Ethernet Routing Switch

8800 8600 8300 5000

Virtual Services Platform

7000 8000 9000

Engineering

> Switch Clustering using Split Multi-Link Trunking (SMLT) with VSP 9000, VSP 8000, VSP 7000, ERS 8600/8800, and ERS 5000 Technical Configuration Guide

Avaya Networking

Document Date: July 2014

Document Number: NN48500-518

Document Version: 6.0

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/ 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 document provides configuration procedures for Avaya's Split Multi-Link Trunking feature for the Virtual Services Platform 9000, 8000, and 7000 series and Ethernet Routing Switch 8800/8600, 8300, and 5000, and series.

Acronym Key

Throughout this guide the following acronyms will be used:

- DMLT: Distributed MultiLink Trunking
- ERS: Ethernet Routing Switch
- FDB: Forwarding Database
- IST: InterSwitch Trunk
- LACP: Link Aggregation Control Protocol
- MLT: MultiLink Trunking
- SMLT: Split MultiLink Trunking
- RSMLT: Routed Split MultiLink Trunking
- SLPP: Simple Loop Prevention Protocol
- SLT: Single Port Slit MultiLink Trunking
- STG: Spanning Tree Group
- VLACP: Virtual Link Aggregation Control Protocol
- VSP: Virtual Services Platform
- VRRP: Virtual Router Redundancy Protocol

Revision Control

March 2011 – Added recommendation to use MLT advance mode on edge Avaya stackable switches when used with ERS 8000 square/full mesh topologies for IP based traffic. Changed VSP CP Limit configuration from port level to MLT level. VRRP hold-down timers can be set in the ERS 5000 6.2 release.

June 4, 2009 – Corrections to Table 2 regarding 802.3ad support on the ERS 8300 and 5x00May 26, 2009 – Document title update and change made to remove VLACP MAC reference for ERS55xx at interface level.

August 14, 2008 – Made changes in reference to VRRP Hold-down timer and critical IP interface for the ERS 5000. Sections 1.3.2.6 and 2.6 have been updated.

February 25, 2008 – Changes to VLACP recommended values and support on ERS 8300. SLPP added on ERS 8300. Changes made to recommended FDB timers for SMLT VLANs. Add MLT port index command.

May 7, 2007 – Changes using two VLANs in RSMLT square or full mesh topology

February 1, 2011 – Add VSP 9000. Add configuration file for base SMLT configuration

March 26, 2012 – Add Loop Detection and Prevention section. Added SLPP Guard and VLACP Flap Detection and Damping information. Changed VSP 9000 configuration examples to include MSTP provisioning for the edge and core devices when connected to a VSP 9000 cluster.

July 29, 2013 – Addition of VSP 7000

July 29, 2014 – Addition of VSP 8000 and SLPP changes

Table of Contents

Figures

Tables

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. Introduction

The purpose of this Technical Configuration Guide is to provide configuration examples on various Avaya Ethernet Routing Switches (ERS) that support Split Multilink Trunking (SMLT). For a detailed overview on SMLT, please refer to the Switch Clustering Best Practices (NN48500-584). This document is intended for using SMLT using traditional Layer 2 switching and Layer 3 routing. For SMLT use with Shortest Path Bridging, please refer to the Shortest Path Bridging (802.1aq) Technical Configuration Guide (NN48500-617).

1.1 Software Levels

The configuration examples in this guide are based on the following minimum software levels.

Table 1: Minimum Software Levels for this TCG

Product	Minimum Software Level
VSP 9000	3.x
VSP 8000	4.x
VSP 7000	10.3
ERS 8600	5.1.x
ERS 8800	7.x
ERS 8300	4.2
ERS 5000	6.2

1.2 SMLT Features

The following displays the various SMLT options available for each Avaya switch that supports SMLT.

Table 2: SMLT Options

Feature	VSP 9000	VSP 8000	VSP 7000	ERS 8800/8600	ERS 8300	ERS 5000
Topologies						
Triangle	√	√	√	√	√	√
Square	√	√	√	√	√	√
Full Mesh	√	√	-	√	√	√
Aggregation						
MLT	√	√	√	√	√	√
802.3ad	√	√	√	√	√	√
Configuration Options						
SMLT	√	√	√	√	√	√
SLT	-	-	√	√	√	√
IST	√	-	√	√	√	√
vIST	-	√	-	-	-	-
Routing						
VRRP with Backup Master	√	√	√	√	√	√
RSMLT Edge	√	√	-	√		-
RSMLT	√	√	-	√		-
SMLT Protection Mechanisms						
CP-Limit	√	-	-	√	√	-
Ext CP-Limit	-	-	-	√	-	-
Loop Detect	√	√	-	√	-	-

SLPP	√	√	√	√	√	√
VLACP	√	√	√	√	√	√
Filter untagged Frames	√	√	√	√	√	√
Other						
Ping Snoop	-	-	-	√	√	-

Please note that for the VSP 8000 in the 4.0 release, a vIST is only supported over a Shortest Path Bridge (SPB) network. This means for non-SPB environments, you will still need to enable SPB on the two VSP 8000 cluster switches. The 4.0.1 release supports a simpltied vIST configuration for enviroments where SPB will not be deployed. With release 4.0.1, the vIST configuration is highly simplified where the SPB parameters are auto-configured and no explicit SPB parameters are required to be entered by the end user.

The VSP 8000 supports a CP Overload protection to protect the CP from overloading with packet processing. Traffic is limited to the CP based on the classified protocols for both non IP and IP packets.

1.3 SMLT Recommendations

1.3.1 SMLT Cluster

All configuration examples are based on the latest recommendations based on the software levels shown in table 1 above. Hence, this TCG will use the following settings for each configuration example.

Table 3: SMLT Recommendations

Feature	VSP 9000	VSP 8000	VSP 7000	ERS 8800/8600	ERS 8300	ERS 5000
Aggregation						
MLT	√	√	√	√	√	√
VLAN Tagging	√	√	√	√	√	√
STP disabled	√	√	√	√	√	√
SMLT Protection Mechanisms						
CP-Limit	√	-	-	√	√	-
Ext CP-Limit with Soft-down Option	-	-	-	√	-	-
SLPP	√	√	√	√	√	√
VLACP	√	√	√	√	√	√
Filter untagged Frames	√	√	√	√	√	√

It is recommended to use MLT in place of 802.3ad as it provides faster recovery. The fastest possible recovery with 802.3ad would be around 1.5 second's compared to less than one second with MLT. If you wish or need to enable 802.3ad, please refer to the document number NN48500-502 (Technical Configuration Guide for Link Aggregation Control Protocol (LACP) 802.3ad and VLACP) for more details.

It is recommended to use the reserved multicast MAC address of 01:80:c2:00:00:0f for the VLACP MAC address for all Ethernet applications. This does not apply if you use an Ethernet over a LAN Extension service where it is recommended to use the default VLACP MAC.

It is recommended to use a SLPP receive threshold of 5 on the primary switch and a value of 50 on the secondary switch in an SMLT cluster. However, depending on the number of VLANs tagged across a trunk, the SLPP receive threshold on the primary switch may have to be increased from the recommended value of 5. A value of 5, for example, works fine on the primary switch for a couple of VLANs.

It is recommended to enable Ext CP-Limit with the soft-down option when using software release 4.1 or higher. The hard-down option should only be used as a loop prevention mechanism in software release 3.7.x.

ERS 5510's do not support both Filter Untagged Frames and VLACP simultaneously

1.3.2 Recommended Values

The following information provides the suggested recommended value for each feature.

Configuration values are always left to the discretion of the user. The values called out in this doc are Avaya recommendations, which the user may wish to alter for their particular network and network needs. The values Avaya recommends have been tested and known to work. If the values are altered and issues are experienced, depending upon the situation, it is suggested to use the recommended values shown in this section.

1.3.2.1 Feature Summary

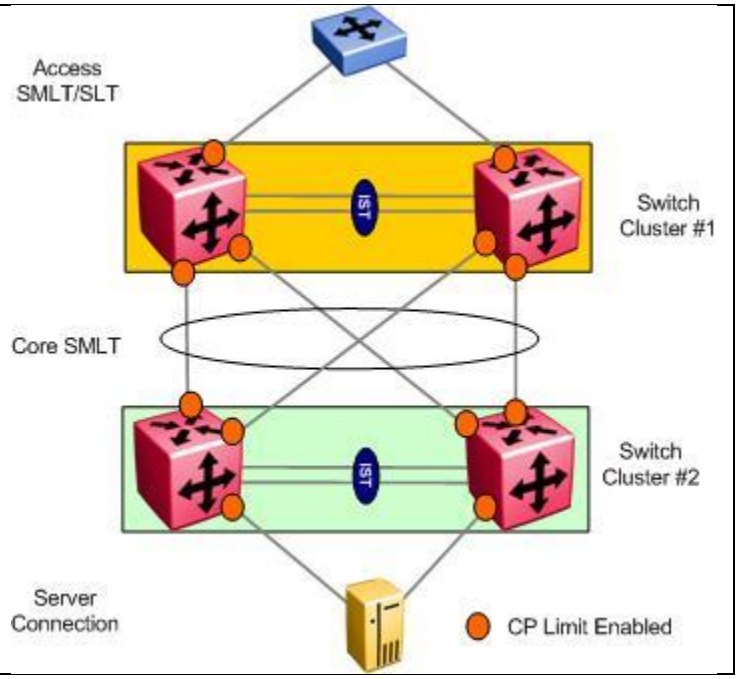
Table 4: Feature Summary

Hardware Platform	CP Limit	Ext CP Limit	SLPP	VLACP
VSP 9000	Yes	N/A	Yes	Yes
VSP 8000	N/A	N/A	Yes	Yes
VSP 7000	N/A	N/A	Yes	Yes
ERS 8800	Yes	Yes	Yes	Yes
ERS 8300	Yes	N/A	Yes	Yes
ERS 5000	N/A	N/A	Yes	Yes

1.3.2.2 CP Limit

Table 5: CP Limit Recommended Values

CP Limit Values		
	Broadcast	**Multicast**
Aggressive		
Access SMLT/SLT	1000	1000
Server	2500	2500
Core SMLT	7500	7500
Moderate		
Access SMLT/SLT	2500	2500
Server	5000	5000
Core SMLT	9000	9000
Relaxed		
Access SMLT/SLT	4000	4000
Server	7000	7000
Core SMLT	10000	10000

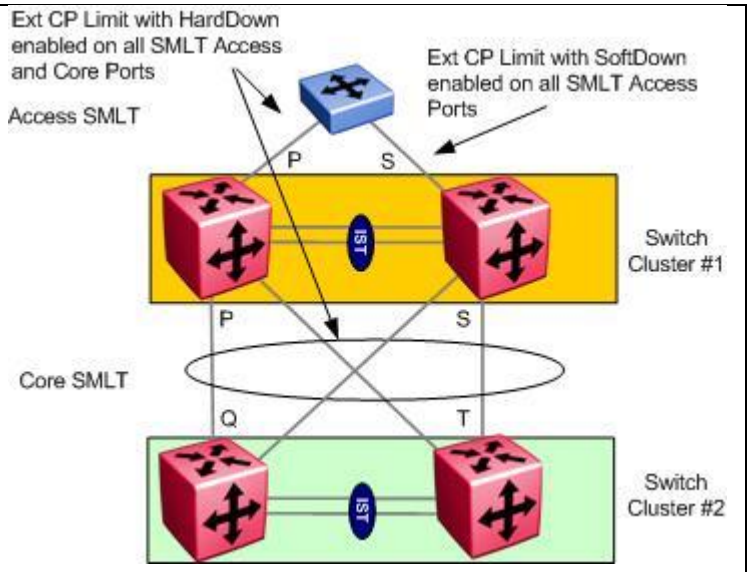


CP Limit protects against control broadcast and multicast traffic destined to the CPU. If the defined rate is exceeded, the corresponding port is shut down and you need to disable and then re-enable the port to recover. CP Limit does not protect against user data traffic nor again traffic types such as SNMP, telnet, ICMP, IP with TLL 1, Unknown SA, etc. It is only supported on the VSP 9000, ERS 8300 and ERS 8800/8600.

1.3.2.3 Ext CP Limit

Table 6: Ext CP Limit Recommended Values

SoftDown – use with 4.1 or higher	
Setting	**Value**
Maximum Ports	5
Minimum Congestion Time	3 seconds (default)
Port Congestion Time	5 seconds (default)
CP Limit Utilization Rate	Dependent on network traffic
HardDown – use wth 3.7	
Maximum Ports	5
Minimum Congestion Time	P = 4,000ms S = 70,000ms T = 140,000ms Q = 210,000ms
Port Congestion Time	P = 4 Sec. S = 70 Sec. T = 140 Sec. Q = 210 Sec.



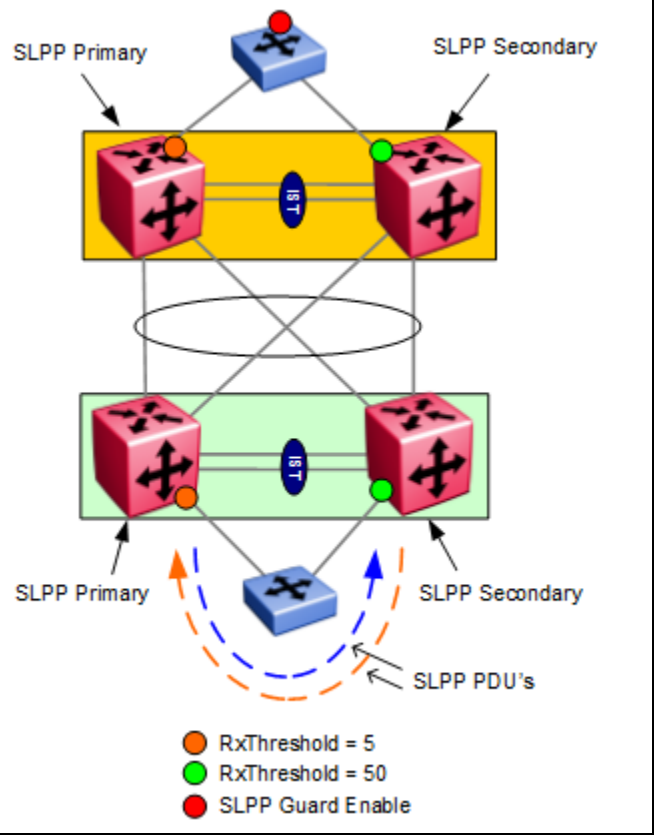
Primary (P) – primary target for convergence, Secondary (S) – secondary target for convergence
Tertiary (T) – third target for convergence, Quaternary (Q) – fourth target for convergence
Note : Ext CP Limit HardDown option is not recommended for software release 4.1 or later. This option should only be used when SLPP is not available.

Can be used in conjunction with CP Limit and expands the ability of CP Limit by monitoring buffer congestion on the CPU and port level congestion on the I/O modules. Like CP Limit, it does not look at user data packets. This feature is only available on the ERS 8800/8600 and if the recommended SoftDown option is enabled, the maximum number of I/O ports that can be monitored is 5.

1.3.2.4 SLPP – Bridge Core

Table 7: SLPP Recommended Values for Bridge Core

	Settings
Enable SLPP	
Access SMLT	Yes
Access SLT	Yes
IST	No
Primary Switch	
Packet Rx Threshold Edge Ports	5*
Transmission Interval	Default (500ms)
Ethertype	Default
Secondary Switch	
Packet Rx Threshold Edge Ports	50
Packet Rx Threshold Core Ports	Disable
Transmission Interval	Default (500ms)
Ethertype	Default
Edge Switch	
SLPP Guard	Enable
Timeout	0



* This number may have to be increased depending on the number of VLANs tagged across a trunk interface. For example, the recommended value of 5 works fine for one or two tagged VLANs.

SLPP is used to detect loops and shut down the appropriate port(s) where the loop is detected. SLPP operates by sending SLPP-PDU's where a loop is detected if the SLPP-PDU is received either on the same switch that originated the PDU's or on the peer switch. SLPP is configured on a per VLAN and port basis

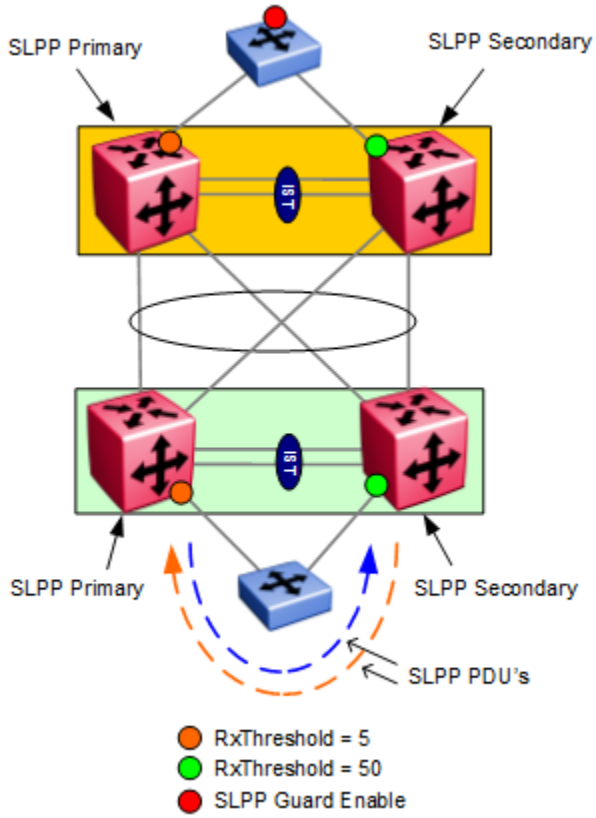
As the number of VLANs running SLPP scale off of a specific uplink port, the Rx-threshold value may need to be increased to prevent complete isolation of the offending edge. Critical to note is that the primary goal of SLPP is to protect the core at all costs. In certain loop conditions, what may occur is the secondary switch also detecting the loop and its SLPP Rx-threshold is reached before the primary can stop the loop by taking its port down. Therefore, both switches eventually take their ports down and the edge becomes isolated. The larger the number of VLANs associated with the port, the more likely this could occur, especially for loop conditions that affect all VLANs. The recommended step here is to increase the Rx-threshold on the secondary only.

As a guideline, when the number of edge VLANs off of a specific uplink exceeds 10, increase the secondary Rx-threshold to 100.

1.3.2.5 SLPP – Routed Core

Table 8: SLPP Recommended Values for Routed Core

	Settings
Enable SLPP	
Access SMLT	Yes
Access SLT	Yes
IST	No
Primary Switch	
Packet Rx Threshold Edge Ports	5*
Packet Rx Threshold Core Ports	5
Transmission Interval	Default (500ms)
Ethertype	Default
Secondary Switch	
Packet Rx Threshold Edge Ports	50
Packet Rx Threshold Core Ports	50
Transmission Interval	Default (500ms)
Ethertype	Default
Edge Switch	
SLPP Guard	Enable
Timeout	0



* This number may have to be increased depending on the number of VLANs tagged across a trunk interface. For example, the recommended value of 5 works fine for a couple of tagged VLANs.

1.3.2.6 SLPP Guard – Edge Switch

The Switch Clustering implementations on the VSP9000, ERS 8000, VSP 7000, and ERS 5000 sends a Simple Loop Prevention Protocol (SLPP) packet which helps to prevent loops occurring when Switch Clustering is implemented. In some customer environments there is a need to provide additional loop protection when used in combination with Avaya's Switch Clustering (SMLT). SLPP-guard helps prevent loops in customer's networks by administratively disabling an edge port if they received a SLPP packet. SLPP is necessary because SMLT requires that STP/MSTP/RSTP is not enabled on links to the switch performing switch clustering.

In some networks due to moves, adds or changes, it could be possible to create a loop within the customers networks by connecting an edge port back to a port of the switch cluster. When operational, SLPP-guard will immediately administratively disable a port when a SLPP packet is received on a port and generate a local log message, syslog message (if the syslog server(s) are configured) and SNMP traps (if SNMP tap receivers are configured).

Each port has its own administrative hold-down timer:

- When the port is shutdown due to reception of a SLPP packet the timer should start for that port.
- When the timer reaches the configured interval, the port is re-enabled and a local log message, syslog message (if the syslog server(s) are configured) and SNMP traps (if SNMP tap receivers are configured).
- This timer is user configurable between 10 seconds and 65535 seconds, with 60 seconds set as the default. The port timer is disabled if it is configured as 0, which means the port will be disabled until an administrator re-enabled the port.
- The default SLPP Ethertype is (hex): 0x8102, though on some switches it has used an old value of 0x8104.
    - You can globally configure the EtherType for SLPP guard
- The admin state of the port which has been disabled due to SLPP-guard will not be saved across switch reboots, ACG or other activities.
    - The show interface verbose commands has been enhanced to show if the port BPDU Filtering and SLPP-guard status are enabled

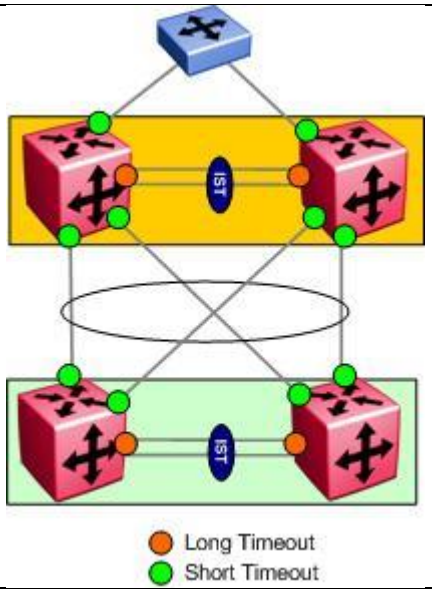
SLPP Guard is available on the following switches:

- ERS 3500: Release 5.2 or higher
- ERS 4000: Release 5.5 or higher
- ERS 5000: Release 6.2.3 or higher
- VSP 7000: Release 10.3 or higher

1.3.2.7 VLACP

Table 9: VLACP Recommended Values

Parameter	Setting
SMLT Access	
Timeout	Short
Timer	500ms
Timeout Scale	5
VLACP MAC	01:80:C2:00:00:0F
SMLT Core	
Timeout	Short
Timer	500ms
Timeout Scale	5
VLACP MAC	01:80:C2:00:00:0F
IST	
Timeout	Long
Timer	10000
Timeout Scale	3
VLACP MAC	01:80:C2:00:00:0F



To use Fast Periodic Timers of less than 200ms between ERS 8800/8600, either a SuperMezz module must be present or 8895SF must be used.

VLACP is used to detect end-to-end link failures on direct point-to-point interfaces. This is accomplished by each switch transmitting VLACP PDU's at a set timer interval in order for a link to maintain a 'link-up' state. For all direct connected point-to-point links, use the reserved multicast MAC address of 01:80:c2:00:00:0f. For end-to-end connections traversing intermediate networks, use the default VLACP MAC address 01:80:c2:00:11:00.

The ERS 8800 beginning in release 7.1.3 introduced VLACP flap detection and damping. VLACP flap detection and damping extends the port flap damping feature to VLACP and is used to automatically shut down selected VLACP links until a network administrator is able to resolve the root cause of the VLACP flapping. VLACP flap detect and damping does not support auto-recovery, therefore a network administrator must re-enable the interface manually.

When enabled, VLACP flap detect and damping shuts off a selected VLACP link if the interface flaps a specified number of times within a user-defined time frame. For example, VLACP flap detect and damping is configured, by default, to detect 3 events within a 60 second time frame. On detection of the first event, the VLACP flap timer is started and counts off how many VLACP events occur within 60 seconds. If the number of events reaches 3 before the end of the timer, the flapping interface is shut down, the timer stops and returns to 0, and the system generates a trap and log.

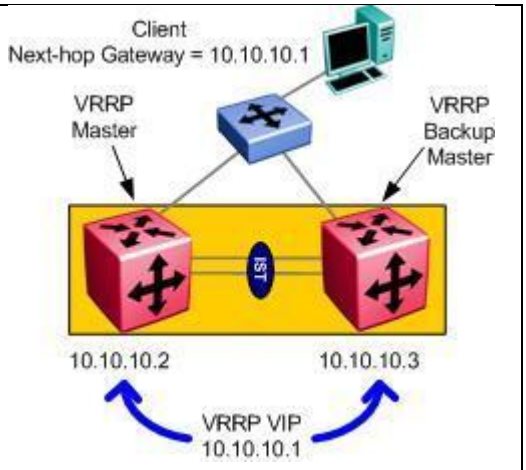
VLACP flap detect and damping is disabled by default, and should only be enabled after consultation with Avaya Client Services. Although there is some interaction with existing LACP link flap functionality, Avaya recommends that you do not use the VLACP flap dampening feature on an LACP-enabled interface.

For the VSP 7000 only, it is recommended to not enable VLACP on the IST port members if SPB is also enabled on the IST.

1.3.2.8 VRRP Backup Master

Table 10: VRRP Backup Master Recommended Values

Item	Configuration
VRRP VIP Guidelines	Do not use the physical IP address of VLAN as VRRP address. Always use three IP addresses, two VLAN physical and one virtual
Backup Master	Enable
VRRP Master	Define the SMLT Primary switch as the master by increasing the VRRP priority with a value higher than the default setting of 100.
DHCP	If you enable DHCP Relay, use the VLAN physical address and not the VRRP virtual IP address
Advertise Interval	10 Seconds
Hold-down Timer	60 seconds Note 1



Note 1: This value should be set to 0 seconds for the ERS 5000 only; please see note below

If there are multiple VLANs being utilized with VRRP enabled, it is recommended to stagger the VRRP Master such that both SMLT cluster switches are VRRP Master for half the VLANs.

