgoing Ports:	Vlan300-2/1, Vlan100-2/1,2/28,
Joined Ports:	Vlan100-2/1, Vlan100-2/28,
Pruned Ports:	
Leaf Ports:	
Asserted Ports:	
Prune Pending Ports:	Vlan100-2/1,
Assert Winner Ifs:	
Assert Loser Ifs:	
TIMERS:	
Entry	JP RS Assert
200	13 0 0
VLAN-Id:	300 100
Join-P:	0 164
Assert:	0 0
<u>8000-4:</u>	
=====	
Pim Multicast Route	
=====	
Src: 0.0.0.0	Grp: 239.100.100.100 RP: 3.3.3.3 Upstream: 10.50.100.3
Flags:	WC RP CACHE
Incoming Port:	Vlan100-2/1,
Outgoing Ports:	Vlan100-2/3,2/28,
Joined Ports:	Vlan100-2/3, Vlan100-2/28,
Pruned Ports:	
Leaf Ports:	
Asserted Ports:	
Prune Pending Ports:	
Assert Winner Ifs:	
Assert Loser Ifs:	
TIMERS:	
Entry	JP RS Assert
163	13 0 0
VLAN-Id:	300 100
Join-P:	0 163
Assert:	0 0

```
-----
Src: 10.50.30.20   Grp: 239.100.100.100  RP: 3.3.3.3   Upstream: NULL
Flags: SPT CACHE SG
Incoming  Port: Vlan300-2/1,
Outgoing Ports: Vlan300-2/1, Vlan100-2/3,
Joined   Ports: Vlan300-2/1, Vlan100-2/3, Vlan100-2/28,
Pruned   Ports:
Leaf     Ports:
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
  Entry   JP    RS  Assert
    199     0   45      0
VLAN-Id:   300   100
Join-P:    164   164
Assert:     0    0
```



For each multicast group there needs to be two entries in the multicast route table, a wildcard entry (*,G) and a SPT entry (S,G). Without these entries a DR will not be able to join a Rendezvous Point Tree and subsequently the DR will not learn the source of the IPMC. Consequently a (S,G) entry will never occur and a SPT will never be formed.



The incoming ports (IIF) and outgoing ports (OIF) are determined by the RPF to either the RP or to the source.



The same information can also be viewed by using *show ip mroute route* and *show ip mroute next-hop* to indicate upstream multicast neighbor to either RPT or SPT; as determined by the RPF algorithm.

5.6 PIM-SM Static RP RSMLT Square/Mesh Design

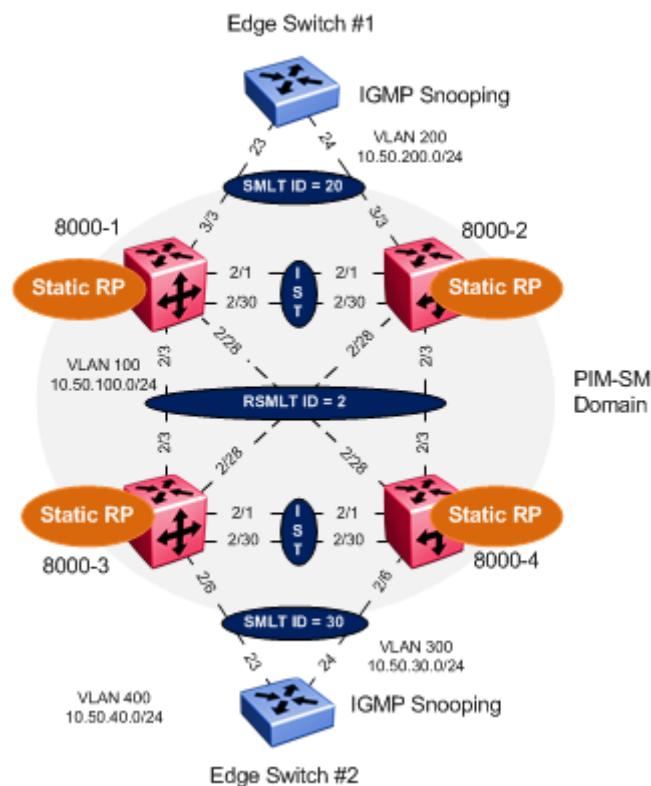


Figure 17: PIM-SM Static RP RSMLT Mesh Design

In this example the following will be configured as per Figure 17.