The VRRP hold-down timer and critical IP interface should not be used in reference to the ERS 5000 only. Please see CR Q01737679 in the 5.1 release notes for the ERS 5000 (NN47200-400). In reference to the ERS 5000 only, if VRRP is used, Avaya recommends that:

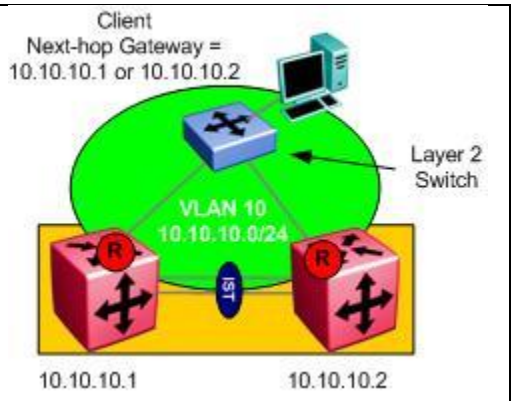
1. VRRP Backup Master should be enabled on both SMLT cluster switches
2. Critical IP functionality should be disabled
3. VRRP Holddown-Timer should be set to 0
4. Customers should upgrade to a code level of 5.0.7 or 5.1.0 or higher as a separate bug (Q1733378) present in 5.0.3 and 5.0.6 code may inappropriately send traffic across the IST causing it to drop

Critical IP should NOT be used with VRRP Backup Master. There are known issues when using this feature with VRRP Backup Master.

1.3.2.9 RSMLT Edge

Table 11: RSMLT Edge Recommended Values

Parameter/Item	Setting/Configuration
Hold-up Timer	Infinity (9999)
IP Address	Any IP address can be used on the Primary or Secondary switch as long as they are different. It is suggested to use a.b.c.1 for the primary and a.b.c.2 for secondary switch
IGP Interface Type	It is recommended to not send IGP updates/hello on the RSMLT edge ports; i.e. use OSPF passive interface.
RSMLT-edge	RSMLT-edge should be enabled which in turn stores the peer's MAC/IP address pair in its local configuration file and restores the configuration if the peer does not restore as a simultaneous reboot of both RSMLT peer switches



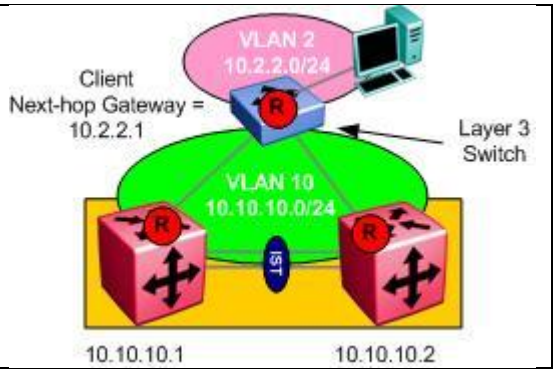
As an alternative to VRRP with Backup Master, RSMLT Edge can be used for Layer 2 connectivity to an Edge. This feature allows both SMLT cluster switches to forward traffic on behalf of the other. Also, it scales beyond the VRRP limit of only 255 instances. Please note that VRRP and RSMLT Edge should not be enabled on the same VLAN and when RSMLT Edge is configured, the configuration file must be saved in order to store the peer's MAC address.

Please remember to save the configuration when RSMLT Edge is configured. This step is required in order the save the peer MAC address.

1.3.2.10 RSMLT

Table 12: RSMLT Recommended Values

Parameter/Item	Setting/Configuration
Hold-up Timer	At least 1.5 times greater than the routing protocol convergence time. Leave default setting of 180 seconds
Hold-down Timer	At least 1.5 times greater than the routing protocol convergence time. Leave default setting of 60 seconds.

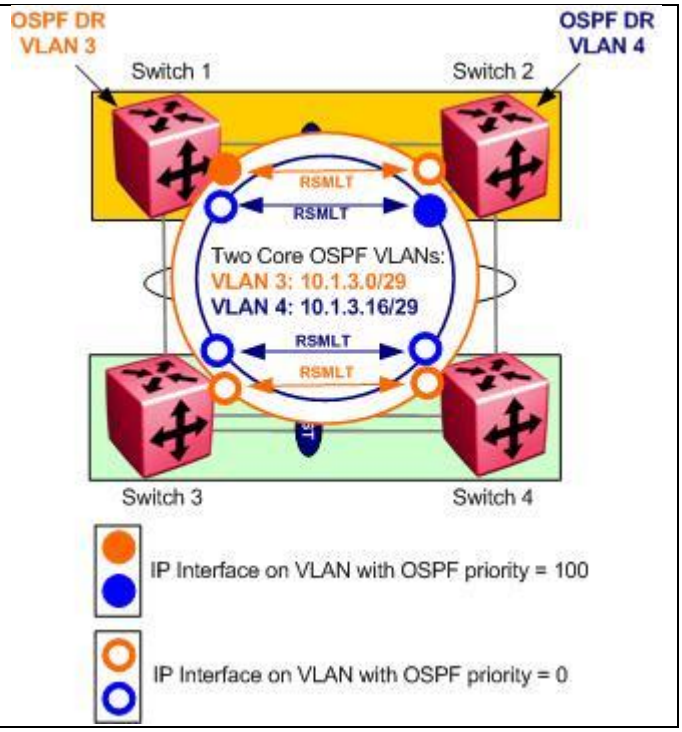


If the Edge switch supports Layer 3, RSMLT can be enabled. RSMLT provides sub-second failover without having to modify any layer 3 routing protocol timers. There is no requirement to use VRRP or ECMP on the Edge VLAN to load-balance traffic to both SMLT peer switches.

1.3.2.11 RSMLT Dual Core with OSPF

Table 13: RSMLT Recommended Values

Parameter/Item	Setting/Configuration
Hold-up Timer	At least 1.5 times greater than the routing protocol convergence time. Leave default setting of 180 seconds
Hold-down Timer	At least 1.5 times greater than the routing protocol convergence time. Leave default setting of 60 seconds.
OSPF DR Priority – Core VLAN A	
Switch 1	100
Switch 2	0
Switch 3	0
Switch 4	0
OSPF DR Priority – Core VLAN B	
Switch 1	100
Switch 2	0
Switch 3	0
Switch 4	0

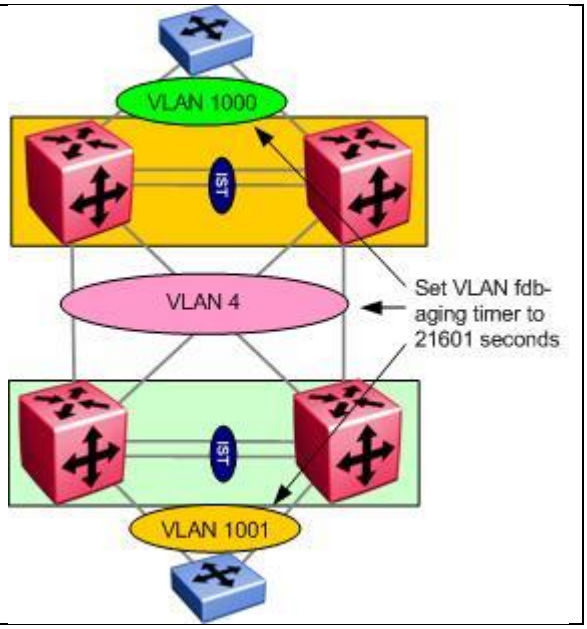


RSMLT can be used with multiple VLANs in the core to provide sub-second failover for routed VLAN traffic using any type of IGP protocol such as OSPF or RIP. There is no requirement to use VRRP or ECMP in the core VLANs. Square of Full Mesh topologies are supported in the core. If OSPF is used in the core, it is recommended to run two SPF instances via two separate VLANs. The reason for this recommendation is in the event of losing an OSPF designated router (DR). Normally, if a DR is lost, a traffic interruption of up to 10 seconds could occur in reference to the ERS 8600/8800. By creating a second OSPF core VLAN and configuring the DR as outlined above, sub-second recover will occur similar to Layer 2 SMLT operation.

It is recommended to use low slot numbers for the MLT ports used in the core between the two SMLT clusters when running OSPF with RSMLT. The reason for this is because CP generated traffic is always sent out on the lowered numbered ports when active.

1.3.2.12 VLAN FDB Aging Timer for SMLT VLANs

Table 14: VLAN FDB Aging Timer for SMLT VLANs

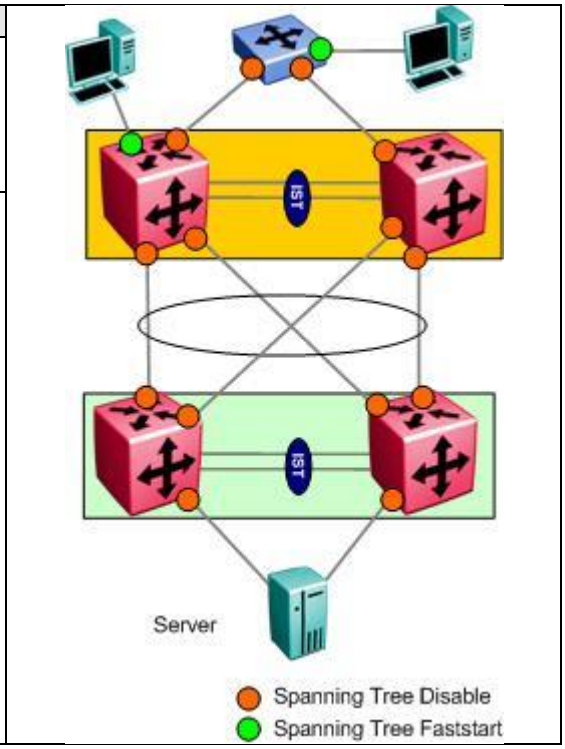
Parameter/Item	Setting/Configuration	
Fdb-entry aging-timer	One second higher than system ARP aging timer or 21601 seconds	

Please note that only for the ERS 5000, VSP 8000, VSP 9000, and VSP 7000, the FBD aging timer should be left at the default setting of 300 seconds. The recommended value of 21601 seconds only applies to the ERS 8800/8600, 8300, or 1600.

1.3.2.13 Spanning Tree Recommendations

Table 15: Spanning Tree Recommendations

Parameter/Item	Setting/Configuration
Spanning Tree Learning on SMLT Cluster switches	Disabled on all SMLT, SLT, and IST port members on SMTL cluster switches. Fast start learning enabled on all other ports.
Spanning Tree learning on Edge switches	Disabled on all uplink aggregation ports on Edge switches to SMLT cluster switches. Fast start learning enabled on all other ports.



Spanning Tree is automatically disabled on all IST, SMLT, and SLT ports when using a VSP 9000, VSP 7000, ERS 8800/8600, ERS 5000, ERS 8300, or ERS 1600 switch.

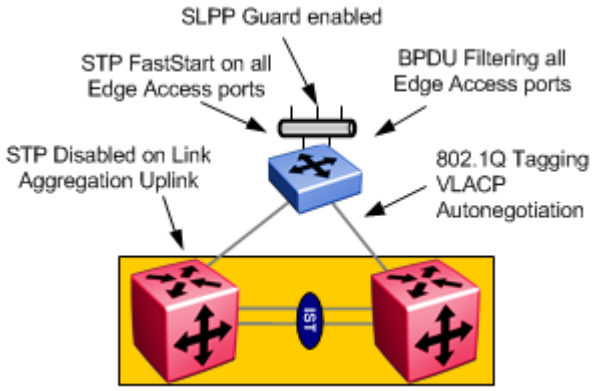
MSTP is the default spanning tree protocol on the VSP 9000 and VSP 8000.

1.3.2.14 Edge Access Switch Recommendations

In regards to the access switch that connects to a SMLT Cluster, the following items should be enabled or used.

Table 16: Edge Access Switch Recommendations

Feature	Uplink Ports to SMLT Cluster	Access ports for Users
STP	Disable on all MLT uplink ports	Enable STP FastStart or MSTP edge-port
VLACP	Enable with Short Timers if available	No
BPDU Filtering	No	Enable with timer set to infinity (set to 0) when available
VLAN Tagging	Always enable	When needed
MLT[1]	Advance Mode if ERS 8000 core	N/A
Autoneg	Enable	Enable
DHCP Snooping	No	Yes (when DHCP is used)
ARP Inspection[1]	No	Yes (when DHCP is used)
IP Source Guard / Reverse Path Check[2]	No[3]	Yes
SLPP Guard	No	Yes



[1]In an ERS 8000 or VSP 9000 RSMLT square/full mesh core topology, Avaya recommends to set the MLT algorithm on Avaya edge stackable switches to advance for IP based traffic. Tests has proven that this will increase overall global throughput over the default MLT setting of basic.

[2]Dymanic ARP Inspection and IP Source Guard use the binding table create by DHCP Snooping, hence, in order to use these features, DHCP Snooping must be enabled. IP Source Guard should not be enabled on uplink ports from the Edge to the Core and should only be enabled on the Edge access ports (untrusted ports) where DHCP Snooping and Dynamic ARP Inspection are enabled.

[3]In an ERS 8000 RSMLT Cluster, if you wish to enable Reverse Path Check, please select “exist-only” and only enable Reverse Path Checking with Edge switches with known IP routes. For unknown routes, i.e. routes learned from the Internet, it is recommended to disable Reverse Path Check on the ERS 8000 cluster switches.

1.3.2.15 MLT Scaling and ID Recommendations

Table 17: MLT/SMLT/SLT Scaling Capabilities

Switch Model	Links per MLT Group	MLT Groups per Switch or Stack	MLT-based SMLT Groups			Port-based SLT Groups		
			Copper	Fiber (1GbE)	Fiber (10GbE)	Copper	Fiber (1GbE)	Fiber (10GbE)
VSP 9000	16	512*	511*	511*	511*	N/A**	N/A&**	N/A**
VSP 8000	8	84	83	83	83	N/A	N/A	N/A
VSP 7000	8	64	63	63	63	256	256	256
ERS 8800	8	128	127	127	127	382	238	22
ERS 8300	4	31	30	30	30	382	398	67
ERS 5000	8	32	31	31	31	398	190	62

* The number of MLT groups that the VSP 9000 supports is limited to the number of ports in the chassis. In Release 3.0, the maximum number of 1GbE ports is 480, and the maximum number of 10GbE ports is 240.

** The VSP 9000 does not support port based SLT, however, a single port can be assigned to a MLT-based SMLT group.

*** The number of MLT group will increase to 64 in the 10.3 software release.

1.3.2.16 SMLT ID Recommended Values

Table 18: SMLT ID Recommended Values

Switch Model	Software Version	MLT-based SMLT ID's	Port-based SLT ID's
VSP 9000	3.0 and higher	1-512	MLT-ID's 1-512
VSP 8000	4.0 and higher	1-48	MLT-ID's 1-48
VSP 7000	10.2 and higher 10.3 and higher	1-32 1-64**	33-512 65-512**
ERS 8800	4.1 and higher	1-128	129-512
ERS 8300	3.0 and higher	1-31	32-512
ERS 5000	5.0 and higher	1-32	33-512

* The VSP 9000 does not support port based SLT, however, a single port can be assigned to a MLT-based SMLT group.

** The number of MLT group will increase to 64 in the 10.3 software release. Hence, it is recommended to start the SLT numbering at 65.

1.4 VSP 7000

SMLT was introduced in the 10.2 release for the VSP 7000 via the front ports only. Two stacks of 8 switches each for a total of 16 switches could be deployed in a dToR supporting up to 512 10GE ports as shown in figure 1 below. The 10.2 release also introduced rear port mode. By default, the rear ports are in stacking mode. Rear port mode configures the VSP 7000 Fabric Interconnect (FI) ports on the rear of the chassis for use as 40 Gbps Avaya interface ports. In the 10.2 release, only SPB is supported in rear port mode and only in standalone mode. In summary, the 10.2 release supported the following:

- SMLT Standalone & Stack-mode Distributed Fabric Interconnect Stacking
- SMLT: square & triangle topology
- SMLT: SLPP & VRRP Backup Master
- SMLT: LACP over SMLT (SMLT with LAGs)

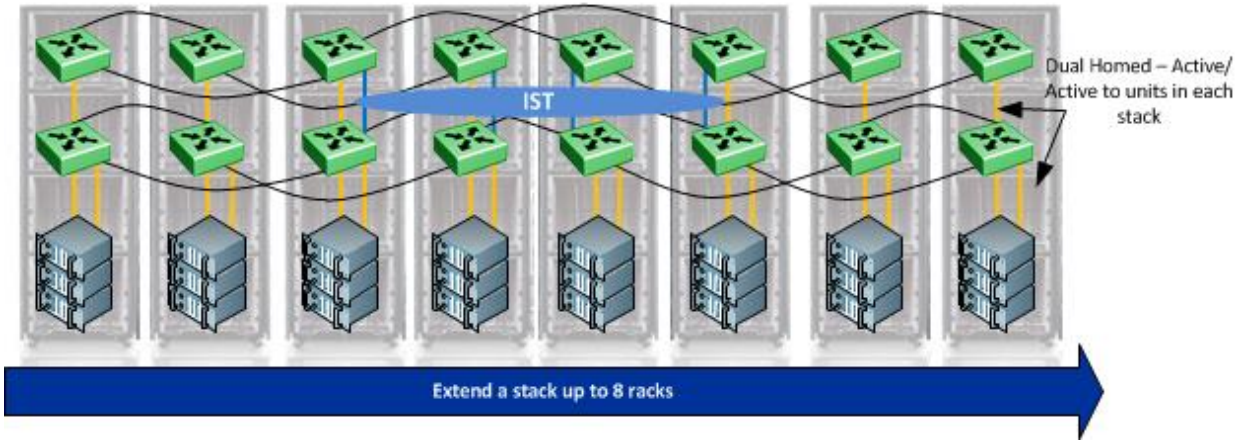


Figure 1: VSP 7000 Stacking and SMLT

In the 10.2.1 release, SPB or SMLT is supported on the rear ports. If rear port is enabled, it can operate in either standard mode supporting SMLT or in SPB mode but not both at the same time – this will be supported in the 13.0 release. If rear mode is enabled in standard mode, one can take advantage of the high-speed rear ports for both an IST link and SMLT/SLT links to another VSP 7000 without having to resort to using expensive front port SFP+ modules and fiber cabling. If the rear port mode is provisioned for Shortest Path Bridging (SPB), the 10.2.1 supports a stack of two with a full stack of 8 supported in the 10.3 release.

In the 10.2.1 release, the following extra features where added:

- Switch Clusting in Rear-Port mode (SMLT over rear port mode)
  - SPB and switch clustering together in rear-port mode are not supported
- Switch Clustering and Dynamic Routing Interoperability
  - OSPF only
  - Standalone only
  - No support for rear port mode
  - 16 OSPF interfaces/16 adjacencies
  - 1 OSPF area
  - 2K routes; 1K ARPs

- No ECMP
- 16 VRRP instances
- 16 SMLTs/SLTs
- 16 K MAC address

1.4.1 Rear Ports

The diagram show the FI port speeds available depending if Standard or SPB operational state is enabled.

To provide greater plug n 'play capability over the virtual ports when rear-port mode is enabled, LACP link aggregation and VLAN tagging are automatically enabled. This ensures that multiple virtual ports which may run within a single cable or if multiple FI cables are run in parallel that all virtual ports are automatically treated as one link. This simplifies any protocol adjacency such as IS-IS or OSPF. When you issue rear-ports mode all virtual ports will have their LACP state set to true, and the LACP Admin Key to 4095.

Color	Physical Fabric Interconnect Port	Rear Port Mode	Throughput	Ports
Black	FI Up (right) Top	Standard	240Gbps	34, 35, 36
		SPB	240Gbps	
Red	FI Down (left) Top	Standard	240Gbps	38, 39, 40
		SPB	160Gbps	38, 39
Blue	FI Up (right) Bottom	Standard	80Gbps	33
		SPB	80Gbps	
Blue	FI Down (left) Bottom	Standard	80Gbps	37

In FI mesh, it is recommended to connect "like" color fabrics interconnect ports together, i.e. red port to an adjacent switch red port to get maximum possible throughput. You can connect any color ports together, i.e. a red port to a blue port, however, the port speed will drop to the lower of two ports.

In rear-port SPB operational state, virtual port 40 is not available. Hence, the red port is reduced to 160Gbps.

In rear port mode, the front panel *Up* and *Down* LEDs blink in a quick pattern (125ms) to indicate rear-port mode is operational.

In the 10.2 release, only SPB is officially supported in rear port SPB mode. 10.2.1 supports SMLT via rear port Standard mode.

Also note that LACP is enabled by default on all rear ports. When you enabled rear port mode, the following applies:

- VLAN tagging for rear ports is set to tagAll.
- The LACP administration key is set to 4095.
- The LACP operating mode for rear ports is set to active.
- The LACP rear ports time-out value is set to short.
- LACP for rear ports is set to enable.

SMLT or IST over rear port Raw-mode is supported in Feature Pack Release 10.2.1. You must disable the default LACP mode before you can enable an IST or SMLT on a rear port.

For the VSP 7000, if Shortest Path Bridging (SPB) is enabled, it is important to not enable the *filter-untagged-frame* option on the IST port members. Also, the default PVID of all IST ports must be the primary B-VLAN ID. This will happen automatically providing SPB is enabled first prior to enabling the IST.

1.5 Simplified vIST – VSP 8000

As noted above in section 1.2, software release 4.0.1 introduces simplied vIST configuration for environments where SPB will not be used. Even though SPB is still required for a vIST, the simplied vIST configuration hides the entire SPB configuration from the user. All the SPB configuration parameters are auto-configured where only one MLT will be designated as the vIST MLT.

To enable simpltied vIST, two items needs to be set at the boot flag and MLT levels:

```
VSP8284(config)#no boot config flags spbm-config-mode

** After you change the above boot flag, you must save your configuration and
reset the switch. Then configure the IST VLAN and MLT the same as you would,
for example, as the VSP 9000. Then enable the simplied vIST setting using the
following command on the IST MLT you plan to use.

VSP8284(config)#interface mlt x

VSP8284(config-if)#virtual-ist enable
```

Overall, the simplied vIST setting will automatically use the following settings:

- The *auto-configured* SPBM values are shown below :

```
spbm

spbm ethertype  : 0x8100
```

- VLAN to I-SID mapping of all existing VLANs and new VLANS created.

```
Vlan i-sid <value> → Where ISID-ID is same as VLAN-ID
```

- ISIS and SPBM

```
router isis

spbm <instance ID> → Auto-configured value 1

is-type L1

manual-area xx.xxxx → Auto-Configured Value : 49

sys-name → Auto-Configured to use System Prompt

spbm <instance> b-vid <primary-vlan-id, secondary-vlan-id> primary <primary-
vlan-id>
        Auto-Configured Primary BVLAN ID : 4086
        Auto-Configured Secondary BVLAN ID : 4087

vlan create <primary-vlan-id> type spbm-bvlan (4086)

vlan create <secondary-vlan-id> type spbm-bvlan (4087)

system-id <xxxx.xxxx.xxxx>
        Auto-Configured value derived from V-IST VLAN ip address.
        If IP address is 10.8.1.1, then system-id is 00:00:0a:08:01:01

spbm <instance> nick-name <x.xx.xx>
        Auto-Configured value for nick-name is derived from System-ID
        If system-id is 00:00:0a:08:01:01 , then nick-name 8.01.01

spbm <instance> smlt-peer-system-id  <xxxx.xxxx.xxxx>
```

```
        Auto-Configured value for smlt-peer-system-id is derived from V-IST
        VLAN Peer IP address.

        If peer IP address is 10.8.1.2, then smlt-peer-system-id is
        00:00:0a:08:01:02

virtual-bmac<xx:xx:xx:xx:xx:xx>

        Virtual-bmac is auto-derived as –

        Higher of {system-id, smlt peer system id} +1

Enable cfm-spbm globally

        Auto configure with cfm-spbm-level 4

        Auto configure with cfm-spbm-MEP ID 1

router isis enable
```

- The Interface level ISIS parameters are auto-configured

```
interface mlt <x>
isis
isis spbm <instance>  - default instance is 1
isis enable
exit
```

1.5.1 Simplified vIST Configuration – VSP 8000

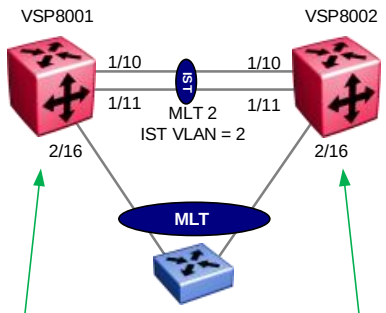
```
#
# BOOT CONFIGURATION
#
no boot config flags spbm-config-mode
# end boot flags

#
# CLI CONFIGURATION
#
prompt "VSP8001"

#
# MLT CONFIGURATION
#
mlt 2 enable name "IST"
mlt 2 member 1/10-1/11
mlt 2 encapsulation dot1q

#
# VLAN CONFIGURATION
#
vlan create 2 type port-mstprstp 0
vlan members 10 1/10-1/11
interface Vlan 2
ip address 10.8.80.1 255.255.255.252
exit

#
# VIRTUAL IST CONFIGURATION
#
virtual-ist peer-ip 10.8.80.2 vlan 2
```




```
#
# BOOT CONFIGURATION
#
no boot config flags spbm-config-mode
# end boot flags

#
# CLI CONFIGURATION
#
prompt "VSP8001"

#
# MLT CONFIGURATION
#
mlt 2 enable name "IST"
mlt 2 member 1/10-1/11
mlt 2 encapsulation dot1q

#
# VLAN CONFIGURATION
#
vlan create 2 type port-mstprstp 0
vlan members 10 1/10-1/11
interface Vlan 2
ip address 10.8.80.2 255.255.255.252
exit

#
# VIRTUAL IST CONFIGURATION
#
virtual-ist peer-ip 10.8.80.1 vlan 2
```

```
VSP8001:1#show isis spbm
=============================================================
SPBM       B-VID      PRIMARY    NICK     LSDB     IP
INSTANCE              VLAN       NAME     TRAP
-------------------------------------------------------------
1          4086-4087  4086       8.50.01  disable  disable

ISIS SPBM SMLT Info
=============================================================
SPBM       SMLT-SPLIT-BEB  SMLT-VIRTUAL-BMAC  SMLT-PEER-SYSTEM-ID
INSTANCE
-------------------------------------------------------------
1          primary         00:00:0a:08:50:04    0000.0a08.5002
                            (10.8.80.4)          (10.8.80.2)
```

```
VSP8002:1#show isis spbm
=============================================================
SPBM       B-VID      PRIMARY    NICK     LSDB     IP
INSTANCE              VLAN       NAME     TRAP
-------------------------------------------------------------
1          4086-4087  4086       8.50.02  disable  disable

ISIS SPBM SMLT Info
=============================================================
SPBM       SMLT-SPLIT-BEB  SMLT-VIRTUAL-BMAC  SMLT-PEER-SYSTEM-ID
INSTANCE
-------------------------------------------------------------
1          primary         00:00:0a:08:50:04    0000.0a08.5001
                            (10.8.80.4)          (10.8.80.1)
```

1.6 Loop Detection and Prevention

1.6.1 IST/SMLT Loop Prevention Mechanisms

IST/SMLT setups are exposed to looping broadcast/multicast packets as by default they have no loop detection or prevention mechanisms because the intention is to use all possible links for best throughput and maximum load sharing. The design assumes that no loops exist and no links need to be withdrawn from the forwarding of traffic.

If for any particular reason a loop is introduced in the network the results are potentially more serious than in normal Spanning Tree designs that typically with all default settings will revert back to a loop free network.

Not only will the looping multicast and broadcast packets be flooded to all attached end stations and limit their throughput and cause additional CPU load, the flooded packets are likely monitored by the CPU of all network devices and may cause the CPU to be busy with packet processing. Other network control frames might be dropped due to network congestion. This might lead to results such as VRRP switchover, OSPF neighbor loss, IST loss and communication outage of end devices.

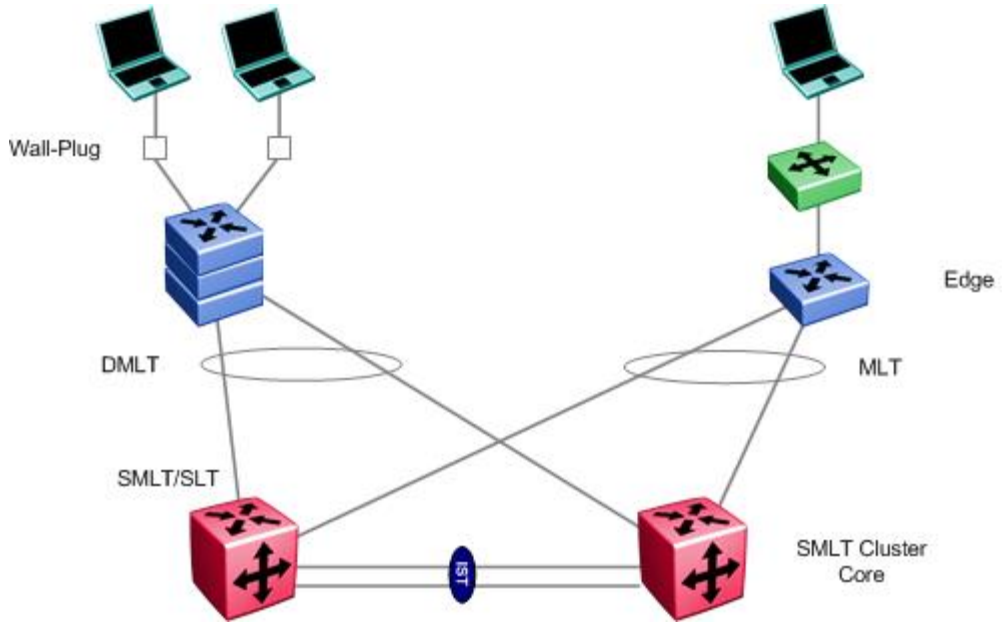
With the wide deployment of IST/SMLT designs several configuration optimizations and protocols have been developed to detect and prevent loops in the networks. These methods include the internal prioritization of certain important traffic, the introduction of SLPP and extended CP-Limit and the usage of Spanning Tree with BPDU filtering and SLPP Guard at the edge.

The load sharing and better redundancy together with sub-second failover typically out weight the additional configuration of preventing loops in the network.

Broadcast or Multicast packets may only infinitely loop in layer 2 networks, if the packets pass layer 3 devices (which only happens for a small amount of eligible packets) the TTL is decremented and the packets stop looping after the TTL has reached 0. Layer-2 looping packets will affect all devices attached to the particular VLAN. Therefore it is recommended not to span VLANs over the whole network but to terminate the VLANs with a layer 3 instance at a useful location. In 3-tier networks the distribution layer would ideally terminate the VLAN from the edge and then use layer 3 to the core layer.

Most of the loops are created at the edge – not in the core – as typically the edge is reconfigured and re-cabled more often and end-users tend to introduce more issues than network support person working in the core.

The following diagram shows a typical setup in an IST/SMLT design towards the edge.

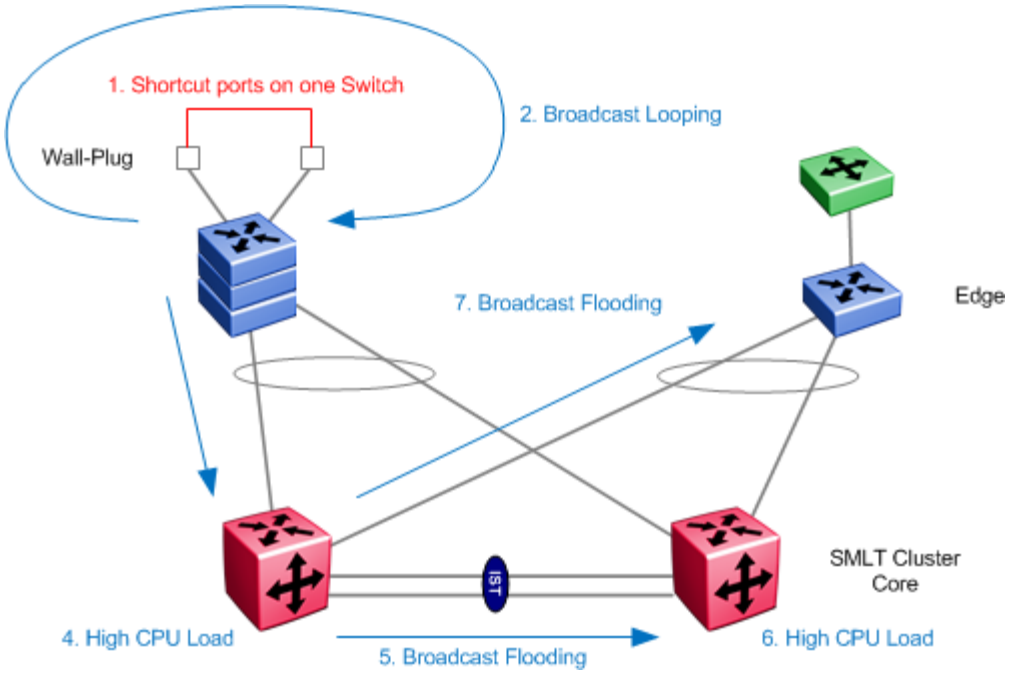


A general recommendation to avoid larger outages while breaking network loops is that the loops should be prevented/broken as close as possible to the source. If a loop was created at an edge switch, it is more useful to disable the affected edge switch ports than to cut links between core and edge.

1.6.1.1 Loop on an Edge Switch – Two Ports Connected

A loop at an edge switch might be created by simply short circuit two wall-plugs with a cable. This is in fact connecting two switch ports directly – however users typically don't have direct access to the switch.

Results of the described loop are seen immediately when the first Broadcast (e.g. ARP) or Multicast (e.g. VRRP) packet is sent into the VLAN that is configured on the two short circuited ports. The packet will be transmitted on all ports and will be received on the short circuited ports, again flooded and transmitted infinitely. As the connected ports have negotiated the maximum speed the looping packets could travel at a rate of 1 Gbps overrunning all 100 and 10 Mbps ports of the same VLAN. These packets will also travel along the SMLT links to the core devices causing a high CPU load with all the related problems.



This scenario is not specific to IST/SMLT but it may cause the IST/SMLT to fail due to the high CPU load.

1.6.1.1.1 Solution: Spanning Tree

An easy method to prevent these types of loops is to enable Spanning Tree on all edge ports. Whenever the link on the edge is coming up, Spanning Tree will send a BPDU and will receive it on the short circuited port. This self-generated BPDU will cause one of the ports to go into blocking mode, breaking the loop permanently. While the port is in blocking mode BPDUs are still sent and the existence of the loop is recognized.

To allow end devices to get online as fast as possible (to avoid DHCP timeouts with normal Spanning Tree requiring 30 sec to go through listening and learning states) the Spanning Tree “faststart” should be enabled. The faststart would open the port immediately but go through the normal state machine of Spanning Tree as soon as a BPDU is received. BPDUs are always sent normally – so a loop would be detected.

Configuration

ACLI – Stackable Switch

```
conf t
interface FastEthernet ALL
! enable Spanning Tree with Faststart Option
spanning-tree port 1-24 learning fast
exit
```

1.6.1.1.2 Solution: Spanning Tree BPDU Filtering

In addition to Spanning Tree Avaya recommends using BPDU filtering. The feature disables a port immediately when a Spanning Tree BPDU is received. As edge devices such as PCs or printers would not participate in Spanning Tree and therefore will not generate their own BPDUs - an edge port should normally never receive a BPDU except if a switch is connected to this port or an invalid connection to another switch or a port of the same switch exists.

Disabling the port permanently on which such a BPDU is received is the recommended configuration. It is possible to auto-enable the port by default but as in most cases the root cause is not resolved, the port will keep toggling. Obviously as BPDU filtering can only react if a BPDU is received - all other edge ports need to have Spanning Tree enabled to send out BPDUs. It does not matter if these ports are configured for faststart or not – they will send the BPDUs normally.

When a port has BPDU-Filtering enabled and it receives an STP BPDU, the following actions take place:

- the port is immediately put in the operational disabled state
- a trap is generated and the following log message is written to the log

```
BPDU received on port with BPDUFiltering enabled Port <x> has been disabled
```

- the port timer starts
- the port stays in the operational disabled state until the port timer expires, if the timeout is set to 0 the port remains disabled until manual intervention to re-enable it

BPDU filtering is configurable on the Avaya devices

- ERS 2500 with release 4.2
- ERS 3500 with release 5.0
- ERS 4000 with release 5.1
- ERS 5500 with release 5.1
- ERS 5600 with release 6.0
- ERS 8300 with release 4.2
- ERS 8000 with release 7.0
- VSP 7000 with release 10.1

Configuration

ACLI – Stackable Switch

```
config t
interface FastEthernet 1
! the command options
spanning-tree bpdu-filtering ?
! enable Spanning-tree bpdu-filtering enable
! port Set port(s) to apply BPDU filtering settings
! timeout Spanning-tree bpdu-filtering timeout (in seconds)
! enabling the BPDU filtering
```

```
spanning-tree bpdu-filtering enable
! if a timeout is configured the port will get active again after the timer
expired
! if the problem is not resolved the port may constantly go down/up
spanning-tree bpdu-filtering timeout 120


show spann bpdu-filtering
!Port Trunk Admin Oper Link LinkTrap Timeout TimerCount BpduFiltering
!---- ----- ------- ---- ---- -------- ---------- ---------- -------------
!1 Enable Up Up Enabled 120 0 Enabled
```

1.6.1.1.3 Solution: Rate Limiting

On edge switches it is possible to configure a limit for incoming Multicast and Broadcast packets. If there is a loop only a certain number of packets would be accepted and forwarded – the network could survive even in case where the loop breaking mechanisms would kick in too late.

The rate limiting can also successfully prevent attacks with high rates of Broadcasts or Multicasts sent into the network by viruses where loop detection mechanisms would not apply.

The settings for rate limiting are specific for every network but on an edge port that is not working with Multicast or Broadcast (e.g. a Multicast sender) a rate of 100 packets per second should never be reached.

Enabling the rate limit can potentially prevent the CP-limit in the core devices to be hit but if the Multicast or Broadcast storm is generated due to a loop the other loop detect mechanisms should disable the affected ports.

The configuration for broadcast rate limiting will also be applied for all packets that are destined to an unknown Unicast address.

Configuration:

ACLI – Stackable Switch

```
conf t
interface FastEthernet 2
! the rate limiting options
rate-limit ?
! both Set rate limiting for both multicast and broadcast packets
! broadcast Set rate limiting for broadcast packets
! multicast Set rate limiting for multicast packets
! port Select port for operation
rate-limit both ?
! <0-10> percent
! percent Change rate-limit in percent
! pps Change rate-limit in pps
! configure the rate-limit in packets per second
```

```
rate-limit both pps 100
exit
! to review the configuration
show rate-limit
! Port Packet Type Limit Last 5 Minutes Last Hour Last 24 Hours
! ---- ----------- ------------- -------------- --------- -------------
! 1 Both None 1.0% 1.0% 0.6%
! 2 Both 100 pkts/sec 0.0% 0.0% 0.0%
! 3 Both None 0.0% 0.0% 0.0%
```

The configuration of Rate Limiting in packets per second is only possible on the ACLI and has been introduced on the 5500 with 5.0.8 and 5.1.2.

When the rate limit is not available in packets per second the percentage should be used.

When using NLB (Microsoft Network Load Balancing) the NLB servers should not be located on the same segment as the clients where rate limiting is configured on the ports. The performance might be severely affected as the destination MAC address is either an unknown Unicast Address (Unicast NLB) or a Multicast address (Multicast and IGMP multicast NLB).

1.6.1.1.4 Alternative Solutions

Most of the short circuits are introduced with 1:1 cables – as users typically do not use cross-over cables.

Older switches would not bring links up when TX and RX are not crossed; modern switches typically autosense the TX/RX pairs along with auto-negotiation. If autonegotiation is disabled (by configuring a fixed speed or duplex setting on the port) typically auto-MDI/MDIX is disabled and only cross-over cables can introduce the short circuit between the links. Normally users don't have cross-over cables available therefore it is less likely to introduce problems.

That seems to imply disabling auto-negotiation could be useful for loop prevention but it usually introduces more performance related issues – therefore the recommendation is to keep auto-negotiation enabled despite the risk of having ports short circuited.

The problem only happens when the transmitted packets can enter the same VLAN on the receiving port. Unused ports should therefore be disabled or removed from the VLANs. At least all ports should be taken out from the default VLAN 1.

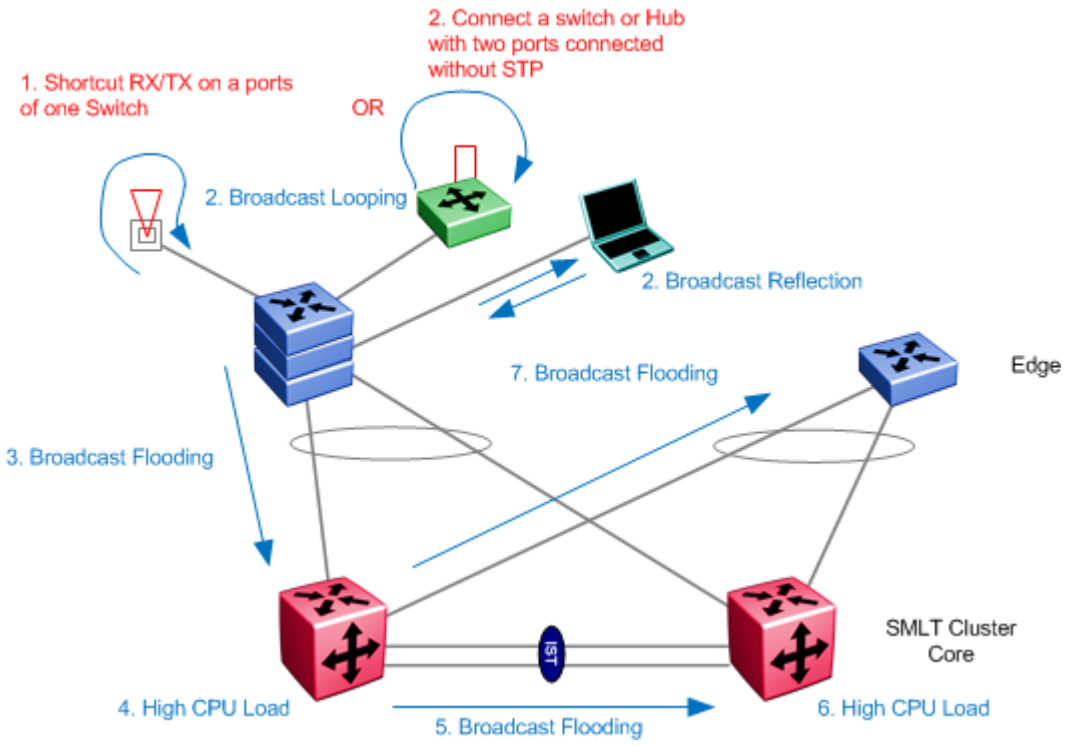
Solutions on the core switches will be reviewed in later sections. These solutions will detect the problem as well but may shut down core ports and may eventually isolate the edge switch completely. Therefore they should only be used in conjunction with the edge solutions.

1.6.1.2 Loop on an Edge Switch – One Port RX-TX Short Circuit

Another loop might be introduced at the edge switch if Broadcast or Multicast frames that are sent out on a port are received back on the same port. There are three main sources of this behavior.

1. The physical or logical cabling returns the transmitted frames directly onto the receiving wires of the same port. Though this looks very unusual in the first place it can have some valid reasons but are typically not end-user caused:
   - a fiber patch cord that has been looped back for measuring and was never disconnected
   - an Ethernet connection of a service provider is looped back for measuring or accidently
   - a loopback connector has been connected to a port
   - the customer is using type 1 cabling with Balun connectors that connect TX and RX when no PC is connected
2. Another switch with two ports shortened is connected to the network infrastructure switch. These devices are often introduced by end-users to connect additional equipment in the offices. Depending on their capabilities the switches or hubs might either be able to take part in Spanning Tree by sending their own BPDUs, they may forward BPDUs transparently or - in the worst case - drop BPDUs.

   If the connected device takes part in Spanning Tree it may - depending on its Bridge priority and the MAC address - become the new root bridge of a segment and therefore lead to communication outages when being connected and disconnected. Bridge priorities of regular network device should therefore be configured manually to lower values (the closer to the core the lower).
3. A device may reflect packets directly back to the sending switch. The device might either work incorrectly or could be configured to reflect packets. Possible configurations are port mirroring or loopback testing.



This behavior again is not specific to IST/SMLT setups but may impact the IST/SMLT stability.

1.6.1.2.1 Solution: Spanning Tree

The solution to avoid the local loopback is again a Spanning Tree configuration on the edge ports. The protocol will detect its own generated BPDUs and will put the port into blocking mode until the loop is cleared.

As described before Spanning Tree “faststart” should be enabled for immediate device connectivity.

Interestingly the situation cannot be resolved with Rapid Spanning Tree or Multiple Spanning Tree (8012.1s/w) as these are ignoring self-generated BPDUs per definition.

Quote from 802.1w standard: "If the Bridge Identifier and Port Identifier both match the values that would be transmitted in a BPDU from this Port, then the BPDU is discarded, in order to prevent processing of the Port's own BPDUs; for example, if they are received by the Port as a result of a loopback condition."

As for workarounds, applying BPDU filtering on the port (with timeout = 10sec) seems to do the trick nicely. If a loopback is applied to the port, RSTP will still take 30secs to make the port Forwarding (unless it is configured to be an Edge port...); with BPDU Filtering the port is immediately shutdown after the 1st BPDU is sent; then after 10secs the port is re-opened; and so on. The port never makes it into Forwarding.

Also a message is logged every time; this can be a good thing or annoying, but as this situation (having loopback applied to port) would be an error condition so the messages are valuable to have.

1.6.1.2.2 Solution: Spanning Tree BPDU Filtering

In the reviewed setups all sent packets are immediately returned to the sending switch including the self-generated BPDUs. These BPDUS can be used to trigger the BPDU filtering function described in the last scenario.

The BPDU filter will also prevent users to connect their own switches into the network that are not under control of the network management authority. When such a switch is connected to the network – most of the small switches use the Spanning Tree protocol – the BPDU filtering will disable the edge port. The user will have to call the network administration for re-enabling the port and can be fined.

1.6.1.2.3 Solution: Rate Limiting

To minimize the effects on the network if the loop detection mechanism such as Spanning Tree or BPDU filtering cannot find the problem (e.g. if the connected switch is looping the packets back but is filtering Spanning Tree BPDUs) rate limiting can at least reduce the number of flooded Broadcast and Multicast packets that hit other network devices. The loop may be then detected by other protocols without the risk for the network.

1.6.1.2.4 SLPP Guard

If SLPP is enabled on the SMLT Cluster core, SLPP Guard should also be enabled on all access ports switch on Edge Switch. When operational, SLPP-guard will immediately administratively disable a port when a SLPP packet is received on a port and generate a local log message, syslog message (if the syslog server(s) are configured) and SNMP traps (if SNMP tap receivers are configured).

SLPP-guard is available on the ERS 4000 starting in release 5.5.

1.6.1.2.5 Alternative Solutions

In most of the scenarios above the packet is immediately returned when being sent. If the port is configured for half duplex this would result in a collision and the packet would be discarded.

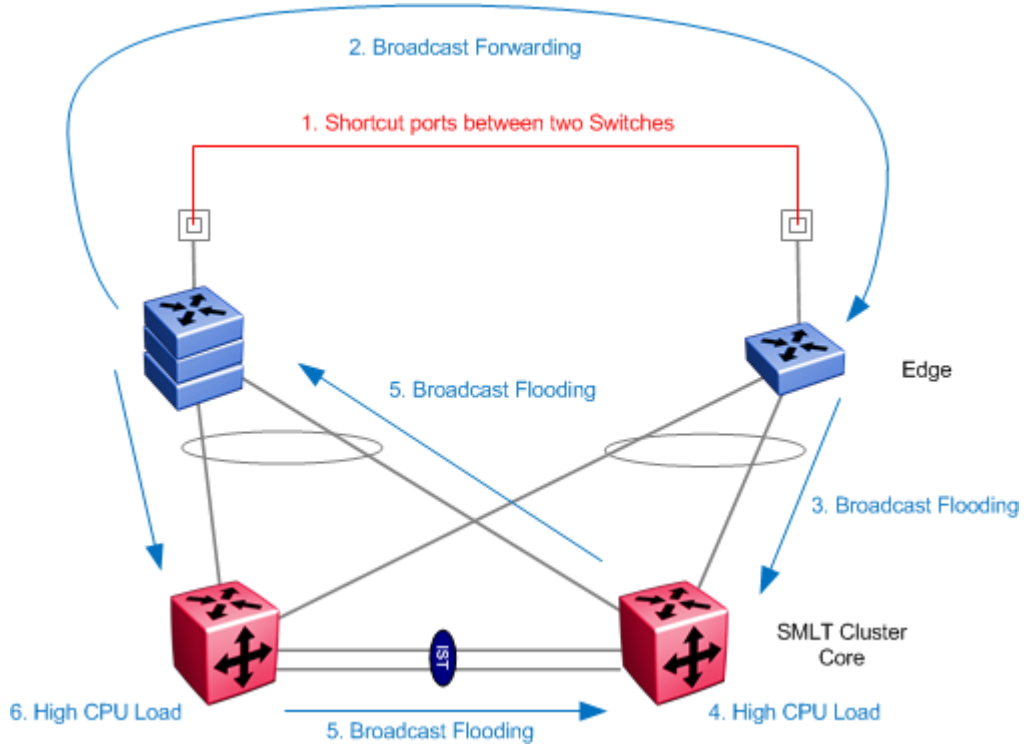
The other alternative is to use CANA to disallow all the full-duplex modes. This way there can never be a loopback loop as the frame cannot be sent and received at the same time.

Avaya however recommends auto-negotiation to achieve the best possible throughput and avoid duplex mismatches.

Solutions on the core switches will be reviewed in later sections.

1.6.1.3 Loop Between Edge Switches – Link Between Two Switches

Depending on the location of the edge switches or the cabling to wall plugs it sometimes happens that neighboring wall plugs are terminated at different edge switches. If a user would short circuit these two switches or the patching is done incorrectly - packets are sent out on one switch entering the neighboring switch. If the packets are Broadcasts or Multicasts and the ports are using the same VLAN the packets will be flooded to the core and back to the originating edge switch which will send it over the invalid link causing an infinite loop.