- IST
 - VLAN 2 is configured and associated to MLT#1
 - Tagging is enabled on ports 2/1,2/30
- VLACP and SLPP settings are configured as defined in the Switch Clustering using SMLT TCG
- SMLT ID 20: VLAN 200 (port 3/3) on switch Cluster #1
- SMLT ID 30: VLAN 300 (port 2/6) on Switch Cluster #2
- Core SMLT ID 2: VLAN 100 (ports 2/3 and 2/28)
- RSMLT Edge is enable on SMLT VLAN 200, 300
- RSMLT is enable on Core SMLT VLAN



RSMLT Edge support for resilient default gateway. The RSMLT peer IP and MAC address and VLAN information are stored in the ERS 8000 configuration files.



The RSMLT holddown timer should be set to 1.5x the IGP convergence time. With OSPF typical holddown time is 90 seconds. RSMLT Edge holdup timer should be set to 9999 (infinity) to allow the RSMLT peer nodes to forward indefinitely on behalf of each other.

CLIP/Loopback address are configured

- PIM-SM is enabled
- PIM-SM active mode on VLANs 200, 300 and 100
- PIM-SM active mode on IST VLAN 2



In order to achieve subsecond failovers/recoveries with PIM-SM, the IST VLAN and all VLANs associated with a SMLT should be configured in PIM active mode. All other VLANs not associated with either a SMLT or PIM adjacencies should be configured in passive mode.

- Mcast-smlt square-smlt flag is enabled



In a square/mesh design the smlt-square flag must be enabled. This flag provides faster recovery when a switch fails. A static route to the source, RP and BSR is created and used until the IGP converges and the recovered switch dynamic learns routes via IGP.

- Static RP is defined on each ERS 8000 for redundant RPs.



It is recommended that the RP is configured using a CLIP/Loopback address. This will prevent a RP failure if a VLAN interface goes down.

Recommended that the OSPF router ID is configured with the same CLIP/Loopback address for management simplicity.

- OSPF Area 0.0.0.0
- OSPF active mode is enabled on VLAN 100
- OSPF passive mode is enabled on VLAN 200, 300 and on the CLIP/Loopback address



The circuitless/loopback IP address must be reachable throughout the network. It is recommended that the CLIP/Loopback address is OSPF enabled. OSPF neighbors will learn the CLIP/Loopback address through OSPF.



It is recommended to make OSPF interfaces passive on VLANs extending to a L2 SMLT access switch. This will prevent adjacencies from forming at the access switches. In addition this will reduce the amount of OSPF control messages to the edge switches.

- On the Edge switches
- VLAN 200 and 300 are configured on switch 1 and 2 respectively
- MLT is configured on switch 1 and 2 respectively
- IGMP Snooping and proxy are configured on VLAN 200 and 300



It is always recommended to enable IGMP snooping and proxy on edge switches. IGMP snooping will ensure that all ports are not flooded with IPMC while proxy consolidates all MHR and sends one MHR to the IGMP Querier.

Three IPMC streams (239.100.50.100, 239.100.50.101, 239.100.50.102) are generated from a multicast source using either MC Hammer or Winsend located on switch #2. A multicast receiver for all three IPMC streams is located off switch #1.

Follow Steps 5.5.1.1 to 5.5.1.5 from the previous example PIM-SM with RSMLT Square/Mesh Design.

5.6.1 8000 SMLT Cluster

For this configuration example SMLT cluster 1 (8000-1 & 8000-2) are provisioned using ACLI while cluster 2 (8000-3 & 8000-4) are provisioned using CLI.

5.6.1.1 PIM

Cluster 1

8000-1: Step 1 – PIM global configuration

```
8000-1:5(config)#multicast smlt-square
8000-1:5(config)#ip pim enable
```

8000-2: Step 1 – PIM global configuration

```
8000-2:5(config)#multicast smlt-square
8000-2:5(config)#ip pim enable
```

8000-1: Step 2 – PIM interface configuration

```
8000-1:5(config)#interface vlan 2
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 100
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#exit
8000-1:5(config)#interface vlan 200
8000-1:5(config-if)#ip pim enable
8000-1:5(config-if)#exit
```