This problem is specific to IST/SMLT setup. In regular Spanning Tree setups the additional link is invoked into the Spanning Tree path calculation (if Spanning Tree is enabled on the ports) and one of the links will be blocked. In IST/SMLT environments Spanning Tree is disabled on the SMLT and IST links (a design requirement), therefore the BPDUs would be dropped on these ports and the loop cannot be detected.

1.6.1.3.1 Solution: Spanning Tree BPDU Filtering

Even if normal Spanning Tree is unable to detect the loop because the core switches are not involved in the Spanning Tree process all edge ports should be configured for Spanning Tree faststart. They will therefore send BPDUs when they come up and with regular intervals.

BPDU filtering on the incorrectly connected ports will detect the bad connection and disable the port until manual intervention.

If BPDU filtering is not available it might be required to use alternative loop detect mechanisms or rely on the core based detection mechanisms.

1.6.1.3.2 Solution: Rate Limiting

Like in all previous scenarios the rate limiting on the edge ports is a useful method to prevent negative impacts onto the network if a loop cannot be detected or is detected too late.

1.6.1.3.3 SLPP Guard

If SLPP is enabled on the SMLT Cluster core, SLPP Guard should also be enabled on all access ports switch on Edge Switch. When operational, SLPP-guard will immediately administratively disable a port when a SLPP packet is received on a port and generate a local log message, syslog message (if the syslog server(s) are configured) and SNMP traps (if SNMP tap receivers are configured).

SLPP-guard is available on the ERS 4000 starting in release 5.5.

1.6.1.3.4 Alternative Solutions

To result in a loop - the packets sent from one switch need to enter the same VLAN on the neighboring switch. If the VLAN assignment is different the packet could be routed and might cause a routing loop which will however not loop infinitely but only until the TTL is expired.

If the VLANs per switch are different (every switch or stack uses its own set of unique VLANs) and VLAN 1 is disabled a layer 2 loop can be avoided. BPDU filtering however would still work if the VLANs are different and detect the incorrect connection.

In reality it might not be possible to have unique VLANs per edge switch as this requires more IP networks/subnetworks and increases the VLANs on the core switches.

Solutions on the core switches will be reviewed in later sections.

1.6.1.4 Edge Switch (MLT) Packet Reflection

Under certain circumstances packets sent from the core switch to the edge on the SMLT ports may travel back to the core port without facing one of the previously covered cases – violating the MLT rules not to send packets back onto an MLT where the packet was received on.

Though it is no full loop the behavior can cause significant problems in the forwarding database letting MAC entries point to incorrect SMLT ports.

The root cause of these “half-loops” can be:

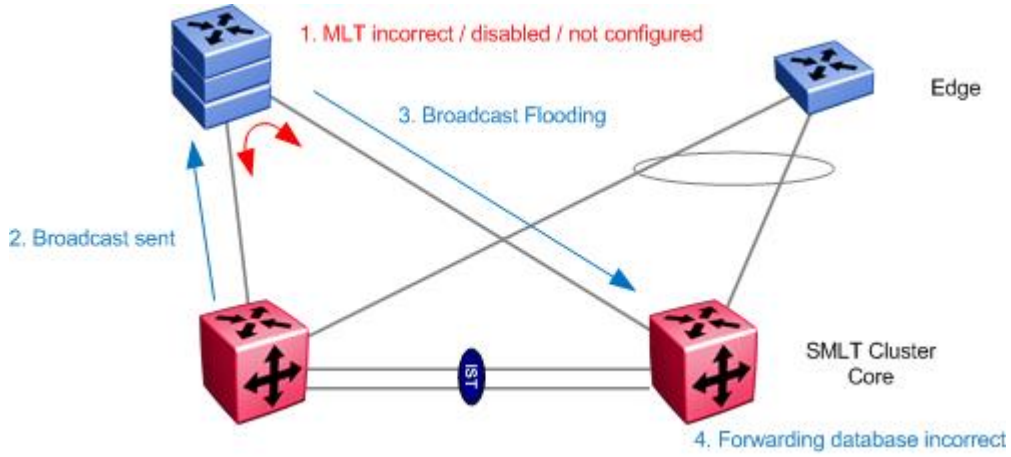
- a miss-configured MLT at the edge,
- MLT not created (or disabled) at the edge but links are plugged in anyway,
- MLT configuration is lost (switch set back to factory default)
- incorrect cabling at core or edge

The most common situation that may cause a reflection of packets on the edge MLT uplinks - is when the edge switch comes up with a default/empty configuration. This might happen due to an incorrect configuration, a corrupt config file or file storage or a power failure while the config was save manually or automatically.

One has to realize that if an edge switch is running in stack mode and has a number of units in the stack - the binary config file could be up to 8 MByte and it may take some time saving it. When saving is done automatically the config is saved at least one minute after a config change was done. If - during this

saving process - the power was interrupted the switch will restart with an all default config this means without any MLT enabled.

Broadcast and Multicast packets that are sent from the core to the edge are flooded onto all ports of the default VLAN 1 and are received by the IST peer switch from the SMLT.



1.6.1.4.1 Solution: Tagging on SMLT/MLT Links, Discard Untagged Frames.

If the packet reflection was caused by a reset to the default config the edge switch will send all packets untagged (in VLAN 1) back to the core. To avoid the core switch to accept these packets the port only needs to discard untagged packets (given that all valid packets are tagged).

The configuration of all VLANs tagged across links between active network components (even if there is only a single VLAN configured on the link) and discarding of untagged frames also reduces possible problems of incorrect patching or cabling between network components. Frames cannot be forwarded into other – incorrect VLANs when untagged frames are not accepted as the VLAN assignment will then only be done for correctly tagged frames.

Configuration:

ACLI
`config t` `vlan ports 1/1-6 tagging tagAll filter-untagged-frame enable filter-unregistered-frames enable`
CLI

`config`
`ethernet 1/1-1/8 perform-tagging enable`
`ethernet 1/1-1/8 untagged-frames-discard enable`

1.6.1.4.2 Solution: VLACP

If the edge switch was reset to default and is therefore reflecting packets back onto the SMLT links other configuration options would also be lost.

The Virtual Link Aggregation Control Protocol (VLACP) can be used to detect the presence of the same protocol on the remote site – if the protocol is not configured the link will kept down logically.

Originally developed to monitor the end to end connectivity of provider links - it will send out Multicast frames to the remote/peering VLACP network device and expects to receive packets from this device. If these link control packets are not received the link is declared to be down.

Obviously an un-configured edge switch is not sending VLACP packets to the core, therefore the core will not use the links towards the edge switch and packets cannot be reflected.

Configuration:

ACLI – Assuming ERS 5000

```
#enable VLACP globally
vlacp enable
vlacp macaddress 180.c200.f
#configure VLACP on ports
interface fastEthernet 47-48
vlacp fast-periodic-time 500
vlacp timeout short
vlacp port timeout-scale 5
vlacp enable
exit
#show vlacp global info
5510-48T#show vlacp
================================================================================
                          Vlacp Global Information
================================================================================
                  Multicast address :  01:80:c2:00:00:0f
                  Vlacp             :  enabled
                  Vlacp hold time   :  0
5510-48T#
#show vlacp interface info
5510-48T#show vlacp interface 47-48
================================================================================
                           VLACP Information
================================================================================
PORT ADMIN   OPER    HAVE    FAST  SLOW  TIMEOUT TIMEOUT ETH  MAC
     ENABLED ENABLED PARTNER TIME  TIME  TYPE    SCALE   TYPE ADDRESS
--------------------------------------------------------------------------------
   1  true   true     yes    500   30000 short   5       8103 00:00:00:00:00:00
   2  true   true     yes    500   30000 short   5       8103 00:00:00:00:00:00
```

CLI

```
#enable VLACP globally
config vlacp enable
#configure VLACP on ports
config
ethernet 1/1,2/1 vlacp  macaddress 01:80:c2:00:00:0f
ethernet 1/1,2/1 vlacp fast-periodic-time 500
ethernet 1/1,2/1 vlacp timeout short
ethernet 1/1,2/1 vlacp  timeout-scale 5
ethernet 1/1 vlacp  flap-detect true
ethernet 1/1,2/1 vlacp enable
#show vlacp global info
ERS-8606:6# show vlacp info
================================================================================
                           Vlacp Global Information
================================================================================
               SystemId: 00:24:43:b4:e0:00
                   Vlacp           : enable
                   Vlacp hold-time : 0
#show vlacp interface info
ERS-8606:6# show ports info vlacp port 1/1,2/1
================================================================================
                              VLACP Information
================================================================================
INDEX ADMIN   OPER    PORT   FAST    SLOW    TIMEOUT TIMEOUT ETHER      MAC

      ENABLED ENABLED STATE  TIME    TIME    TIME    SCALE   TYPE       ADDR

--------------------------------------------------------------------------------
1/1   true    true    UP    500     30000   short     5      0x8103    01:80:c2:
00:00:0f
2/1   true    true    UP    500     30000   short     5      0x8103    01:80:c2:
00:00:0f

================================================================================
                         VLACP Flap Detect Information
================================================================================
INDEX FLAP    FLAP    FLAP     TOTAL      FIRST-FLAP      LAST-FLAP
      DETECT  FREQ    INTERVAL FLAP       TIME            TIME
```

```
--------------------------------------------------------------------------------
1/1    true    3        60        3          02/24/12 04:42:42 03/13/12 22:22:14
2/4    false   3        60        2          03/07/12 02:27:44 03/08/12 21:33:59
```

1.6.1.5 Solution: Simple Loop Prevention Protocol (SLPP)

If the edge switch ports are configured correctly but only the MLT function was not enabled – tagging and discard untagged frames will have no effect on preventing the loops. In this case the Simple Loop Prevention Protocol (SLPP) can be used.

The protocol is able to detect all previously discussed problems.

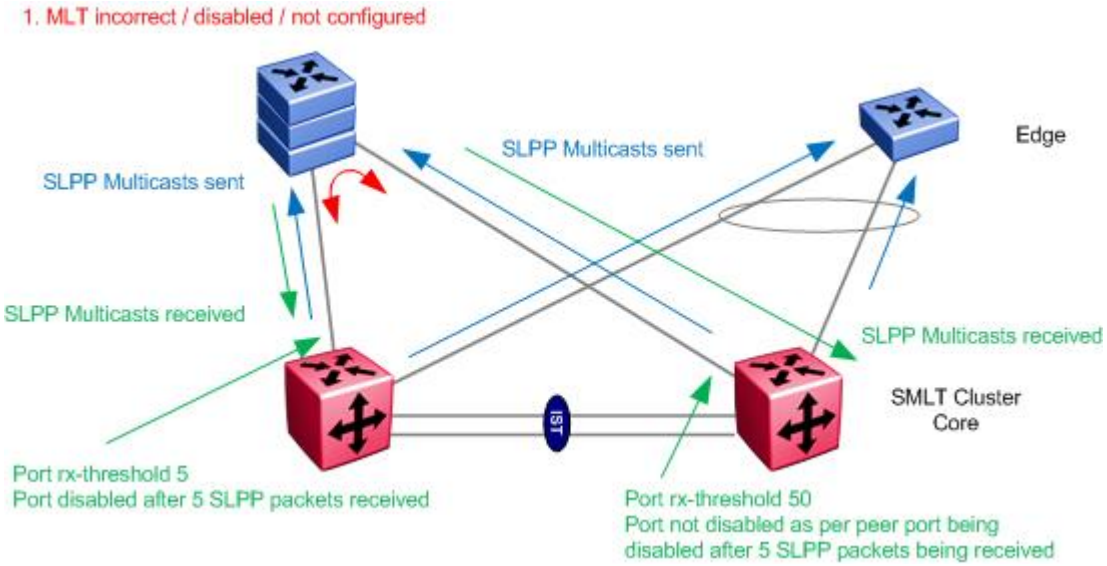
SLPP is enabled globally and on a per VLAN basis. Every SLPP enabled VLAN will generate one SLPP-PDU every 500ms (default). The SLPP-PDU is a multicast packet, and will thus flood across all port members of the VLAN. The source address of the BPDU is the sending Switch MAC address. The SLPP-PDU will only be handled specifically by the originated switch or the IST peer switch. All other switches treat the SLPP-PDU as normal multicast packet and will forward it on the VLAN.

Under normal conditions an SLPP-PDUs should never come back to the originating node or its peer SMLT node.

The SLPP receive and action mechanism is enabled on a port basis. If a self-generated (or an IST neighbor generated) packet is received on an SLPP RX-enabled port (regardless of which VLAN) is received the port is taken down after a configurable threshold of received packets is exceeded. A log file entry is generated and an SNMP trap is sent.

To avoid the shutdown of all SMLT ports to an edge switch and therefore to isolate the edge switch from the core - the RX thresholds for SLPP should be different for the different ports. Links to one core switch should be treated as primary links and should be configured with a higher threshold – to keep the ports up while ports with a lower threshold would be disabled first.

Once the port is down (and auto-recovery is disabled – which is the recommended setting), it will stay in the down state and need manual intervention to be enabled.



SLPP transmission should be enabled on the edge VLANs and SLPP receiving on SMLT edge uplinks. The SLPP receive should never be enabled on the IST links as the IST should never be disabled.

When SLPP-PDU receiving process works on the port which is a member of an MLT, all port members in that MLT will be taken down

SLPP is available on VSP 9000, VSP 7000, ERS 8600/8800, ERS 8300 and ERS 5000.

Configuration:

ACLI – ERS 5000

```
# sending of SLPP is configured on a per VLAN base
config t
slpp enable
# slpp add <vid>
slpp vid 10
slpp vid 11
slpp vid 12
# repeat for all VLANs where SLPP should be sent out
# receiving of SLPP is configured on ports
interface fastEthernet 1/1
slpp packet-rx
# threshold to shut down ports after a number of SLPP packets
slpp packet-rx-threshold 5
```

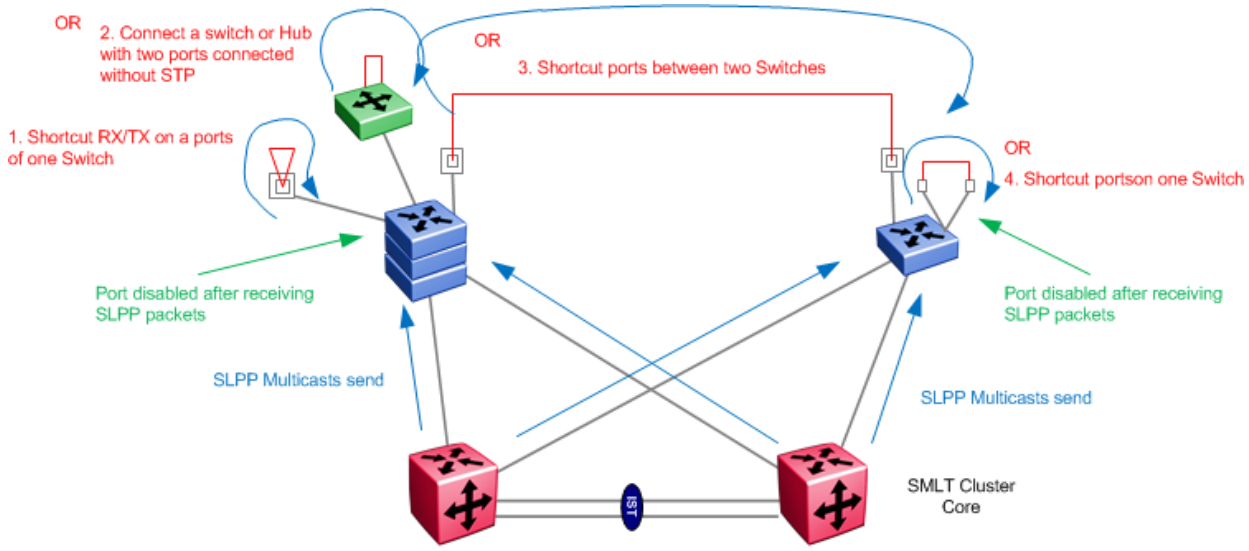
CLI

```
# sending of SLPP is configured on a per VLAN base
config
slpp operation enable
# slpp add <vid>
slpp add 10
slpp add 11
slpp add 12
# repeat for all VLANs where SLPP should be sent out
# receiving of SLPP is configured on ports
ethernet 1/1 slpp packet-rx enable
# threshold to shut down ports after a number of SLPP packets
ethernet 1/1 slpp packet-rx-threshold 5
```

1.6.1.5.1 SLPP Guard

If SLPP is enabled on the SMLT Cluster core, SLPP Guard should also be enabled on all access ports switch on Edge Switch. When operational, SLPP-guard will immediately administratively disable a port when a SLPP packet is received on a port and generate a local log message, syslog message (if the syslog server(s) are configured) and SNMP traps (if SNMP tap receivers are configured).

SLPP-guard is available on the ERS 4000 starting in release 5.5, the ERS 5000 in release 6.2.4, and will be added to the VSP 7000 in the 10.3 release.



Configuration:

ACLI – ERS 4000 / ERS 5000

`config t`
`# SLPP is configured on ports where threshold is set to recommended value of infinity`
`interface fastEthernet 1/1`
`slpp-guard enable timeout 0`

1.6.1.5.2 Alternative Solutions

A config corruption might be the result of the autosave function during a power outage. To avoid configurations being saved automatically on the edge switches (ES or ERS up to 56xx series) the autosave function could be disabled. This prevents automatic saving of the config at critical times (e.g. at a planned a power cut). The config then needs to be saved manually.

LACP (802.1d Dynamic Link Aggregation) could be used but adds additional complexity to the network and is not supported on all devices.

1.6.1.6 Additional Loop Prevention Methods

1.6.1.6.1 Loop Detect

The Loop-Detect feature on the Ethernet Routing Switch 8600 was originally designed for stacked VLANs but can be used in SMLT access applications. When using stacked VLANs, loop detect is used to detect the same MAC address across difference ports and will shut down the VLAN where it detected the loop. In this way, only one stacked VLAN is shut down while the other stacked VLANs continue to operate.

The Loop-Detect feature has been enhanced for SMLT access applications in that you can choose between shutting down a port, a group of ports, or a VLAN if a loop is detected. It is recommended to select port(s) shutdown versus a VLAN shutdown. The reason being if VLAN shutdown is selected, the VLAN itself is shutdown, not the port. Hence, the access switch still sees the port up and will continue to forward traffic to SMLT Core Aggregation Switch. If loop detect port shutdown is selected, then the access switch will recover by detecting the failed link.

The Loop-Detect feature is used to prevent loops by detecting if the same MAC address shows up on separate ports. This feature will either shutdown a VLAN or a port, or group of ports if it detects the same MAC address between two different ports 5 times in a configurable amount of time.

The loop detect feature is not the preferred method of detecting loops in the network. It is recommended to use SLPP, with extended-CP-limit in the core instead.

1.6.1.6.2 CP-Limit

The “CP-limit” feature provides maximum system stability when network abnormal occur, such as network loops or malicious traffic, enter the system CPU. This prevents the CPU from being overloaded by excessive multicast or broadcast control or exception traffic. For example, traffic generated by a network loop introducing broadcast storms in a network will not impact the stability of the system.

The “CP-limit” and “Extended CP-limit” features are different from the rate-limit feature in that “CP-limit” and “Extended CP-limit” monitor only packets that are sent to the CPU (control plane), and do not monitor packets that are forwarded through the switch (data plane).

The general rule of CP-Limit is that it should be enabled for all SMLT ports such that the Ethernet Routing Switch 8600 can disable any ports that are receiving excess control traffic, normally indicating some network error. In the case of SMLT there is an exception because of the importance of the IST trunk, thus, it is recommended to disable the CP-Limit feature on all IST ports to remove the possibility of having these ports disabled and possibly compromising the stability of SMLT.

1.6.1.6.3 Extended-CP-Limit

The “Extended CP-limit” feature, available on the ERS 8600/8800 only, goes one step further by looking at virtually any traffic going to the CPU. All the frames going to the CPU are counted and monitored depending on how congested the CPU is. This feature will protect the CPU from excessive traffic hitting the CPU by shutting down the port(s) which are responsible for sending traffic to CPU at a rate greater than desired.

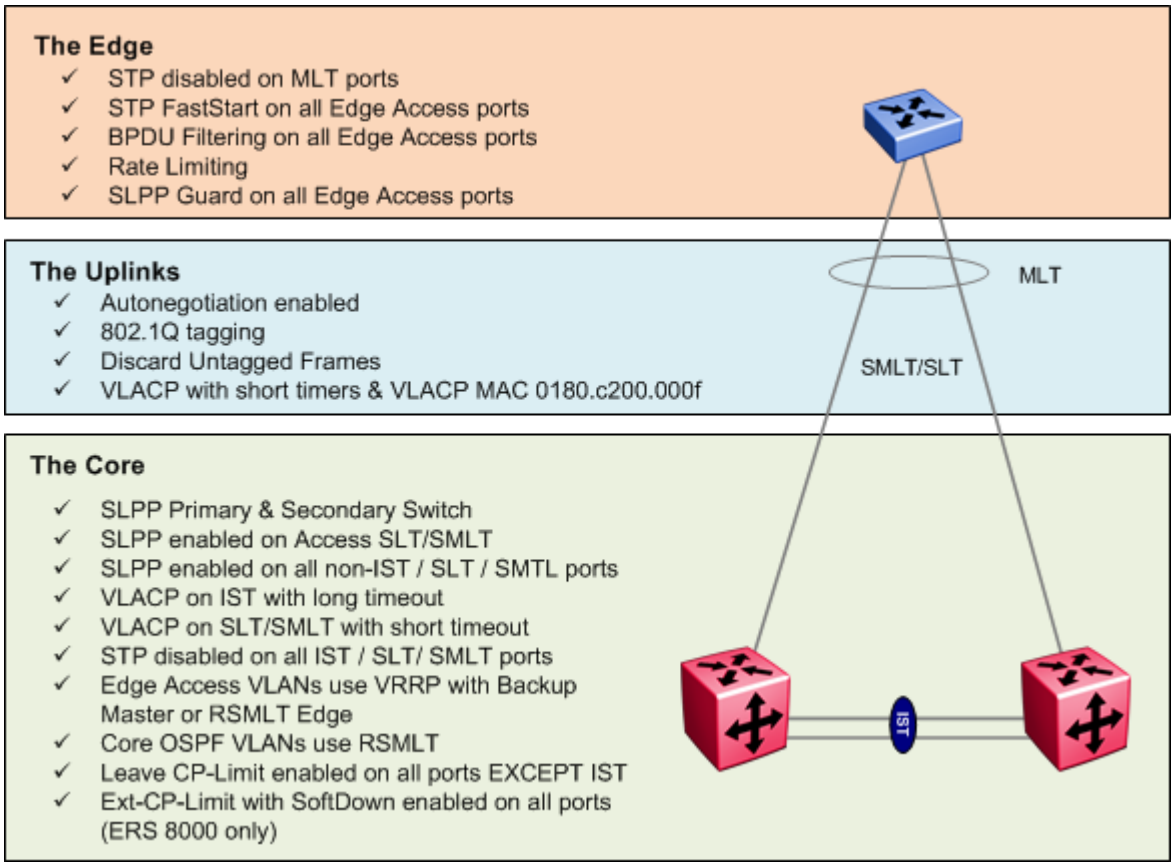
When setting up Extended CP-Limit, you have the choice of enabling HardDown or SoftDown at a port level. If HardDown is used, it uses the global ‘min-congestion-time’ to calculate when to shutdown the port. If SoftDown is selected then both the global ‘port-congestion-time and port level ‘threshold-util-rate’ is used to calculate when to shutdown a port. Please note that in both cases, HardDown and SoftDown, congestion is observed at the port level and not at the CPU level.

With the Ext CP-Limit HardDown option enabled, all interfaces set to HardDown will be disabled. This is not the case with SoftDown where only the affected port is disabled.

1.6.1.7 Summary of the Recommendations

Most of the discussed loops are not related to IST/SMLT designs. They need to be detected and prevented in any other network design. IST/SMLT designs are more affected if the Broadcast/Multicast load leads to an extreme CPU load and the IST is dropped. The proposed mechanisms can effectively prevent the problems and provide a stable network even under critical circumstances.

The following picture quickly summarizes the configuration options that should be used for optimal configuration. It also adds some proposals that are not directly related to loop detection but add reliability to the IST/SMLT designs.



2. Configuring SMLT – Triangle Topology Examples

2.1 Configuration – VSP 9000 Layer 2 SMLT Triangle Switch Cluster Configuration

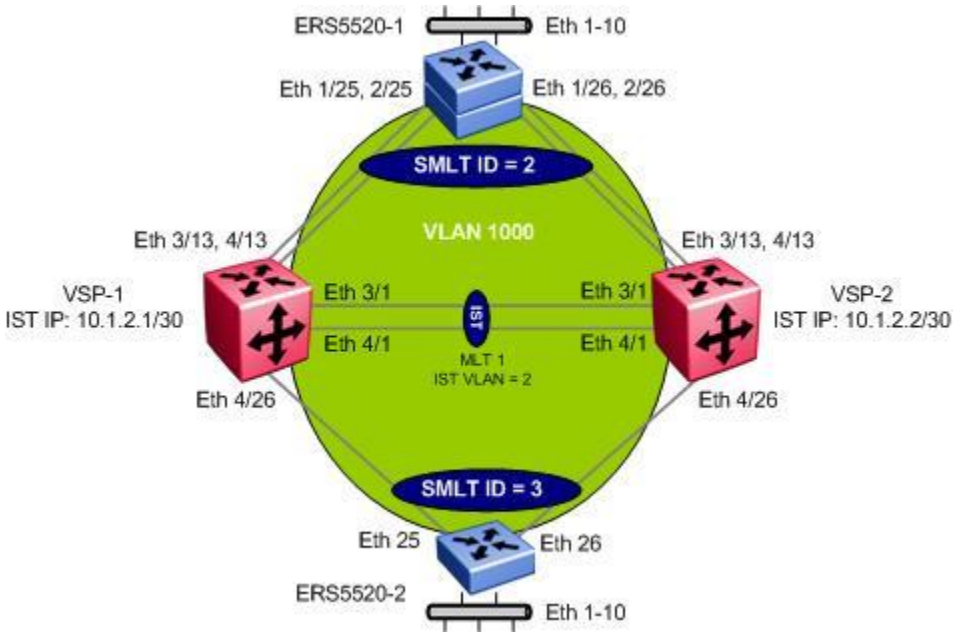


Figure 2: VSP 9000 Layer 2 Triangle SMLT Configuration with SLPP

For this example, we will configure the SMLT switch cluster with the following:

- IST
  - IST VLAN 2 using MLT ID = 1
  - Tagged port members 3/1 and 4/1
  - All IST ports are Gigabit Ethernet ports using default setting of Autonegotiation enable
  - VLACP using the recommend reserved multicast MAC (01:80:C2:00:00:0F), long timers, and slow-periodic-time of 10,000 ms
- SMLT
  - SMLT VLAN 1000
  - VSP-1 is assumed to the SMLT Primary switch while VSP-2 is the SMLT Secondary switch
  - MLT and SMLT ID of 2 for ERS5520-1 with tagged port member 3/13 and 4/13
  - MLT and SMLT ID of 3 for ERS5520-2 with tagged port member 4/26
  - All SMLT are Gigabit Ethernet ports using default setting of Autonegotiation enable
  - Enable SLPP
  - Enable VLACP with recommended reserved multicast MAC address and with short timers of 500ms and set timeout scale to 5

- Enable “Discard Untagged Frames” on all Access SMLT port members, this includes ports 3/13, 4/13, and 4/26
- Disable STP on all SMLT ports (default setting when SMLT is enabled)
- Set the recommended moderate CP Limit settings for broadcast and multicast traffic

- Access Switches

  On both ERS5520-1 and ERS5520-2, the following will be configured:

  - Broadcast and multicast rate limiting with a threshold to 10%
  - Enable Spanning Tree Fast Start and BPDU filtering on all edge ports
  - Disable Spanning Tree on MLT core ports to SMLT Cluster switches
  - BPDU filtering on all edge ports
  - VLAN Tagging on MLT access trunk ports

It is recommended to use the lowest MLT number for the IST. For the VLAN ID, it makes no difference if you use a low or high number.

2.1.1 Configuration – VSP 9000 Layer 2 Switch Cluster

2.1.1.1 Configuration Mode

Go to configuration mode

```
config terminal
```

2.1.1.2 Create VLANs

The following port based VLANs will be configured on the SMLT Switch cluster

- VLAN 2 to be used by the Inter Switch Trunk (IST)
- VLAN 1000 to be used at a Layer 2 level to ERS5520-1 and ERS5520-2 for connecting users.

VSP 9000 SMLT Cluster: Create VLANs 2 and 1000

VSP-1:

```
VSP-1:1(config)#vlan create 2 name "IstVlan" type port-mstprstp 0
VSP-1:1(config)#vlan create 1000 name "SmltVlan" type port-mstprstp 0
VSP-1:1(config)#interface Vlan 2
VSP-1:1(config-if)#ip address 10.1.2.1 255.255.255.252
VSP-1:1(config-if)#exit
```

VSP-2: Same configuration as VSP-1 except for the IP address

```
VSP-2:1(config)#interface Vlan 2
VSP-2:1(config-if)#ip address 10.1.2.2 255.255.255.252
```

The IST and SMLT port numbers will be added when the corresponding MLT is created.

2.1.1.3 Create IST

Multilink Trunking 1 (MLT 1) will be used for the IST with port members 2/1 and 3/1. 802.1Q tagging will be enabled on all IST port members and Spanning Tree will be disabled on all IST port members by default. VLACP will be enabled on the IST trunk.

It is recommended to use the reserved multicast MAC address of 01:80:c2:00:00:0f for the VLACP MAC address.

By default, unless you specify the VLACP timeout, the default setting of *long* will be used. Hence, we do not have to configure the VLACP timeout for the IST.

VSP 9000 SMLT Cluster: Step 1 – Create MLT 1 for IST

VSP-1 & VSP 2: Same configuration on both switches

```
VSP-1:1(config)#mlt 1 enable name "Ist"
VSP-1:1(config)#mlt 1 member 3/1,4/1
VSP-1:1(config)#mlt 1 encapsulation dot1q
VSP-1:1(config)#vlan mlt 2 1
```

VSP 9000 SMLT Cluster: Step 2 – Create IST

VSP-1:

```
VSP-1:1(config)#interface mlt 1
VSP-1:1(config-if)#ist peer-ip 10.1.2.2 vlan 2
VSP-1:1(config-if)#ist enable
VSP-1:1(config-if)#exit
```

VSP 2:

```
VSP-2:1(config)#interface mlt 1
VSP-2:1(config-if)#ist peer-ip 10.1.2.1 vlan 2
VSP-2:1(config-if)#ist enable
VSP-2:1(config-if)#exit
```

VSP 9000 SMLT Cluster: Step 3 – Enable VLACP

VSP-1 & VSP 2: Same configuration on both switches

```
VSP-1:1(config)#vlacp enable
VSP-1:1(config)#interface GigabitEthernet 2/1,3/1
VSP-1:1(config-if)#vlacp funcmac-addr 01:80:c2:00:00:0f
VSP-1:1(config-if)#vlacp slow-periodic-time 10000
VSP-1:1(config-if)#vlacp enable
VSP-1:1(config-if)#exit
```

2.1.1.4 SMLT-2 to ERS5520-1

VSP 9000 SMLT Cluster: Step 1 – Create SMLT-2

VSP-1 & VSP 2: Same configuration on both switches

```
VSP-1:1(config)#mlt 2 enable name "Smlt-2"
VSP-1:1(config)#mlt 2 member 3/13,4/13
VSP-1:1(config)#mlt 2 encapsulation dot1q
VSP-1:1(config-if)#interface mlt 2
VSP-1:1(config-if)#smlt
VSP-1:1(config-if)#exit
VSP-1:1(config)#vlan mlt 1000 2
```

2.1.1.5 SMLT-3 to ERS5520-2

VSP 9000 SMLT Cluster: Create SMLT-3

VSP-1 & VSP 2: Same configuration on both switches

```
VSP-1:1(config)#mlt 2 enable name "Smlt-3"
VSP-1:1(config)#mlt 2 member 4/26
VSP-1:1(config)#mlt 2 encapsulation dot1q
VSP-1:1(config-if)#interface mlt 3
VSP-1:1(config-if)#smlt
VSP-1:1(config-if)#exit
VSP-1:1(config)#vlan mlt 1000 3
```

2.1.1.6 Add VLAN 1000 to IST

VSP 9000 SMLT Cluster: Add VLAN 1000 to IST

VSP-1 & VSP 2: Same configuration on both switches

```
VSP-1:1(config)#vlan mlt 1000 1
```

2.1.1.7 CP Limit – MLT 2 & mlt 3

CP Limit will be enabled on all the Access MLTs which in our example is MLT 2. For this example, we will select the default recommendations for CP-Limit, enable Shutdown, and AutoRecoverPort.

VSP 9000 SMLT Cluster: CP Limit

VSP-1 & VSP 2: Same configuration on both switches

```
VSP-1:1(config)#interface mlt 2
VSP-1:1(config-if)#cp-limit 10000 shutdown
VSP-1:1(config-if)#exit
VSP-1:1(config)#interface mlt 3
VSP-1:1(config-if)#cp-limit 10000 shutdown
VSP-1:1(config-if)#exit
```

2.1.1.8 SLPP

SLPP will be enabled globally and only on the SMLT access ports 3/13 and 4/13 and SMLT access port 4/26 for VLAN 1000. On the SMLT primary switch we will set the SLPP packet-rx-threshold to 5, while on the SMLT secondary switch we will set the SLPP packet-rx-threshold to 50. For this example, we will pick VSP-1 as the primary switch.

The recommended SLPP receive threshold value for the primary switch is 5 and 50 for the secondary switch in an SMLT cluster.

SLPP should only be enabled on the SMLT access ports and not on the IST port members.

VSP 9000 SMLT Cluster: Enable SLPP

VSP-1:

```
VSP-1:1(config)#slpp enable
VSP-1:1(config)#slpp vid 1000
VSP-1:1(config)#interface GigabitEthernet 3/13,4/13,4/26
VSP-1:1(config-if)#slpp packet-rx
VSP-1:1(config-if)#slpp packet-rx-threshold 5
VSP-1:1(config-if)#exit
```

VSP 2: Same configuration as VSP-1 except the SLPP packet receive threshold is 50

```
VSP-2:1(config-if)#slpp packet-rx-threshold 50
```

2.1.1.9 VLACP

As the access switches, ERS5520-1 and ERS5520-2, supports VLACP, we will enable this feature 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.

VSP 9000 SMLT Cluster: Enable VLACP

```
VSP-1 & VSP 2: Same configuration on both switches
VSP-1:1(config)#interface GigabitEthernet 3/13,4/13,4/26
VSP-1:1(config-if)#vlacp timeout short timeout-scale 5 funcmac-addr 01:80:c2:00:00:0f
VSP-1:1(config-if)#vlacp enable
VSP-1:1(config-if)#exit
```

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

2.1.1.10 Discard Untagged Frames

It is recommended to enable discard untagged frames on all IST and SMLT ports.

VSP 9000 SMLT Cluster: Enable Discard Untagged Frames

```
VSP-1 & VSP 2: Same configuration on both switches
VSP-1:1(config)#interface GigabitEthernet 3/1,4/1,3/13,4/13,4/26
VSP-1:1(config-if)#untagged-frames-discard
VSP-1:1(config-if)#exit
```

2.1.2 Configuration - Edge Switch

2.1.2.1 MSTP

Edge switch: Enable MSTP

```
5520-1 & 5520-2: Same configuration on both switches
5520-1(config)#spanning-tree mode mst
New operational mode MSTP will take effect upon reset
5520-1(config)#boot
Reboot the unit(s) (y/n) ? y
```

As the VSP 9000 uses MSTP by default, it is recommended to change the Spanning mode on the access stackable switches to also use MSTP. Even though Spanning Tree is not used and is disabled on the core ports, the Spanning Tree mode is used by some Network Management tools such as VLAN Manager in COM. VLAN Manager will regroup all VLANs per Spanning Tree group type, hence, if you leave the stackable edge switch in their default Spanning Tree mode of STPG, then VLAN Manager will not be able to display, create, delete, or sync a VLAN

across the VSP and the edge stackable switches.

2.1.2.2 Create VLAN

Edge switch: Create VLAN 1000

5520-1:

```
5520-1(config)#vlan create 1000 name Services type port cist
5520-1(config)#vlan members remove 1 1/1-10,1/25-26,2/1-10,2/25-26
5510-1(config)#vlan ports 1/25-26,2/25-26 tagging tagall
5520-1(config)#vlan members 1000 1/1-10,1/25-26,2/1-10,2/25-26
```

5520-2:

```
5520-2(config)#vlan create 1000 name Services type port cist
5520-2(config)#vlan members remove 1 1-10,25-26
5520-2(config)#vlan ports 25-26 tagging tagall
5520-2(config)#vlan members 1000 1-10,25-26
```

2.1.2.3 Create MLT

Edge switch: Create MLT 1

5520-1:

```
5520-1(config)# mlt 1 member 1/25-26,2/25-26 learning disable
5520-1(config)# mlt 1 enable
```

5520-2:

```
5520-2(config)# mlt 1 member 25,26 learning disable
5520-2(config)#mlt 1 enable
```

2.1.2.4 VLACP

Please note that on an ERS 5000 switch, the VLACP MAC is entered as a hexadecimal value in the format of 'H.H.H'. Hence, the recommended VLACP MAC value of 01:80:c2:00:00:0f is entered as *180.c200.f*.

Edge switch: Enable VLACP

5520-1:

```
5520-1(config)#vlacp macaddress 180.c200.f
5520-1(config)#vlacp enable
5520-1(config)#interface fastEthernet 1/25-26,2/25-26
5520-1(config-if)#vlacp timeout short
5520-1(config-if)#vlacp timeout-scale 5
5520-1(config-if)#vlacp enable
5520-1(config-if)#exit
```

5520-2:

```
5520-2(config)#vlacp macaddress 180.c200.f
5520-2(config)#vlacp enable
5520-2(config)#interface fastEthernet 25,26
5520-2(config-if)#vlacp timeout short
5520-2(config-if)#vlacp timeout-scale 5
5520-2(config-if)#vlacp enable
5520-2(config-if)#exit
```

2.1.2.5 Enable Spanning MSTP Edge Port and BPDU filtering on all Access Ports

Edge switch: Enable MSTP edge port and BPDU Filtering

5520-1:

```
5520-1(config)#interface fastEthernet 1/1-10,2/1-10
5520-1(config-if)#spanning-tree mstp edge-port true
5520-1(config-if)#spanning-tree bpdu-filtering timeout 0
5520-1(config-if)#spanning-tree bpdu-filtering enable
5520-1(config-if)#exit
```

5520-2:

```
5520-2(config)#interface fastEthernet 1-10
5520-2(config-if)#spanning-tree mstp edge-port true
5520-2(config-if)#spanning-tree bpdu-filtering timeout 0
```

```
5520-2(config-if)#spanning-tree bpdu-filtering enable
5520-2(config-if)#exit
```

2.1.2.6 Enable Rate Limiting

Edge switch: Enable Rate Limiting to 10% of total traffic for both broadcast and multicast traffic

5520-1:

```
5520-1(config)#interface fastEthernet all
5520-1(config-if)#rate-limit port 1/1-10,2/1-10 both 10
5520-1(config-if)#exit
```

5520-2:

```
5520-2(config)#interface fastEthernet all
5520-2(config-if)#rate-limit port 1-10 both 10
5520-2(config-if)#exit
```

Please note that the rate limit parameter on the ERS 5000 is expressed as percentage of total traffic. The values used in this example are just a suggestion and may vary depending on your needs.

When measuring the Broadcast Rate Limit, note that the rate limiting feature displays a calculation based on packets rather than octets. To obtain the actual value, use the following equation (the average packet size is 500 bytes):

(Line speed (bit/sec)/ Average packet size x 8) X (Rate Limit/100) = Packets per second

2.1.2.7 Discard Untagged Frames

Edge switch: Enable Discard Untagged Frames

5520-1:

```
5520-1(config)#vlan ports 1/25-26,2/25-26 filter-untagged-frame enable
```

5520-2:

```
5520-2(config)#vlan ports 25-26 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.

2.1.3 Configuration File

VSP-1	VSP-2
config terminal cfm ethertype 0x8902 # # CLI CONFIGURATION # prompt "VSP-1" password password-history 3 # # LACP CONFIGURATION # vlacp enable # # MLT CONFIGURATION # mlt 1 enable name "IST" mlt 1 member 3/1,4/1 mlt 1 encapsulation dot1q mlt 2 enable name “Smlt-2” mlt 2 member 3/13,4/13 mlt 2 encapsulation dot1q mlt 3 enable name “Smlt-3” mlt 3 member 4/26 mlt 3 encapsulation dot1q interface mlt 1 ist peer-ip 10.1.2.2 vlan 2 ist enable exit interface mlt 2 smlt 2 exit	config terminal cfm ethertype 0x8902 # # CLI CONFIGURATION # prompt "VSP-2" password password-history 3 # # LACP CONFIGURATION # vlacp enable # # MLT CONFIGURATION # mlt 1 enable name "IST" mlt 1 member 3/1,4/1 mlt 1 encapsulation dot1q mlt 2 enable name “Smlt-2” mlt 2 member 3/13,4/13 mlt 2 encapsulation dot1q mlt 3 enable name “Smlt-3” mlt 3 member 4/26 mlt 3 encapsulation dot1q interface mlt 1 ist peer-ip 10.1.2.1 vlan 2 ist enable exit interface mlt 2 smlt 2 exit

```
interface mlt 3
smlt 3
exit



#
# VLAN CONFIGURATION - PHASE I
#


vlan create 2 name "IstVlan" type port-mstprstp
0
vlan mlt 2 1
vlan members 2 3/1,4/1 portmember
interface Vlan 2
ip address 10.1.2.1 255.255.255.252 3
exit
vlan create 1000 name " SmltVlan" type port-
mstprstp 0
vlan mlt 1000 1
vlan mlt 1000 2
vlan mlt 1000 3
vlan members 1000 3/1,3/13,4/1,4/13,4/26
portmember
exit


#
# PORT CONFIGURATION - PHASE II
#


interface GigabitEthernet 3/1
untagged-frames-discard
default-vlan-id 2
vlacp slow-periodic-time 10000 funcmac-addr
01:80:c2:00:00:0f
vlacp enable
no spanning-tree mstp force-port-state enable
exit
interface GigabitEthernet 3/13
untagged-frames-discard
default-vlan-id 1000
auto-recover-port enable
cp-limit 10000 shutdown
slpp packet-rx
```

```
interface mlt 3
smlt 3
exit



#
# VLAN CONFIGURATION - PHASE I
#


vlan create 2 name "IstVlan" type port-mstprstp
0
vlan mlt 2 1
vlan members 2 3/1,4/1 portmember
interface Vlan 2
ip address 10.1.2.2 255.255.255.252 3
exit
vlan create 1000 name " SmltVlan" type port-
mstprstp 0
vlan mlt 1000 1
vlan mlt 1000 2
vlan mlt 1000 3
vlan members 1000 3/1,3/13,4/1,4/13,4/26
portmember
exit


#
# PORT CONFIGURATION - PHASE II
#


interface GigabitEthernet 3/1
untagged-frames-discard
default-vlan-id 2
vlacp slow-periodic-time 10000 funcmac-addr
01:80:c2:00:00:0f
vlacp enable
no spanning-tree mstp force-port-state enable
exit
interface GigabitEthernet 3/13
untagged-frames-discard
default-vlan-id 1000
auto-recover-port enable
cp-limit 10000 shutdown
slpp packet-rx
```

```
slpp packet-rx-threshold 5
vlacp fast-periodic-time 500 timeout short
timeout-scale 5 funcmac-addr 01:80:c2:00:00:0f
vlacp enable
no spanning-tree mstp force-port-state enable
exit
interface GigabitEthernet 4/1
untagged-frames-discard
default-vlan-id 2
vlacp slow-periodic-time 10000 funcmac-addr
01:80:c2:00:00:0f
vlacp enable
no spanning-tree mstp force-port-state enable
exit
interface GigabitEthernet 4/13
untagged-frames-discard
default-vlan-id 1000
auto-recover-port enable
cp-limit 10000 shutdown
slpp packet-rx
slpp packet-rx-threshold 5
vlacp fast-periodic-time 500 timeout short
timeout-scale 5 funcmac-addr 01:80:c2:00:00:0f
vlacp enable
no spanning-tree mstp force-port-state enable
exit
interface GigabitEthernet 4/26
untagged-frames-discard
default-vlan-id 1000
auto-recover-port enable
cp-limit 10000 shutdown
slpp packet-rx
slpp packet-rx-threshold 5
smlt 129
vlacp fast-periodic-time 500 timeout short
timeout-scale 5 funcmac-addr 01:80:c2:00:00:0f
vlacp enable
no spanning-tree mstp force-port-state enable
exit


#
# SLPP CONFIGURATION
#
```

```
slpp packet-rx-threshold 5
vlacp fast-periodic-time 500 timeout short
timeout-scale 5 funcmac-addr 01:80:c2:00:00:0f
vlacp enable
no spanning-tree mstp force-port-state enable
exit
interface GigabitEthernet 4/1
untagged-frames-discard
default-vlan-id 2
vlacp slow-periodic-time 10000 funcmac-addr
01:80:c2:00:00:0f
vlacp enable
no spanning-tree mstp force-port-state enable
exit
interface GigabitEthernet 4/13
untagged-frames-discard
default-vlan-id 1000
auto-recover-port enable
cp-limit 10000 shutdown
slpp packet-rx
slpp packet-rx-threshold 5
vlacp fast-periodic-time 500 timeout short
timeout-scale 5 funcmac-addr 01:80:c2:00:00:0f
vlacp enable
no spanning-tree mstp force-port-state enable
exit
interface GigabitEthernet 4/26
untagged-frames-discard
default-vlan-id 1000
auto-recover-port enable
cp-limit 10000 shutdown
slpp packet-rx
slpp packet-rx-threshold 5
smlt 129
vlacp fast-periodic-time 500 timeout short
timeout-scale 5 funcmac-addr 01:80:c2:00:00:0f
vlacp enable
no spanning-tree mstp force-port-state enable
exit


#
# SLPP CONFIGURATION
#
```

slpp enable slpp vid 1000	slpp enable slpp vid 1000

2.1.4 Verify Operations

2.1.4.1 Verify MLT Configuration

Verify that the MLT instances is configured correctly and is functioning by issuing the following command:

show mlt

Results:

```
================================================================================
                                    Mlt Info
================================================================================
                          PORT    SVLAN  MLT   MLT        PORT         VLAN
MLTID IFINDEX NAME        TYPE    TYPE   ADMIN CURRENT    MEMBERS      IDS
1     4098    IST         trunk   normal ist   ist        3/1,4/1       2 1000
2     4100    5520-1      trunk   normal smlt  smlt       3/13,4/13     1000
3     4100    5520-2      trunk   normal smlt  smlt       4/26          1000


                 MULTICAST             DESIGNATED   LACP      LACP
MLTID IFINDEX    DISTRIBUTION  NT-STG  PORTS        ADMIN     OPER
--------------------------------------------------------------------------------
1       4098     disable       enable   2/1         disable   down
2       4100     disable       enable   3/13        disable   down
3       4100     disable       enable   4/26        disable   down
```

On each VSP 9000 in the switch cluster verify the following information:

Option	Verify
VLAN IDS	Verify that the VLAN ids assigned to the IST and SMLT MLT are correct: • IST MLT 1: Member of VLANs ***1000*** & ***2*** with port members ***3/1 and 4/1*** • MLT 2: Member of VLAN ***1000*** with port member ***3/13*** and ***4/13*** • MLT 3: Member of VLAN ***1000*** with port member ***4/26***
MLT ADMIN	Displays as ***smlt*** or ***ist*** if configured correctly. The value ***normal*** indicates that the IST or SMLT is not configured.
MLT CURRENT	Displays as ***smlt*** or ***ist*** if the SMLT or IST is operational.
PORT TYPE	Displays as ***trunk*** for all IST and SMLT ports and will pass tagged frames. The value ***access*** indicates that the port will pass untagged frames.

2.1.4.2 Virtual LANs (VLANs):

Verify the VLAN port assignments and 802.1Q tagging settings by issuing the following command:

show interfaces gigabitEthernet vlan

Results:

```
================================================================
                        Port Vlans
================================================================
PORT          DISCARD DISCARD   DEFAULT VLAN   PORT     UNTAG
NUM   TAGGING TAGFRAM UNTAGFRAM VLANID  IDS    TYPE     DEFVLAN
----------------------------------------------------------------
3/1   enable  false   true      2       2 1000 normal   disable
4/1   enable  false   true      2       2 1000 normal   disable
3/13  enable  false   true      1000    1000   normal   disable
4/13  enable  false   true      1000    1000   normal   disable
4/26  enable  false   true      1000    1000   normal   disable
```

On each VSP 9000 in the switch cluster verify the following information:

Option	Verify
VLAN IDS	Verify that the VLAN ids assigned to the IST and SMLT ports are correct: • IST Ports: Member of VLANs ***1000*** & ***2***. • SMLT 2 Ports: Member of VLAN ***1000***. • SMLT 3 Ports: Member of VLAN ***1000***.
TAGGING	Displays as ***enable*** for all IST and SMLT ports. The value ***disable*** indicates that the port is in an untagged mode.
DISCARD UNTAGFRAM	Displays as ***true*** for all IST and SMLT ports. The value ***false*** indicates that the port will pass untagged frames.

2.1.4.3 Inter Switch Trunk (IST):

Verify that the IST is configured correctly and is functioning by issuing the following command:

show ist mlt

Results:

```
================================================
                    Mlt IST Info
================================================
MLT    IP                VLAN     ENABLE    IST
ID     ADDRESS           ID       IST       STATUS
------------------------------------------------
1      10.1.2.2          2        true      up
```

On each VSP 9000 in the switch cluster verify the following information:

Option	Verify
MLT ID	Verify the MLT ID assigned to the IST is correct.
IP ADDRESS	Verify that the IST peer IP address is correct: • VSP-1: Will display the peer IP ***10.1.2.2*** • VSP-2: Will display the peer IP ***10.1.2.1***
VLAN ID	Displays the IST VLAN which for this example is VLAN 2.
ENABLE IST	Displays as ***true***. The value ***false*** indicates that the IST is not enabled.
IST STATUS	Displays as ***up***. The value ***down*** indicates that the IST is not operational.

2.1.4.4 Split MultiLink Trunking (SMLT):

Verify that SMLT is functioning correctly by issuing the following command:

show smlt mlt

Results:

```
==============================================
                    Mlt SMLT Info
==============================================
MLT    SMLT     ADMIN    CURRENT
ID     ID       TYPE     TYPE
----------------------------------------------
2      2        smlt     smlt
3      3        smlt     smlt
```

On each VSP 9000 in the switch cluster verify the following information:

Option	Verify
SMLT ID	Verify that the SMLT IDs match the MLT IDs.
ADMIN TYPE	Displays as ***smlt*** for each SMLT ID. A ***normal*** value indicates that the MLT is not configured as an SMLT trunk.
CURRENT TYPE	Displays as ***smlt*** for each SMLT ID. A ***normal*** value indicates that the SMLT ports are disconnected or the SMLT IDs are mis-configured.

2.1.4.5 Virtual Link Aggregation Control Protocol (VLACP):

Step 1: Verify that VLACP is globally enabled by using the following command:

Show vlacp

Results:

```
================================================================================
                          Vlacp Global Information
================================================================================
                  SystemId: 00:01:81:28:84:00
                      Vlacp: enable
```

On each VSP 9000 in the switch cluster verify the following information:

Option	Verify
Vlacp	Displays as ***enable***. The value ***disable*** indicates that VLACP is globally disabled on the switch.
SystemId	Displays as ***00:01:81:28:84:00***. Please note that the VLACP reserved MAC shows up at the interface level.

Step 2: Verify the IST and SMLT per port VLACP settings by issuing the following command:

show vlacp interface gigabitethernet 2/1,3/1,3/13,4/13

Results:

```
================================================================================
                             VLACP Information
================================================================================
INDEX ADMIN   OPER    PORT   FAST    SLOW    TIMEOUT TIMEOUT ETHER      MAC
      ENABLED ENABLED STATE  TIME    TIME    TIME    SCALE   TYPE       ADDR
--------------------------------------------------------------------------------
3/1   true    true    UP     200     10000   long    3       0x8103     01:80:c2:00:00:0f
4/1   true    true    UP     200     10000   long    3       0x8103     01:80:c2:00:00:0f
3/13  true    true    UP     500     30000   short   5       0x8103     01:80:c2:00:00:0f
4/13  true    true    UP     500     30000   short   5       0x8103     01:80:c2:00:00:0f
4/26  true    true    UP     500     30000   short   5       0x8103     01:80:c2:00:00:0f
```

On each VSP 9000 in the switch cluster verify the following information:

Option	Verify
ADMIN ENABLED	Displays as ***true*** for the IST, SMLT-2, and SMLT-3 ports. The value ***false*** indicates that VLACP is disabled for the port.
OPER ENABLED	Displays as ***true*** for the IST, SMLT-2, and SMLT-3 ports. The value ***false*** indicates that VLACP is not operational on the port.
FAST TIME	Displays as ***500*** for the SMLT-2 and SMLT-3 ports. The value must match for each switch port in the link pair.
SLOW TIME	Displays as ***10000*** for the IST port members. If not, please change the VLACP slow-periodic-time setting to this value.
TIMEOUT TIME	Displays as ***long*** for the IST ports and ***short*** for SMLT-2 and SMLT-3 ports. This value must match for each switch port in the link pair.
TIMEOUT SCALE	Displays as ***5*** for the SMLT-2 and SMLT-3 ports. The default timeout scale of ***3*** will be displayed for the IST port members 3/1 and 4/1.
MAC ADDR	The VLACP MAC address is assigned to each IST, SMLT-2 and SMLT-3 port members: • IST port 3/1 and 4/1: ***01:80:c2:00:00:0f***. • SMLT-2 & SMLT-3 ports: ***01:80:c2:00:00:0f***. The VLACP MAC address must match for each switch port in the link pair.

2.1.4.6 Simple Loop Prevention Protocol (SLPP):

Step 1: Verify that SLPP is globally enabled on the switch by issuing the following command:

show slpp

Results:

```
================================================================================
                            SLPP Info
================================================================================
              etherType (hex) : 0x8104
                    operation : enabled
                  tx-interval : 500
                         vlan : 1000
```

On each VSP 9000 in the switch cluster verify the following information:

Option	Verify
operation	Displays as ***enable***. The value ***disable*** indicates that SLPP is globally disabled on the switch.
vlan	Displays as ***1000*** indicating SLPP is enabled for VLAN 1000.

Step 2: Verify the SLPP settings by issuing the following command:

show interfaces gigabitEthernet slpp 3/13,4/13,4/26

Results:

```
=======================================================
                          Port Interface
=======================================================

PORT        PKT-RX      PKT-RX      INCOMING    SLPP PDU
NUM                     THRESHOLD   VLAN ID     ORIGINATOR
-------------------------------------------------------
3/13        enabled     5
4/13        enabled     5
4/26        enabled     5
```

On each VSP 9000 in the switch cluster verify the following information:

Option	Verify
PORT NUM	Displays the port numbers for SMLT ports.
PKT-RX	Displays as ***enabled*** for all SMLT ports. The value ***false*** indicates that SLPP is disabled for the port.
PKT-RX THRESHOLD	Displays as ***5*** for each SMLT/SLT port on 8000-1 and ***50*** for each SMLT/SLT port on ERS6800-2.

If port 4/13 is disabled on either VSP-1 or VSP-2 due to either switch receiving its own SLPP-PDU, a message is logged and a trap will be issued. The following is an example of log message received on VSP-1 upon detecting its own SLPP-PDU caused by a loop in the network.

- ***show logging file tail***

```
CPU6 [03/02/06 15:41:15] SNMP INFO Slpp port down(SlppRxPort = 269, SlppRxVlan =
1000, SlppIncomingVlanId = 1000, SlppSrcMacAddress = 00:01:81:28:84:00)
CPU6 [03/02/06 15:41:15] SNMP INFO Smlt Link Down Trap(SmltId=10)
CPU6 [03/02/06 15:41:15] SNMP INFO Smlt Link Up Trap(SmltId=10)
CPU6 [03/02/06 15:41:15] SNMP INFO Smlt Link Down Trap(SmltId=10)
CPU6 [03/02/06 15:41:15] SNMP INFO Port 4/13 is a trunk port
CPU6 [03/02/06 15:41:15] SNMP INFO Link Down(4/13) due to slpp
CPU6 [03/02/06 15:41:15] SW WARNING slppRx: SLPP packet received Rx-Vlan 1000,
Rx-
Port 4/13, PDU-Vlan 1000, SRC-Mac 00:01:81:28:84:00
```

Also, you view the port state by using the following command

- ***show interfaces gigabitEthernet state 4/13***

```
================================================================
                          Port State
================================================================
PORT NUM    ADMINSTATUS   PORTSTATE    REASON      DATE
----------------------------------------------------------------
4/13          up            down          SLPP        03/02/06 15:41:15
```

NOTE: To bring port 4/13 back up, you must disable and then re-enable the port using the following commands:

- `VSP-1:1(config)#`***`interface gigabitEthernet 4/13`***
- `VSP-1:1(config-if)#`***`shutdown`***
- `VSP-1:1(config-if)#`***`no shutdown`***
- `VSP-1:1(config-if)#`***`exit`***

If you wish, you can also bring the port(s) back up automatically by using the following command:

- `VSP-1:1(config)#`***`interface gigabitEthernet 4/13`***
- `VSP-1:1(config-if)#`***`auto-recover-port enable`***
- `VSP-1:1(config-if)#`***`exit`***

NOTE: Although you can configure a port to bring it back up automatically, it is not recommended to enable this feature and use the default setting of disable.

2.2 Configuration – ERS 8600/8800 Layer 2 SMLT Triangle Switch Cluster Configuration

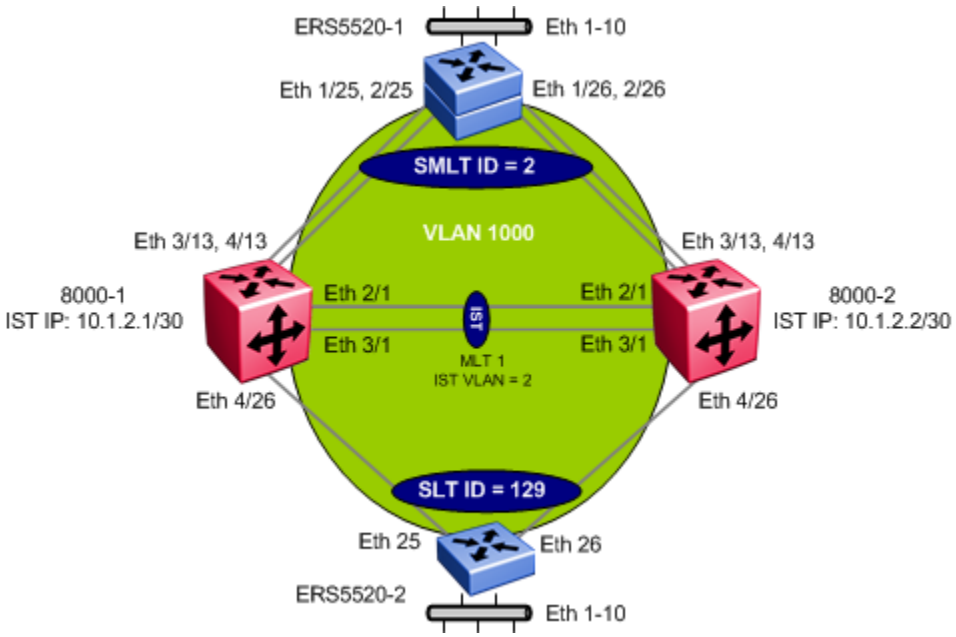


Figure 3: ERS 8600/8800 Layer 2 Triangle SMLT Configuration with SLPP and Ext-CP-Limit

For this example, we will configure the SMLT switch cluster with the following:

- IST
  - IST VLAN 2 using MLT ID = 1 assuming the SMLT cluster is configured for mixed mode (R-modules and non R-modules)
  - Tagged port members 2/1 and 3/1
  - All IST ports are Gigabit Ethernet ports using default setting of Autonegotiation enable
  - VLACP using the recommend reserved multicast MAC (01:80:C2:00:00:0F), long timers, and slow-periodic-time of 10,000 ms
- SMLT and SLT
  - SMLT VLAN 1000
  - 8000-1 is assumed to the SMLT Primary switch while 8000-2 is the SMLT Secondary switch
  - MLT and SMLT ID of 2 for ERS5520-1 with tagged port member 3/13 and 4/13
  - SLT ID of 129 for ERS5520-2 with tagged port member 4/26
  - All SMLT and SLT ports are Gigabit Ethernet ports using default setting of Autonegotiation enable
  - Enable SLPP
  - Enable VLACP with recommended reserved multicast MAC address and with short timers of 500ms and set timeout scale to 5

- Enable “Discard Untagged Frames” on all Access SMLT/SLT port members, this includes ports 3/13, 4/13, and 4/26
- Disable STP on all SMLT ports (default setting when SMLT is enabled)
- Set the recommended moderate CP Limit settings for broadcast and multicast traffic
- Enable Extended CP-Limit with SoftDown option
  - Maximum ports to check to 5
  - SoftDown utilization threshold set to 10%

- Access Switches

  On both ERS5520-1 and ERS5520-2, the following will be configured:

  - Broadcast and multicast rate limiting with a threshold to 10%
  - Enable Spanning Tree Fast Start and BPDU filtering on all edge ports
  - Disable Spanning Tree on MLT core ports to SMLT Cluster switches
  - BPDU filtering on all edge ports
  - VLAN Tagging on MLT access trunk ports

For this example, the IST was created using GE ports on 8630GBR I/O modules. It’s important to note that SMLT does not have any restrictions on the port types (copper, fiber, GE, 10GE) or I/O modules (E, M or R) that can be used for IST and SMLT connections. The only restriction is that the IST and SMLT ports must be of the same link speed (i.e. you cannot use 10GE and 1GE ports to form an IST or an SMLT) and same physical port type.

It is recommended to use the lowest MLT number for the IST. For the VLAN ID, it makes no difference if you use a low or high number.

It is recommended to start the SLT numbering at 129 up to 512 even though you can use any number from 1 to 512. As of software release 4.1 for the ERS 8600/8800, with R-mode enabled, up to 128 link aggregation groups (MLT or 802.3ad/LACP) are supported using ID’s starting at 1 up to 128. This is to avoid taking away a valid MLT ID that can be used for either a MLT or SMLT instance.

2.2.1 Configuration – ERS 8600/8800 Layer 2 Switch Cluster

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

2.2.1.1 Create VLANs

The following port based VLANs will be configured on the SMLT Switch cluster

- VLAN 2 to be used by the Inter Switch Trunk (IST)
- VLAN 1000 to be used at a Layer 2 level to ERS5520-1 and ERS5520-2 for connecting users.

ERS 8000 SMLT Cluster: Create VLANs 2 and 1000

8000-1:

```
8000-1:5(config)#vlan create 2 name IST type port 1
8000-1:5(config)#vlan create 1000 name Services type port 1
```

8000-2:

```
8000-2:5# config vlan 2 create byport 1 name IST
8000-2:5# config vlan 1000 create byport 1 name Services
```

The IST and SMLT port numbers will be added when the corresponding MLT is created.

2.2.1.2 Change fdb aging timer for VLAN 1000

ERS 8000 SMLT Cluster: Change fdb aging timer on VLAN 1000 to recommended value of 21601 seconds

8000-1:

```
8000-1:5(config)#vlan mac-address-entry 1000 aging-time 21601
```

8000-2:

```
8000-2:5# config vlan 1000 fdb-entry aging-time 21601
```

2.2.1.3 Create IST

Multilink Trunking 1 (MLT 1) will be used for the IST with port members 2/1 and 3/1. 802.1Q tagging will be enabled on all IST port members and Spanning Tree will be disabled on all IST port members by default. VLACP will be enabled on the IST trunk.

It is recommended to use the reserved multicast MAC address of 01:80:c2:00:00:0f for the VLACP MAC address.

By default, unless you specify the VLACP timeout, the default setting of *long* will be used. Hence, we do not have to configure the VLACP timeout for the IST.

ERS 8000 SMLT Cluster: Step 1 - Create MLT 1 for IST

8000-1:

```
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)#mlt 1 encapsulation dot1q
8000-1:5(config)#vlan mlt 2 1
```

8000-2:

```
8000-2:5# config mlt 1 create
8000-2:5# config mlt 1 name IST
8000-2:5# config mlt 1 add port 2/1,3/1
8000-2:5# config vlan 2 add-mlt 1
```

ERS 8000 SMLT Cluster: Step 2 - Create IST

8000-1:

```
8000-1:5(config)#interface vlan 2
8000-1:5(config-if)#ip address 10.1.2.1 255.255.255.252
8000-1:5(config-if)#exit
8000-1:5(config)#interface mlt 1
8000-1:5(config-mlt)#ist peer-ip 10.1.2.2 vlan 2
8000-1:5(config-mlt)#ist enable
8000-1:5(config-mlt)#end
```

8000-2:

```
8000-2:5# config vlan 2 ip create 10.1.2.2/30
8000-2:5# config mlt 1 ist create ip 10.1.2.1 vlan-id 2
8000-2:5# config mlt 1 ist enable
```

ERS 8000 SMLT Cluster: Step 3 - Enable VLACP

8000-1:

```
8000-1:5(config)# interface gigabitEthernet 2/1,3/1
8000-1:5(config-if)#vlacp slow-periodic-time 10000
8000-1:5(config-if)#vlacp enable
8000-1:5(config-if)#exit
```

8000-2:

```
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
```

2.2.1.4 SMLT-2 to ERS5520-1

ERS 8000 SMLT Cluster: Create SMLT-2

8000-1:

```
8000-1:5(config)#mlt 2
8000-1:5(config)#mlt 2 name ERS5520-1
8000-1:5(config)#mlt 2 member 3/13,4/13 vlan 1000
8000-1:5(config)#mlt 2 encapsulation dot1q
8000-1:5(config)#interface mlt 2
8000-1:5(config-mlt)#smlt 2
8000-1:5(config-mlt)#end
```

8000-2:

```
8000-2:5# config mlt 2 create
8000-2:5# config mlt 2 name ERS5520-1
8000-2:5# config mlt 2 perform-tagging enable
8000-2:5# config mlt 2 add port 3/13,4/13
8000-2:5# config vlan 1000 add-mlt 2
8000-2:5# config mlt 2 smlt create smlt-id 2
```

2.2.1.5 SLT-129 to ERS5520-2

ERS 8000 SMLT Cluster: Create SLT-129

8000-1:

```
8000-1:5(config)#vlan ports 4/26 tagging tagAll
8000-1:5(config)#vlan members add 1000 4/26
8000-1:5(config)#vlan members remove 1 4/26
8000-1:5(config)#interface gigabitEthernet 4/26
8000-1:5(config-if)#smlt 129
8000-1:5(config-if)#exit
```

8000-2:

```
8000-2:5# config ethernet 4/26 perform-tagging enable
8000-2:5# config vlan 1000 ports add 4/26
8000-2:5# config vlan 1 ports remove 4/26
8000-2:5# config ethernet 4/26 smlt 129 create
```

2.2.1.6 Add VLAN 1000 to IST

ERS 8000 SMLT Cluster: Add VLAN 1000 to IST

8000-1:

```
8000-1:5(config)#vlan mlt 1000 1
```

8000-2:

```
8000-2:5# config vlan 1000 add-mlt 1
```

2.2.1.7 CP Limit – SMLT port members

CP Limit will be enabled on all the SMLT Access port members. For this example, we will select the moderate recommendations for CP-Limit.

ERS 8000 SMLT Cluster: CP Limit

8000-1:

```
8000-1:5(config)#interface gigabitEthernet 3/13,4/13,4/26
8000-1:5(config-if)#cp-limit multicast 2500 broadcast 2500
```

8000-2:

```
8000-2:5# config ethernet 3/13,4/13,4/26 cp-limit enable multicast-limit 2500
broadcast-limit 2500
```

2.2.1.8 SLPP

SLPP will be enabled globally and only on the SMLT access ports 3/13 and 4/13 and SLT access port 4/26 for VLAN 1000. On the SMLT primary switch we will set the SLPP packet-rx-threshold to 5, while on the SMLT secondary switch we will set the SLPP packet-rx-threshold to 50. For this example, we will pick 8000-1 as the primary switch.

The recommended SLPP receive threshold value for the primary switch is 5 and 50 for the secondary switch in an SMLT cluster.

SLPP should only be enabled on the SMLT access ports and not on the IST port members.

ERS 8000 SMLT Cluster: Enable SLPP

8000-1:

```
8000-1:5(config)#slpp vid 1000
8000-1:5(config)#slpp enable
8000-1:5(config)# interface gigabitEthernet 3/13,4/13,4/26
ERS8600:5(config-if)#slpp packet-rx-threshold 5
ERS8600:5(config-if)# slpp packet-rx
ERS8600:5(config-if)#exit
```

8000-2:

```
8000-2:5# config slpp add 1000
8000-2:5# config slpp operation enable
8000-2:5# config ethernet 3/13,4/13,4/26 slpp packet-rx enable
8000-2:5# config ethernet 3/13,4/13,4/26 slpp packet-rx-threshold 50
```

2.2.1.9 VLACP

As the access switches, ERS5520-1 and ERS5520-2, supports VLACP, we will enable this feature 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.

ERS 8000 SMLT Cluster: Enable VLACP

8000-1:

```
8000-1:5(config)#interface gigabitEthernet 3/13,4/13,4/26
8000-1:5(config-if)#vlacp timeout short
8000-1:5(config-if)#vlacp timeout-scale 5
8000-1:5(config-if)#vlacp fast-periodic-time 500
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:

```
8000-2:5# config ethernet 3/13,4/13,4/26 vlacp fast-periodic-time 500
8000-2:5# config ethernet 3/13,4/13,4/26 vlacp timeout short
8000-2:5# config ethernet 3/13,4/13,4/26 vlacp timeout-scale 5
8000-2:5# config ethernet 3/13,4/13,4/26 vlacp macaddress 01:80:c2:00:00:0f
8000-2:5# config ethernet 3/13,4/13,4/26 vlacp enable
```

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

2.2.1.10 Ext-CP Limit

Ext-CP Limit will be enabled globally and on the SMLT access ports in the SMLT switch cluster. The SoftDown option will be used with the bandwidth utilization threshold set to 10%.

ERS 8000 SMLT Cluster: Enable EXT-CP-Limit

8000-1:

```
8000-1:5(config)#sys ext-cp-limit
8000-1:5(config)#sys ext-cp-limit max-ports-to-check 5
8000-1:5(config)#sys ext-cp-limit trap-level Normal
8000-1:5(config)#interface gigabitEthernet 3/13,4/13,4/26
8000-1:5(config-if)#ext-cp-limit softDown threshold-util-rate 10
8000-1:5(config-if)#exit
```

8000-2:

```
8000-2:5# config sys ext-cp-limit extcplimit enable
8000-2:5# config sys ext-cp-limit max-ports-to-check 5
8000-2:5# config sys ext-cp-limit trap-level Normal
8000-2:5# config ethernet 3/13,4/13,4/26 ext-cp-limit SoftDown threshold-util-rate 10
```

2.2.1.11 Discard Untagged Frames

It is recommended to enable discard untagged frames on all IST and SMLT ports.

ERS 8000 SMLT Cluster: Enable Discard Untagged Frames

8000-1:

```
8000-1:5(config)#interface gigabitEthernet 2/1,3/1,3/13,4/13,4/26
8000-1:5(config-if)#untagged-frames-discard
8000-1:5(config-if)#exit
```

8000-2:

```
8000-2:5# config ethernet 2/1,3/1,3/13,4/13,4/26  untagged-frames-discard enable
```

2.2.2 Configuration - Edge Switch

2.2.2.1 Create VLAN

Edge switch: Create VLAN 1000

5520-1:

```
5520-1(config)#vlan create 1000 name Services type port cist
5520-1(config)#vlan members remove 1 1/1-10,1/25-26,2/1-10,2/25-26
5510-1(config)#vlan ports 1/25-26,2/25-26 tagging tagall
5520-1(config)#vlan members 1000 1/1-10,1/25-26,2/1-10,2/25-26
```

5520-2:

```
5520-2(config)#vlan create 1000 name Services type port cist
5520-2(config)#vlan members remove 1 1-10,25-26
5520-2(config)#vlan ports 25-26 tagging tagall
5520-2(config)#vlan members 1000 1-10,25-26
```

2.2.2.2 Create MLT

Edge switch: Create MLT 1

5520-1:

```
5520-1(config)# mlt 1 member 1/25-26,2/25-26 learning disable
5520-1(config)# mlt 1 enable
```

5520-2:

```
5520-2(config)# mlt 1 member 25,26 learning disable
5520-2(config)#mlt 1 enable
```

2.2.2.3 VLACP

Please note that on an ERS 5000 switch, the VLACP MAC is entered as a hexadecimal value in the format of 'H.H.H'. Hence, the recommended VLACP MAC value of 01:80:c2:00:00:0f is entered as *180.c200.f*.

Edge switch: Enable VLACP

5520-1:

```
5520-1(config)#vlacp macaddress 180.c200.f
5520-1(config)#vlacp enable
5520-1(config)#interface fastEthernet 1/25-26,2/25-26
5520-1(config-if)#vlacp timeout short
```

```
5520-1(config-if)#vlacp timeout-scale 5
5520-1(config-if)#vlacp enable
5520-1(config-if)#exit
```

5520-2:

```
5520-2(config)#vlacp macaddress 180.c200.f
5520-2(config)#vlacp enable
5520-2(config)#interface fastEthernet 25,26
5520-2(config-if)#vlacp timeout short
5520-2(config-if)#vlacp timeout-scale 5
5520-2(config-if)#vlacp enable
5520-2(config-if)#exit
```

2.2.2.4 Enable Spanning Tree Fast Start and BPDU filtering on all Access Ports

Edge switch: Enable STP fast start and BPDU Filtering

5520-1:

```
5520-1(config)#interface fastEthernet 1/1-10,2/1-10
5520-1(config-if)#spanning-tree learning fast
5520-1(config-if)#spanning-tree bpdu-filtering timeout 0
5520-1(config-if)#spanning-tree bpdu-filtering enable
5520-1(config-if)#exit
```

5520-2:

```
5520-2(config)#interface fastEthernet 1-10
5520-2(config-if)#spanning-tree learning fast
5520-2(config-if)#spanning-tree bpdu-filtering timeout 0
5520-2(config-if)#spanning-tree bpdu-filtering enable
5520-2(config-if)#exit
```

2.2.2.5 Enable Rate Limiting

Edge switch: Enable Rate Limiting to 10% of total traffic for both broadcast and multicast traffic

5520-1:

```
5520-1(config)#interface fastEthernet all
5520-1(config-if)#rate-limit port 1/1-10,2/1-10 both 10
5520-1(config-if)#exit
```

5520-2:

```
5520-2(config)#interface fastEthernet all
5520-2(config-if)#rate-limit port 1-10 both 10
5520-2(config-if)#exit
```

Please note that the rate limit parameter on the ERS 5000 is expressed as percentage of total traffic. The values used in this example are just a suggestion and may vary depending on your needs.