8000-2: Step 2 – PIM interface configuration

```
8000-2:5(config)#interface vlan 2
8000-2:5(config-if)#ip pim enable
8000-2:5(config-if)#exit
8000-2:5(config)#interface vlan 100
8000-2:5(config-if)#ip pim enable
8000-2:5(config-if)#exit
8000-2:5(config)#interface vlan 200
8000-2:5(config-if)#ip pim enable
8000-2:5(config-if)#exit
```

8000-1: Step 3 – PIM static rendezvous point configuration

```
8000-1:5(config)#interface loopback 1
8000-1:5(config-if)#ip pim
8000-1:5(config-if)#exit
8000-1:5(config)#ip pim static-rp
8000-1:5(config)#ip pim static-rp 239.100.0.0/16 1.1.1.1
8000-1:5(config)#ip pim static-rp 239.100.0.0/16 2.2.2.2
8000-1:5(config)#ip pim static-rp 239.100.0.0/16 3.3.3.3
8000-1:5(config)#ip pim static-rp 239.100.0.0/16 4.4.4.4
```

8000-2: Step 3 – PIM static rendezvous point configuration

```
8000-2:5(config)#interface loopback 1
8000-2:5(config-if)#ip pim
8000-2:5(config-if)#exit
8000-2:5(config)#ip pim static-rp
8000-2:5(config)#ip pim static-rp 239.100.0.0/16 1.1.1.1
8000-2:5(config)#ip pim static-rp 239.100.0.0/16 2.2.2.2
8000-2:5(config)#ip pim static-rp 239.100.0.0/16 3.3.3.3
8000-2:5(config)#ip pim static-rp 239.100.0.0/16 4.4.4.4
```

Cluster 2

8000-3: Step 1 – PIM global configuration

```
8000-3:5# config sys mcast-smlt square-smlt enable
8000-3:5# config ip pim enable
8000-3:5# config ip pim fast-joinprune enable
```

8000-4: Step 1 – PIM global configuration

```
8000-4:5# config sys mcast-smlt square-smlt enable
8000-4:5# config ip pim enable
8000-4:5# config ip pim fast-joinprune enable
```

8000-3: Step 2 – PIM interface configuration

```
8000-3:5# config vlan 2 ip pim enable
8000-3:5# config vlan 100 ip pim enable
8000-3:5# config vlan 300 ip pim enable
```

8000-4: Step 2 – PIM interface configuration

```
8000-4:5# config vlan 2 ip pim enable
```

```
8000-4:5# config vlan 100 ip pim enable
```

```
8000-4:5# config vlan 300 ip pim enable
```

8000-3: Step 3 – PIM static rendezvous point configuration

```
8000-3:5# config ip circuitless-ip-int 1 pim enable
```

```
8000-3:5# config ip pim static-rp enable
```

```
8000-3:5# config ip pim static-rp add grp 239.100.0.0 mask 255.255.0.0 rp 1.1.1.1
```

```
8000-3:5# config ip pim static-rp add grp 239.100.0.0 mask 255.255.0.0 rp 2.2.2.2
```

```
8000-3:5# config ip pim static-rp add grp 239.100.0.0 mask 255.255.0.0 rp 3.3.3.3
```

```
8000-3:5# config ip pim static-rp add grp 239.100.0.0 mask 255.255.0.0 rp 4.4.4.4
```

8000-4: Step 3 – PIM static rendezvous point configuration

```
8000-4:5# config ip circuitless-ip-int 1 pim enable
```

```
8000-4:5# config ip pim static-rp enable
```

```
8000-4:5# config ip pim static-rp add grp 239.100.0.0 mask 255.255.0.0 rp 1.1.1.1
```

```
8000-4:5# config ip pim static-rp add grp 239.100.0.0 mask 255.255.0.0 rp 2.2.2.2
```

```
8000-4:5# config ip pim static-rp add grp 239.100.0.0 mask 255.255.0.0 rp 3.3.3.3
```

```
8000-4:5# config ip pim static-rp add grp 239.100.0.0 mask 255.255.0.0 rp 4.4.4.4
```


6. Reference Documentation

Document Title	Publication Number	Description
Configuration — IP Multicast Routing Protocols Avaya Ethernet Routing Switch 8800/8600	NN46205-501	
Configuration — IP Multicast Routing Protocols Avaya Virtual Services Platform 9000	NN46250-504	
Configuration — IP Multicast Routing Protocols Ethernet Routing Switch 8300	NN46200-520	

7. Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

7.1 Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

7.2 Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

7.3 Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

7.4 Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.