When measuring the Broadcast Rate Limit, note that the rate limiting feature displays a calculation based on packets rather than octets. To obtain the actual value, use the following equation (the average packet size is 500 bytes):

(Line speed (bit/sec)/ Average packet size x 8) X (Rate Limit/100) = Packets per second

2.2.2.6 Discard Untagged Frames

Edge switch: Enable Discard Untagged Frames

5520-1:

```
5520-1(config)#vlan ports 1/25-26,2/25-26 filter-untagged-frame enable
```

5520-2:

```
5520-2(config)#vlan ports 25-26 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.

2.2.3 Configuration File

8000-1	8000-2
config terminal cfm ethertype 0x8902 # # CLI CONFIGURATION # telnet-access login-timeout 600 prompt "8000-1" password password-history 3 # # SYSTEM CONFIGURATION # sys ext-cp-limit sys ext-cp-limit max-ports-to-check 5 sys ext-cp-limit trap-level Normal # # LACP CONFIGURATION # vlacp enable # # PORT CONFIGURATION - PHASE I # interface GigabitEthernet 3/13 ext-cp-limit SoftDown threshold-util-rate 10 exit interface GigabitEthernet 4/13 ext-cp-limit SoftDown threshold-util-rate 10 exit	config cfm ethertype 0x8902 # # CLI CONFIGURATION # cli prompt "8000-2" cli password password-history 3 # # SYSTEM CONFIGURATION # sys ext-cp-limit extcplimit enable sys ext-cp-limit max-ports-to-check 5 sys ext-cp-limit trap-level Normal # # LACP CONFIGURATION # vlacp enable # # PORT CONFIGURATION - PHASE I # ethernet 3/13 ext-cp-limit SoftDown threshold-util-rate 10 ethernet 4/13 ext-cp-limit SoftDown threshold-util-rate 10 ethernet 4/26 ext-cp-limit SoftDown threshold-util-rate 10 ethernet 4/26 perform-tagging enable # # MLT CONFIGURATION #

```
interface GigabitEthernet 4/26
encapsulation dot1q
ext-cp-limit SoftDown threshold-util-rate 10
exit

#
# MLT CONFIGURATION
#

mlt 1 enable name "IST"
mlt 1 member 2/1,3/1
mlt 1 encapsulation dot1q
mlt 2 enable
mlt 2 member 3/13,4/13
mlt 2 encapsulation dot1q
interface mlt 1
ist peer-ip 10.1.2.2 vlan 2
ist enable
exit
interface mlt 2
smlt 2
exit

#
# VLAN CONFIGURATION - PHASE I
#

vlan create 2 name "IST" type port 1 color 1
vlan mlt 2 1
vlan members 2 2/1,3/1 portmember
interface Vlan 2
ip address 10.1.2.1 255.255.255.252 3
exit
vlan create 1000 name "Services" type port 1
color 2
vlan mlt 1000 1
vlan mlt 1000 2
vlan members 1000 2/1,3/1,3/13,4/13 portmember
vlan mac-address-entry 1000 aging-time 21601
exit

#
```

```
mlt 1 create
mlt 1 add ports 2/1,3/1
mlt 1 name "IST"
mlt 1 perform-tagging enable
mlt 1 ist create ip 10.1.2.1 vlan-id 2
mlt 1 ist enable
mlt 2 create
mlt 2 add ports 3/13,4/13
mlt 2 perform-tagging enable
mlt 2 smlt create smlt-id 2

#
# VLAN CONFIGURATION - PHASE I
#

vlan 2 create byport 1 name "IST"
vlan 2 add-mlt 1
vlan 2 ports add 2/1,3/1 member portmember
vlan 2 ip create 10.1.2.2/255.255.255.252
mac_offset 0
vlan 1000 create byport 1 name "Services"
vlan 1000 add-mlt 1
vlan 1000 add-mlt 2
vlan 1000 ports add 2/1,3/1,3/13,4/13 member
portmember
vlan 1000 fdb-entry aging-time 21601

#
# PORT CONFIGURATION - PHASE II
#

ethernet 2/1 untagged-frames-discard enable
ethernet 2/1 default-vlan-id 2
ethernet 2/1 stg 1 stp disable
ethernet 2/1 vlacp  macaddress
01:80:c2:00:00:0f
ethernet 2/1 vlacp  enable
ethernet 2/1 vlacp  slow-periodic-time 10000
ethernet 2/2 default-vlan-id 0
ethernet 3/1 untagged-frames-discard enable
```

```
# PORT CONFIGURATION - PHASE II
#


interface GigabitEthernet 2/1
untagged-frames-discard
default-vlan-id 2
vlacp slow-periodic-time 10000 funcmac-addr
01:80:c2:00:00:0f
vlacp enable
no spanning-tree stp 1 enable
exit
interface GigabitEthernet 3/1
untagged-frames-discard
default-vlan-id 2
vlacp slow-periodic-time 10000 funcmac-addr
01:80:c2:00:00:0f
vlacp enable
no spanning-tree stp 1 enable
exit
interface GigabitEthernet 3/13
untagged-frames-discard
default-vlan-id 1000
cp-limit multicast 2500 broadcast 2500
slpp packet-rx
slpp packet-rx-threshold 5
vlacp fast-periodic-time 500 timeout short
timeout-scale 5 funcmac-addr 01:80:c2:00:00:0f
vlacp enable
no spanning-tree stp 1 enable
exit
interface GigabitEthernet 4/13
untagged-frames-discard
default-vlan-id 1000
cp-limit multicast 2500 broadcast 2500
slpp packet-rx
slpp packet-rx-threshold 5
vlacp fast-periodic-time 500 timeout short
timeout-scale 5 funcmac-addr 01:80:c2:00:00:0f
vlacp enable
no spanning-tree stp 1 enable
exit
interface GigabitEthernet 4/26
untagged-frames-discard
ethernet 3/1 default-vlan-id 2
ethernet 3/1 stg 1 stp disable
ethernet 3/1 vlacp  macaddress
01:80:c2:00:00:0f
ethernet 3/1 vlacp  enable
ethernet 3/1 vlacp  slow-periodic-time 10000
ethernet 3/13 untagged-frames-discard enable
ethernet 3/13 default-vlan-id 1000
ethernet 3/13 cp-limit enable multicast-limit
2500 broadcast-limit 2500
ethernet 3/13 slpp packet-rx enable
ethernet 3/13 slpp packet-rx-threshold 50
ethernet 3/13 stg 1 stp disable
ethernet 3/13 vlacp  macaddress
01:80:c2:00:00:0f
ethernet 3/13 vlacp  enable
ethernet 3/13 vlacp  fast-periodic-time 500
ethernet 3/13 vlacp  timeout short
ethernet 3/13 vlacp  timeout-scale 5
ethernet 4/13 untagged-frames-discard enable
ethernet 4/13 default-vlan-id 1000
ethernet 4/13 cp-limit enable multicast-limit
2500 broadcast-limit 2500
ethernet 4/13 slpp packet-rx enable
ethernet 4/13 slpp packet-rx-threshold 50
ethernet 4/13 stg 1 stp disable
ethernet 4/13 vlacp  macaddress
01:80:c2:00:00:0f
ethernet 4/13 vlacp  enable
ethernet 4/13 vlacp  fast-periodic-time 500
ethernet 4/13 vlacp  timeout short
ethernet 4/13 vlacp  timeout-scale 5
ethernet 4/26 untagged-frames-discard enable
ethernet 4/26 default-vlan-id 1000
ethernet 4/26 cp-limit enable multicast-limit
2500 broadcast-limit 2500
ethernet 4/26 slpp packet-rx enable
ethernet 4/26 slpp packet-rx-threshold 50
ethernet 4/26 stg 1 stp disable
ethernet 4/26 smlt 129 create
ethernet 4/26 vlacp  macaddress
01:80:c2:00:00:0f
ethernet 4/26 vlacp  enable
ethernet 4/26 vlacp  fast-periodic-time 500
```

```
default-vlan-id 1000
cp-limit multicast 2500 broadcast 2500
slpp packet-rx
slpp packet-rx-threshold 5
smlt 129
vlacp fast-periodic-time 500 timeout short
timeout-scale 5 funcmac-addr 01:80:c2:00:00:0f
vlacp enable
no spanning-tree stp 1 enable
exit


#
# SLPP CONFIGURATION
#


slpp enable
slpp vid 1000
```

```
ethernet 4/26 vlacp  timeout short
ethernet 4/26 vlacp  timeout-scale 5


#
# SLPP CONFIGURATION
#


slpp operation enable
slpp add 1000
```

2.2.4 Verify Operations

2.2.4.1 Verify MLT Configuration

Verify that the MLT instances is configured correctly and is functioning by issuing the following command:

ACLI: ***show mlt***

CLI: ***show mlt info***

Results:

```
==============================================================================
                                    Mlt Info
==============================================================================

                          PORT     SVLAN  MLT    MLT         PORT         VLAN
MLTID IFINDEX NAME        TYPE     TYPE   ADMIN  CURRENT     MEMBERS      IDS
1     4098    IST         trunk    normal ist    ist          2/1,3/1      2 1000
2     4100    5520-1      trunk    normal smlt   smlt       3/13,4/13      1000


                MULTICAST              DESIGNATED   LACP      LACP
MLTID IFINDEX   DISTRIBUTION  NT-STG   PORTS        ADMIN     OPER
------------------------------------------------------------------------------
1       4098      disable       enable   2/1          disable   down
2       4100      disable       enable   3/13         disable   down
```

On each ERS 8800/8600 in the switch cluster verify the following information:

Option	Verify
VLAN IDS	Verify that the VLAN ids assigned to the IST and SMLT MLT are correct: • IST MLT 1: Member of VLANs ***1000*** & ***2*** with port members ***2/1 and 3/1*** • MLT 2: Member of VLAN ***1000*** with port member ***3/13*** and ***4/13***
MLT ADMIN	Displays as ***smlt*** or ***ist*** if configured correctly. The value ***normal*** indicates that the IST or SMLT is not configured.
MLT CURRENT	Displays as ***smlt*** or ***ist*** if the SMLT or IST is operational.
PORT TYPE	Displays as ***trunk*** for all IST and SMLT ports and will pass tagged frames. The value ***access*** indicates that the port will pass untagged frames.

2.2.4.2 Virtual LANs (VLANs):

Verify the VLAN port assignments and 802.1Q tagging settings by issuing the following command:

ACLI: ***show interfaces gigabitEthernet vlan***

CLI: ***show ports info vlans port 2/1,3/1,3/13,4/13,4/26***

Results:

```
==========================================================================
                          Port Vlans
==========================================================================
PORT           DISCARD DISCARD    DEFAULT VLAN    PORT      UNTAG
NUM    TAGGING TAGFRAM UNTAGFRAM VLANID  IDS     TYPE      DEFVLAN
--------------------------------------------------------------------------
2/1    enable  false   true      2       2 1000  normal    disable
3/1    enable  false   true      2       2 1000  normal    disable
3/13   enable  false   true      1000    1000    normal    disable
4/13   enable  false   true      1000    1000    normal    disable
4/26   enable  false   true      1000    1000    normal    disable
```

On each ERS 8800/8600 in the switch cluster verify the following information:

Option	Verify
VLAN IDS	Verify that the VLAN ids assigned to the IST and SMLT ports are correct: • IST Ports: Member of VLANs ***1000*** & ***2***. • SMLT 2 Ports: Member of VLAN ***1000***. • SLT 129 Ports: Member of VLAN ***1000***.
TAGGING	Displays as ***enable*** for all IST and SMLT ports. The value ***disable*** indicates that the port is in an untagged mode.
DISCARD UNTAGFRAM	Displays as ***true*** for all IST and SMLT ports. The value ***false*** indicates that the port will pass untagged frames.

2.2.4.3 Inter Switch Trunk (IST):

Verify that the IST is configured correctly and is functioning by issuing the following command:

ACLI: ***show ist mlt***

CLI: ***show mlt ist info***

Results:

```
                        Mlt IST Info
=============================================================
MLT    IP                   VLAN      ENABLE    IST
ID     ADDRESS              ID        IST       STATUS
-------------------------------------------------------------
1      10.1.2.2             2         true      up
```

On each ERS 8800/8600 in the switch cluster verify the following information:

Option	Verify
MLT ID	Verify the MLT ID assigned to the IST is correct.
IP ADDRESS	Verify that the IST peer IP address is correct: • 8000-1: Will display the peer IP ***10.1.2.2*** • 8000-2: Will display the peer IP ***10.1.2.1***
VLAN ID	Displays the IST VLAN which for this example is VLAN 2.
ENABLE IST	Displays as ***true***. The value ***false*** indicates that the IST is not enabled.
IST STATUS	Displays as ***up***. The value ***down*** indicates that the IST is not operational.

2.2.4.4 Split MultiLink Trunking (SMLT):

Verify that SMLT is functioning correctly by issuing the following command:

ACLI: ***show smlt mlt, show smlt gigabitethernet***

CLI: ***show smlt info***

Results:

```
==========================================
                    Mlt SMLT Info
==========================================
MLT    SMLT     ADMIN    CURRENT
ID     ID       TYPE     TYPE
------------------------------------------
2      2        smlt     smlt

==============================================================================
                         Port SMLT Info
==============================================================================
PORT   SMLT     ADMIN    CURRENT
NUM    ID       TYPE     TYPE
------------------------------------------------------------------------------
4/26   129      smlt     smlt
```

On each ERS 8800/8600 in the switch cluster verify the following information:

Option	Verify
SMLT ID	Verify that the SMLT IDs match the MLT IDs. For the SLT, port 4/26 should display SLT ID 129.
ADMIN TYPE	Displays as ***smlt*** for each SMLT/SLT ID. A ***normal*** value indicates that the MLT is not configured as an SMLT trunk.
CURRENT TYPE	Displays as ***smlt*** for each SMLT/SLT ID. A ***normal*** value indicates that the SMLT ports are disconnected or the SMLT IDs are mis-configured.

2.2.4.5 Virtual Link Aggregation Control Protocol (VLACP):

Step 1: Verify that VLACP is globally enabled by using the following command:

ACLI: ***show vlacp***

CLI: ***show vlacp info***

Results:

```
================================================================================
                          Vlacp Global Information
================================================================================

                  SystemId: 00:01:81:28:84:00
                     Vlacp: enable
```

On each ERS 8800/8600 in the switch cluster verify the following information:

Option	Verify
Vlacp	Displays as ***enable***. The value ***disable*** indicates that VLACP is globally disabled on the switch.
SystemId	Displays as ***00:01:81:28:84:00***. Please note that the VLACP reserved MAC shows up at the interface level.

Step 2: Verify the IST and SMLT per port VLACP settings by issuing the following command:

ACLI: ***show vlacp interface gigabitethernet 2/1,3/1,3/13,4/13***

CLI: ***show ports info vlacp port 2/1,3/1,3/13,4/13***

Results:

```
================================================================================
                            VLACP Information
================================================================================
INDEX ADMIN   OPER    PORT   FAST    SLOW    TIMEOUT TIMEOUT ETHER      MAC
      ENABLED ENABLED STATE  TIME    TIME    TIME    SCALE   TYPE       ADDR
--------------------------------------------------------------------------------
2/1   true    true    UP     200     10000   long    3       0x8103     01:80:c2:00:00:0f
3/1   true    true    UP     200     10000   long    3       0x8103     01:80:c2:00:00:0f
3/13  true    true    UP     500     30000   short   5       0x8103     01:80:c2:00:00:0f
4/13  true    true    UP     500     30000   short   5       0x8103     01:80:c2:00:00:0f
4/26  true    true    UP     500     30000   short   5       0x8103     01:80:c2:00:00:0f
```

On each ERS 8800/8600 in the switch cluster verify the following information:

Option	Verify
ADMIN ENABLED	Displays as ***true*** for the IST, SMLT-2, and SLT-129 ports. The value ***false*** indicates that VLACP is disabled for the port.
OPER ENABLED	Displays as ***true*** for the IST SMLT-2, and SLT-129 ports. The value ***false*** indicates that VLACP is not operational on the port.
FAST TIME	Displays as ***500*** for the SMLT-2 and SLT-129 ports. The value must match for each switch port in the link pair.
SLOW TIME	Displays as ***10000*** for the IST port members. If not, please change the VLACP slow-periodic-time setting to this value.
TIMEOUT TIME	Displays as ***long*** for the IST ports and ***short*** for SMLT-2 and SLT-129 ports. This value must match for each switch port in the link pair.
TIMEOUT SCALE	Displays as ***5*** for the SMLT-2 and SLT-129 ports. The default timeout scale of ***3*** will be displayed for the IST port members 2/1 and 3/1.
MAC ADDR	The VLACP MAC address is assigned to each IST, SMLT-2 and SLT-129 port members: • IST port 2/1 and 3/1: ***01:80:c2:00:00:0f***. • SMLT-2 & SLT-129 ports: ***01:80:c2:00:00:0f***. The VLACP MAC address must match for each switch port in the link pair.

2.2.4.6 Simple Loop Prevention Protocol (SLPP):

Step 1: Verify that SLPP is globally enabled on the switch by issuing the following command:

ACLI & CLI: ***show slpp***

Results:

```
================================================================================
                              SLPP Info
================================================================================
                 etherType (hex) : 0x8104
                       operation : enabled
                     tx-interval : 500
                            vlan : 1000
```

On each ERS 8800/8600 in the switch cluster verify the following information:

Option	Verify
operation	Displays as ***enable***. The value ***disable*** indicates that SLPP is globally disabled on the switch.
vlan	Displays as ***1000*** indicating SLPP is enabled for VLAN 1000.

Step 2: Verify the SLPP settings by issuing the following command:

ACLI: ***show interfaces gigabitEthernet slpp 3/13,4/13,4/26***

CLI: ***show ports info slpp port 3/13,4/13,4/26***

Results:

```
                        Port Interface
=======================================================


PORT        PKT-RX      PKT-RX      INCOMING    SLPP PDU
NUM                     THRESHOLD   VLAN ID     ORIGINATOR
-------------------------------------------------------------
3/13        enabled     5
4/13        enabled     5
4/26        enabled     5
```

On each ERS 8800/8600 in the switch cluster verify the following information:

Option	Verify
PORT NUM	Displays the port numbers for SMLT ports.
PKT-RX	Displays as ***enabled*** for all SMLT ports. The value ***false*** indicates that SLPP is disabled for the port.
PKT-RX THRESHOLD	Displays as ***5*** for each SMLT/SLT port on 8000-1 and ***50*** for each SMLT/SLT port on ERS6800-2.

If port 4/13 is disabled on either 8000-1 or 8000-2 due to either switch receiving its own SLPP-PDU, a message is logged and a trap will be issued. The following is an example of log message received on 8000-1 upon detecting its own SLPP-PDU caused by a loop in the network.

- ACLI: 8000-1:5#***show logging file tail***
- CLI: 8000-1:5# ***show log file tail***

```
CPU6 [03/02/06 15:41:15] SNMP INFO Slpp port down(SlppRxPort = 269, SlppRxVlan =
```

```
1000, SlppIncomingVlanId = 1000, SlppSrcMacAddress = 00:01:81:28:84:00)
CPU6 [03/02/06 15:41:15] SNMP INFO Smlt Link Down Trap(SmltId=10)
CPU6 [03/02/06 15:41:15] SNMP INFO Smlt Link Up Trap(SmltId=10)
CPU6 [03/02/06 15:41:15] SNMP INFO Smlt Link Down Trap(SmltId=10)
CPU6 [03/02/06 15:41:15] SNMP INFO Port 4/13 is a trunk port
CPU6 [03/02/06 15:41:15] SNMP INFO Link Down(4/13) due to slpp
CPU6 [03/02/06 15:41:15] SW WARNING slppRx: SLPP packet received Rx-Vlan 1000,
Rx-
Port 4/13, PDU-Vlan 1000, SRC-Mac 00:01:81:28:84:00
```

Also, you view the port state by using the following command

- ACLI: 8000-1:5#***show interfaces gigabitEthernet state 4/13***
- CLI: 8000-1:5# ***show port info state port 4/13***

```
================================================================
                          Port State
================================================================
PORT NUM    ADMINSTATUS   PORTSTATE    REASON      DATE
----------------------------------------------------------------
4/13          up            down          SLPP        03/02/06 15:41:15
```

NOTE: To bring port 4/13 back up, you must disable and then re-enable the port using the following commands:

- ACLI
  - 8000-1:5(config)#***interface gigabitEthernet 4/13***
  - 8000-1:5(config-if)#***shutdown***
  - 8000-1:5(config-if)#***no shutdown***
  - 8000-1:5(config-if)#***exit***
- CLI:
  - 8000-1:5# ***config ethernet 4/13 state disable***
  - 8000-1:5# ***config ethernet 4/13 state enable***

If you wish, you can also bring the port(s) back up automatically by using the following command:

- ACLI:
  - 8000-1:5(config)#***interface gigabitEthernet 4/13***
  - 8000-1:5(config-if)#***auto-recover-port enable***
  - 8000-1:5(config-if)#***exit***
- CLI:
  - 8000-1:5# ***config ethernet <slot/port> auto-recover-port enable***

NOTE: Although you can configure a port to bring it back up automatically, it is not recommended to enable this feature and use the default setting of disable.

2.2.4.7 Ext-CP-Limit:

Step 1: Verify that EXT-CP-Limit is globally enabled on each switch by issuing the following command:

ACLI & CLI: ***show sys ext-cp-limit***

Results:

```
extcplimit           : enable
max-ports-to-check   : 5
min-congestion-time  : 3000
port-congestion-time : 5
trap-level           : Normal
```

On each ERS 8800/8600 in the switch cluster verify the following information:

Option	Verify
extcplimit	Displays as ***enable***. The value ***disable*** indicates that EXT-CP-Limit is globally disabled on the switch.
max-ports-to-check	Displays as ***5***. The value **5** indicated the maximum number of ports to check for Ext-CP Limit.

Step 2: Verify the SMLT ports EXT-CP-Limit settings by issuing the following command:

ACLI: ***show interfaces gigabitEthernet ext-cp-limit 2/1,3/1,3/13,4/13,4/26***

CLI: ***show ports info ext-cp-limit port 2/1,3/1,3/13,4/13,4/26***

Results:

```
================================================================================
                        Port Ext-CP-Limit Info
================================================================================
PORT  EXT-CP-LIMIT    UTIL-RATE     SHUTDOWN
--------------------------------------------------------------------------------
2/1   None            50            false
3/1   None            50            false
3/13  SoftDown        10            false
4/13  SoftDown        10            false
4/26  SoftDown        10            false
```

On each ERS 8800/8600 in the switch cluster verify the following information:

Option	Verify
EXT-CP-LIMIT	Displays as ***None*** for IST ports and ***SoftDown*** for all SMLT/SLT ports.
UTIL-RATE	Displays as ***10*** for all SMLT/SLT ports. A different value indicates a different percentage threshold has been defined for the port(s).
SHUTDOWN	Displays as ***false*** for all SMLT/SLT ports. The value ***true*** indicates that EXT-CP-Limit has disabled a port due to excessive traffic exceeding the specified threshold from the port was impacting the CPU.

2.3 Configuration – VSP 9000 Triangle Switch Cluster using VRRP with Backup Master

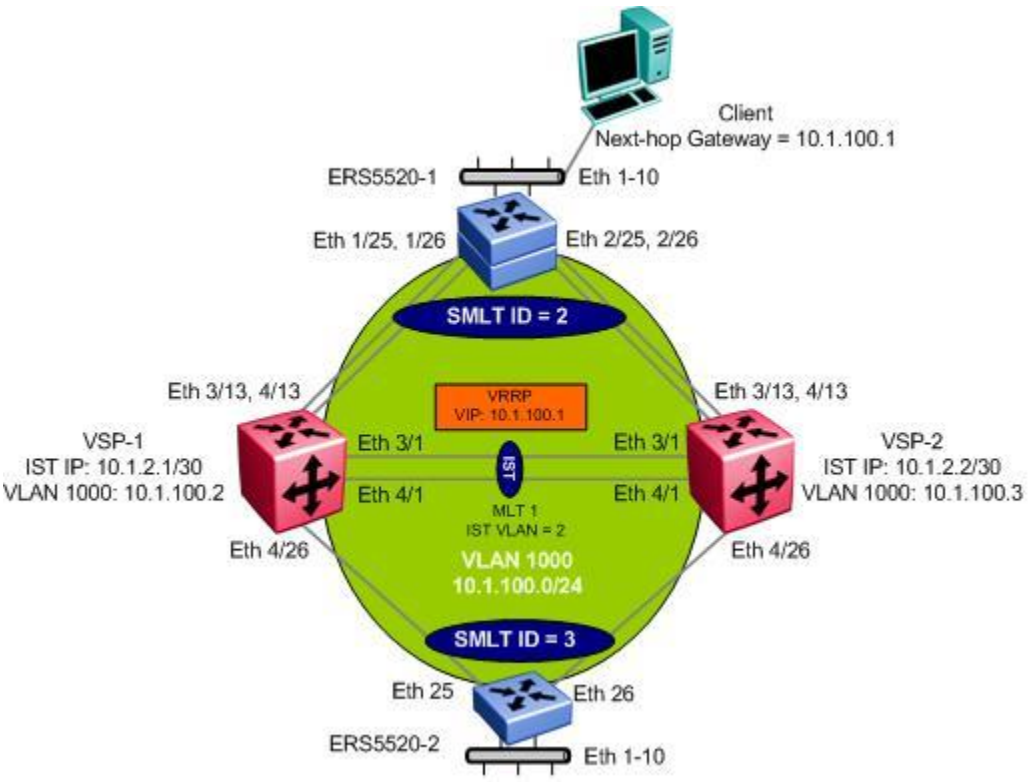


Figure 4: VSP 9000 Triangle SMLT Configuration with VRRP Backup Master

Assuming we take the same base setup as used in Section 2.1.1 but we now add a Layer 3 routing protocol with VRRP Backup Master. The configuration remains the same with the addition of enabling a routing protocol on VLAN 10 and enabling VRRP Backup-Master.

Overall, we will use the same configuration steps as used in Section 2.2.1 and will add the following:

- Enable OSPF on VLAN 1000
  - VLAN 1000 on VSP-1 will be configured with IP address 10.1.100.2/24
  - VLAN 1000 on VSP-2 will be configured with IP address 10.1.100.3/24
  - Both VSP-1 and VSP-2 will be configured with OSPF passive interface as both switches are connected to Layer 2 access switches. This prevent OSPF messages being send to the access switches
  - Use default OSPF timers
- Enable VRRP on VLAN 1000 with the following settings
  - Enable backup master
  - Set the hold down timer to 60 seconds on VSP-1 and VSP-2
  - Set the VRRP VIP to 10.1.100.1 on both switches in the SMLT cluster
  - Set VRRP virtual router id (vrid) to 10

- Set the VRRP priority to 200 on VSP-1 so that it becomes the VRRP master and use the default value of 100 on VSP-2 so that it becomes the VRRP backup

The VRRP hold down timer should be set long enough such that the IGP routing protocol has time to converge and update the routing table. In some cases, setting the VRRP hold down timer a minimum of 1.5 times the IGP convergence time should be sufficient. For OSPF, it is suggested to use a value of 60 seconds if using the default OSPF timers.

Please note that the VSP 9000 supports up to 512 VRRP instances per system. If you decide to use VRRP interface fast timers (200ms), up to 24 instances are supported

2.3.1 Configuration – VSP 9000 Layer 3 Switch Cluster using VRRP Backup Master

2.3.1.1 Add IP address to VLAN 1000

VSP 9000 SMLT Cluster: Add IP address to VLAN 1000

VSP-1:

```
VSP-1:1(config)#interface Vlan 1000
VSP-1:1(config-if)#ip address 10.1.100.2 255.255.255.0
VSP-1:1(config-if)#exit
```

VSP-2:

```
VSP-2:1(config)#interface Vlan 1000
VSP-2:1(config-if)#ip address 10.1.100.3 255.255.255.0
VSP-2:1(config-if)#exit
```

2.3.1.2 Enable OSPF

VLAN 1000 will be configured with OSPF passive interface on the SMLT Switch cluster.

VSP 9000 SMLT Cluster: Step 1 – Enable OSPF to VLAN 1000 with passive interface

VSP-1 & VSP-2: Same configuration on both switches

```
VSP-1:1(config)#interface Vlan 1000
VSP-1:1(config-if)#ip ospf enable
VSP-1:1(config-if)#ip ospf network passive
VSP-1:1(config-if)#exit
```

VSP 9000 SMLT Cluster: Step 2 – Enable OSPF globally

VSP-1 & VSP-2: Same configuration on both switches

```
VSP-1:1(config)#router ospf enable
```

2.3.1.3 Enable VRRP

VSP 9000 SMLT Cluster: Enable VRRP backup master using vrid 10 and set the VRRP hold-down timer to 60 seconds

VSP-1:

```
VSP-1:1(config)#interface Vlan 1000
VSP-1:1(config-if)#ip vrrp 10 address 10.1.100.1
VSP-1:1(config-if)#ip vrrp 10 backup-master enable
VSP-1:1(config-if)#ip vrrp 10 holddown-timer 60
VSP-1:1(config-if)#ip vrrp 10 priority 200
VSP-1:1(config-if)#ip vrrp 10 enable
VSP-1:1(config-if)#exit
```

VSP-2: Same configuration as VSP-1 except for the VRRP priority

```
VSP-1:1(config-if)#ip vrrp 10 priority 100
```

2.3.1.4 DHCP Relay Option

If you wish to enable DHCP Relay on VLAN 1000, please enter the following commands assuming the DHCP relay agent is 172.30.30.20.

VSP 9000 SMLT Cluster: Step 1 - Enable DHCP Relay on VLAN 1000

VSP-1 & VSP 2: Same configuration on both switches

```
VSP-1:1(config)#interface Vlan 1000
VSP-1:1(config-if)#ip dhcp-relay
VSP-1:1(config-if)#exit
```

VSP 9000 SMLT Cluster: Step 2 - Enable DHCP agent

VSP-1:

```
VSP-1:1(config)#ip dhcp-relay fwd-path 10.1.100.2 172.30.30.20
VSP-1:1(config)#ip dhcp-relay fwd-path 10.1.100.2 172.30.30.20 enable
```

VSP 2:

```
VSP-2:1(config)#ip dhcp-relay fwd-path 10.1.100.3 172.30.30.20
VSP-2:1(config)#ip dhcp-relay fwd-path 10.1.100.3 172.30.30.20 enable
```

2.3.2 Configuration File

VSP-1	VSP-2
#	#
# VLAN CONFIGURATION - PHASE I	# VLAN CONFIGURATION - PHASE I
#	#
vlan create 1000 name " SmltVlan" type port-mstprstp 0	vlan create 1000 name " SmltVlan" type port-mstprstp 0
vlan mlt 1000 1	vlan mlt 1000 1
vlan mlt 1000 2	vlan mlt 1000 2
vlan mlt 1000 3	vlan mlt 1000 3
vlan members 1000 3/1,3/13,4/1,4/13,4/26 portmember	vlan members 1000 3/1,3/13,4/1,4/13,4/26 portmember
vlan mac-address-entry 1000 aging-time 21601	vlan mac-address-entry 1000 aging-time 21601
interface Vlan 1000	interface Vlan 1000
ip address 10.1.100.2 255.255.255.0 6	ip address 10.1.100.3 255.255.255.0 6
ip ospf network passive	ip ospf network passive
ip vrrp address 10 10.1.100.1	ip vrrp address 10 10.1.100.1
ip vrrp 10 backup-master enable holddown-timer 60 priority 200	ip vrrp 10 backup-master enable holddown-timer 60
ip vrrp 10 backup-master enable	ip vrrp 10 backup-master enable
ip vrrp 10 enable	ip vrrp 10 enable
exit	exit
#	#
# OSPF CONFIGURATION - GlobalRouter	# OSPF CONFIGURATION - GlobalRouter
#	#
router ospf	router ospf
exit	exit
router ospf enable	router ospf enable

2.3.3 Verify Operations

2.3.3.1 VRRP Operations

Verify that the MLT instances is configured correctly and is functioning by issuing the following command:

show ip vrrp interface vrid 10

Results:

```
==============================================================================
                          Vrrp Info
==============================================================================

VRID  P/V   IP              MAC               STATE    CONTROL  PRIO  ADV
------------------------------------------------------------------------------
10    260   10.1.100.1      00:00:5e:00:01:0a Master   Enabled  200   1

VRID  P/V   MASTER          UP TIME              HLD DWN  CRITICAL IP (ENABLED)
------------------------------------------------------------------------------
10    260   10.1.100.1      0 day(s), 00:01:53   0        0.0.0.0         (No)

VRID  P/V   BACKUP MASTER   BACKUP MASTER STATE   FAST ADV (ENABLED)
------------------------------------------------------------------------------
10    260   enable          down                  200       (NO)
```

On each VSP 9000 in the switch cluster verify the following information:

Option	Verify
VRID	Verify that the VRRP VID is ***10*** on both VSP-1 and VSP-2. If not, there is a configuration error.
IP	Verify that the VRRP IP address is ***10.1.100.1*** on both VSP-1 and VSP-2. If not, there is a configuration error.
MAC	The VRRP MAC on both switches in the SMLT cluster should be the same.
STATE	Verify the VRRP state: • VSP-1: ***Master*** • VSP-2: ***Back Up***
PRIO	Verify that the VRRP priority is set to ***200*** on VSP-1 and ***100*** on VSP-2. If not, configure the appropriate VRRP priority.

MASTER	Verify that VRRP master's IP address belongs to VSP-1 on both switches: • VSP-1: ***10.1.100.2*** • VSP-2: ***10.1.100.2***
BACKUP MASTER	Verify that backup master is set to ***enable*** on both switches. If not, enable VRRP backup master.
BACKUP MASTER STATE	Verify that VRRP backup master state on both switches: • VSP-1: ***down*** • VSP-2: ***up***
(ENABLED)	Verify that the VRRP fast advertise is set to ***NO*** on VSP-1 and VSP-2. It is not necessary to enable VRRP fast advertise.

2.4 Configuration – ERS 8600/8800 Triangle Switch Cluster using VRRP with Backup Master

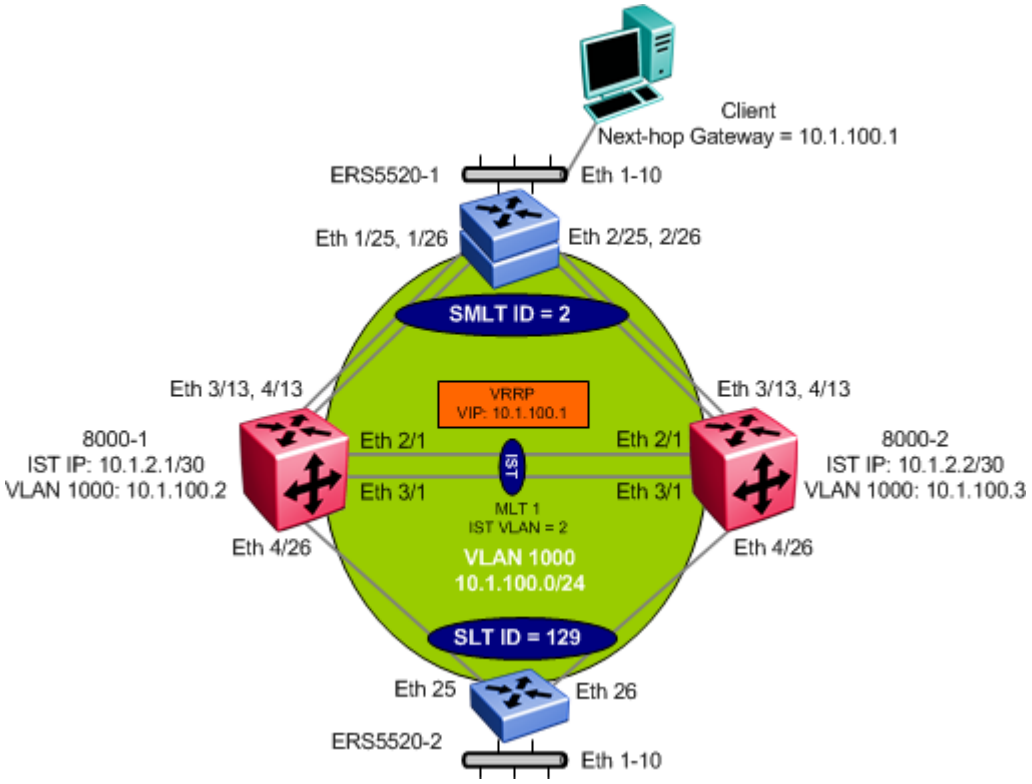


Figure 5: ERS 8600/8800 Triangle SMLT Configuration with VRRP Backup Master

Assuming we take the same base setup as used in Section 2.1.1 but we now add a Layer 3 routing protocol with VRRP Backup Master. The configuration remains the same with the addition of enabling a routing protocol on VLAN 10 and enabling VRRP Backup-Master.

Overall, we will use the same configuration steps as used in Section 2.2.1 and will add the following:

- Enable OSPF on VLAN 1000
  - VLAN 1000 on 8000-1 will be configured with IP address 10.1.100.2/24
  - VLAN 1000 on 8000-2 will be configured with IP address 10.1.100.3/24
  - Both 8000-1 and 8000-2 will be configured with OSPF passive interface as both switches are connected to Layer 2 access switches. This prevent OSPF messages being send to the access switches
  - Use default OSPF timers
- Enable VRRP on VLAN 1000 with the following settings
  - Enable backup master
  - Set the hold down timer to 60 seconds on 8000-1 and 8000-2
  - Set the VRRP VIP to 10.1.100.1 on both switches in the SMLT cluster
  - Set VRRP virtual router id (vrid) to 10

- Set the VRRP priority to 200 on 8000-1 so that it becomes the VRRP master and use the default value of 100 on ERS-8600-2 so that it becomes the VRRP backup

The VRRP hold down timer should be set long enough such that the IGP routing protocol has time to converge and update the routing table. In some cases, setting the VRRP hold down timer a minimum of 1.5 times the IGP convergence time should be sufficient. For OSPF, it is suggested to use a value of 60 seconds if using the default OSPF timers.

Please note that the ERS8600 supports up to 255 VRRP instances. If you have a requirement for more than 255 routing instances to a Layer 2 access in a SMLT cluster, you can use RSMLT Edge instead of VRRP backup master or a mix of both.

2.4.1 Configuration – ERS 8600/8800 Layer 3 Switch Cluster using VRRP Backup Master

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

2.4.1.1 Add IP address to VLAN 1000

ERS 8000 SMLT Cluster: Add IP address to VLAN 1000

8000-1:

```
8000-1:5(config)#interface vlan 1000
8000-1:5(config-if)#ip address 10.1.100.2 255.255.255.0
8000-1:5(config-if)#exit
```

8000-2:

```
8000-2:5# config vlan 1000 ip create 10.1.100.3/24
```

2.4.1.2 Enable OSPF

VLAN 1000 will be configured with OSPF passive interface on the SMLT Switch cluster.

ERS 8000 SMLT Cluster: Step 1 – Enable OSPF to VLAN 1000 with passive interface

8000-1:

```
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:

```
8000-2:5# config vlan 1000 ip ospf interface-type passive
8000-2:5# config vlan 1000 ip ospf enable
```

ERS 8000 SMLT Cluster: Step 2 – Enable OSPF globally

8000-1:

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

8000-2:

```
8000-2:5# config ip ospf enable
```

2.4.1.3 Enable VRRP

ERS 8000 SMLT Cluster: Enable VRRP backup master using vrid 10 and set the VRRP hold-down timer to 60 seconds

8000-1:

```
8000-1:5(config)#interface vlan 1000
8000-1:5(config-if)#ip vrrp address 10 10.1.100.1
8000-1:5(config-if)#ip vrrp 10 backup-master enable
8000-1:5(config-if)#ip vrrp 10 holddown-timer 60
8000-1:5(config-if)#ip vrrp 10 priority 200
8000-1:5(config-if)#ip vrrp 10 enable
8000-1:5(config-if)#exit
```

8000-2:

```
8000-2:5# config vlan 1000 ip vrrp 10 address 10.1.100.1
8000-2:5# config vlan 1000 ip vrrp 10 backup-master enable
8000-2:5# config vlan 1000 ip vrrp 10 holddown-timer 60
8000-2:5# config vlan 1000 ip vrrp 10 enable
```

2.4.1.4 DHCP Relay Option

If you wish to enable DHCP Relay on VLAN 1000, please enter the following commands assuming the DHCP relay agent is 172.30.30.20.

ERS 8000 SMLT Cluster: Step 1 - Enable DHCP Relay on VLAN 1000

8000-1:

```
8000-1:5(config)#interface vlan 1000
8000-1:5(config-if)#ip dhcp-relay
8000-1:5(config-if)#exit
```

8000-2:

```
8000-2:5# config vlan 1000 ip dhcp-relay enable
```

ERS 8000 SMLT Cluster: Step 2 - Enable DHCP agent

8000-1:

```
8000-1:5(config)#ip dhcp-relay fwd-path 10.1.100.2 172.30.30.20 mode dhcp
```

8000-2:

```
8000-2:5# config ip dhcp-relay create-fwd-path agent 10.1.100.3 server 172.30.30.20
mode dhcp state enable
```

2.4.2 Configuration File

8000-1	8000-2
# # VLAN CONFIGURATION - PHASE I # vlan create 1000 name "Services" type port 1 color 2 vlan mlt 1000 1 vlan mlt 1000 2 vlan members 2 2/1,3/1,3/13,4/13 portmember vlan mac-address-entry 1000 aging-time 21601 interface Vlan 1000 ip address 10.1.100.2 255.255.255.0 6 ip ospf network passive ip vrrp address 10 10.1.100.1 ip vrrp 10 backup-master enable holddown-timer 60 priority 200 ip vrrp 10 backup-master enable ip vrrp 10 enable exit # # OSPF CONFIGURATION - GlobalRouter # router ospf exit router ospf enable	# # VLAN CONFIGURATION - PHASE I # vlan 1000 create byport 1 name "Services" vlan 1000 add-mlt 1 vlan 1000 add-mlt 2 vlan 1000 ports add 2/1,3/1,3/13,4/13 member portmember vlan 1000 fdb-entry aging-time 21601 vlan 1000 ip create 10.1.100.3/255.255.255.0 mac_offset 10 vlan 1000 ip ospf interface-type passive vlan 1000 ip ospf enable vlan 1000 ip vrrp 10 address 10.1.100.1 vlan 1000 ip vrrp 10 backup-master enable vlan 1000 ip vrrp 10 holddown-timer 60 vlan 1000 ip vrrp 10 enable # # OSPF CONFIGURATION - GlobalRouter # ip ospf admin-state enable ip ospf enable

2.4.3 Verify Operations

2.4.3.1 VRRP Operations

Verify that the MLT instances is configured correctly and is functioning by issuing the following command:

ACLI: ***show ip vrrp interface vrid 10***

CLI: ***show ip vrrp info vrid 10***

Results:

```
                        Vrrp Info
================================================================================

VRID  P/V   IP              MAC                STATE    CONTROL  PRIO  ADV
--------------------------------------------------------------------------------
10    260   10.1.100.1      00:00:5e:00:01:0a  Master   Enabled  200   1

VRID  P/V   MASTER          UP TIME               HLD DWN  CRITICAL IP (ENABLED)
--------------------------------------------------------------------------------
10    260   10.1.100.1      0 day(s), 00:01:53    0        0.0.0.0          (No)

VRID  P/V   BACKUP MASTER   BACKUP MASTER STATE   FAST ADV (ENABLED)
--------------------------------------------------------------------------------
10    260   enable          down                  200       (NO)
```

On each ERS 8800/8600 in the switch cluster verify the following information:

Option	Verify
VRID	Verify that the VRRP VID is ***10*** on both 8000-1 and 8000-2. If not, there is a configuration error.
IP	Verify that the VRRP IP address is ***10.1.100.1*** on both 8000-1 and 8000-2. If not, there is a configuration error.
MAC	The VRRP MAC on both switches in the SMLT cluster should be the same.
STATE	Verify the VRRP state: • 8000-1: ***Master*** • 8000-2: ***Back Up***
PRIO	Verify that the VRRP priority is set to ***200*** on 8000-1 and ***100*** on 8000-2. If not, configure the appropriate VRRP priority.

MASTER	Verify that VRRP master's IP address belongs to 8000-1 on both switches: • 8000-1: ***10.1.100.2*** • 8000-2: ***10.1.100.2***
BACKUP MASTER	Verify that backup master is set to ***enable*** on both switches. If not, enable VRRP backup master.
BACKUP MASTER STATE	Verify that VRRP backup master state on both switches: • 8000-1: ***down*** • 8000-2: ***up***
(ENABLED)	Verify that the VRRP fast advertise is set to ***NO*** on 8000-1 and 8000-2. It is not necessary to enable VRRP fast advertise.

2.5 Configuration – VSP 9000 Layer 2 Edge Routed SMLT (RSMLT Edge) Triangle Switch Cluster Configuration

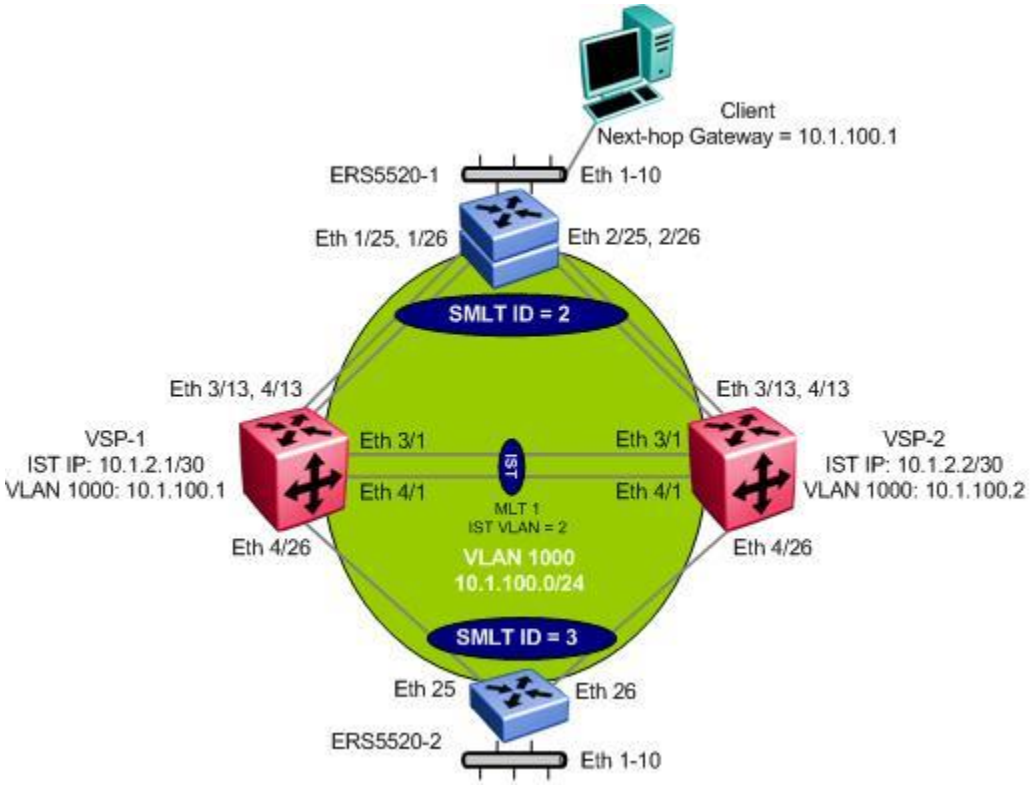


Figure 6: VSP 9000 RSMLT Edge

If a redundant layer 3 triangle edge is required via a layer 2 access switch, this can be accomplished using either VRRP with backup-master enabled or RSMLT Edge. Either option will work.

For this configuration example, we will enable RSMLT Edge on VLAN 1000 on the VSP 9000 Switch Cluster. The users connected to either ERS5520-1 or ERS5520-2 can use the IP address of either VSP 9000 peer switch as the default gateway. For this example, VSP-1 will be used as the default gateway while VSP-2 will forward traffic on behalf of its peer.

In reference to the diagram above, we will configure the following:

- Overall, this configuration example will cover the configuration steps required for VSP-1 and VSP-2 assuming we take the same base setup as used in Section 2.2.1
- OSPF will be used as the IGP on VLAN 1000
- We will set the RSMLT holdup timer to infinity (value of 9999) as required for RSMLT Edge

The hold-down timer should be configured to be at least 1.5 times greater than the routing protocol convergence time, thus allowing RIP, OSPF or BGP enough time to build up the routing table of the recovering router before L3 forwarding for its peer router's MAC address is activated again. For example, if the default routing timers are used, the hold-down timer could be set for 60 seconds for OSPF while for RIP, 180 second could be used. The default hold-down timer is set for 60 seconds and since we

are using OSPF in this example, we do not have to change this setting.

The default RSMLT hold-up timer is 180 seconds, which is designed for interconnecting to Layer 3 switches. For RSMLT Edge, the hold-up timer should be set to infinity (9999), which allows the core nodes in the Switch Cluster to forward traffic indefinitely on behalf of their peers similar to the VRRP backup-master function.

2.5.1 Configuration – VSP 9000 Switch Cluster using RSMLT Edge

2.5.1.1 Add IP address to VLAN 1000

VSP 9000 SMLT Cluster: Add IP address to VLAN 1000

VSP-1:

```
VSP-1:1(config)#interface Vlan 1000
VSP-1:1(config-if)#ip address 10.1.100.1 255.255.255.0
VSP-1:1(config-if)#exit
```

VSP-2:

```
VSP-2:1(config)#interface Vlan 1000
VSP-2:1(config-if)#ip address 10.1.100.2 255.255.255.0
VSP-2:1(config-if)#exit
```

2.5.1.2 Enable OSPF

VLAN 1000 will be configured with OSPF passive interface on the SMLT Switch cluster.

VSP 9000 SMLT Cluster: Step 1 – Enable OSPF to VLAN 1000 with passive interface

VSP-1 & VSP-2: Same configuration on both switches

```
VSP-1:1(config)#interface Vlan 1000
VSP-1:1(config-if)#ip ospf enable
VSP-1:1(config-if)#ip ospf network passive
VSP-1:1(config-if)#exit
```

VSP 9000 SMLT Cluster: Step 2 – Enable OSPF globally

VSP-1 & VSP-2: Same configuration on both switches

```
VSP-1:1(config)#router ospf enable
```

2.5.1.3 Enable RSMLT Edge

VLAN 1000 will be configured with RSMLT on the SMLT Switch cluster.

VSP 9000 SMLT Cluster: Step 1 – Enable RSMLT Edge by setting the holdup-timer to infinity (9999)

VSP-1 & VSP-2: Same configuration on both switches

```
VSP-1:1(config)#interface Vlan 1000
VSP-1:1(config-if)#ip rsmlt
VSP-1:1(config-if)#ip rsmlt holdup-timer 9999
VSP-1:1(config-if)#exit
```

VSP 9000 SMLT Cluster: Step 2 – Enable RSMLT-edge support

VSP-1 & VSP-2: Same configuration on both switches

```
VSP-1:1(config)#ip rsmlt edge-support
```

2.5.1.4 DHCP Option

Please see section 2.3.1.4.

2.5.2 Configuration File

VSP-1	VSP-2
#	#
# VLAN CONFIGURATION - PHASE I	# VLAN CONFIGURATION - PHASE I
#	#
vlan create 1000 name " SmltVlan" type port-mstprstp 0	vlan create 1000 name " SmltVlan" port-mstprstp 0
vlan mlt 1000 1	vlan mlt 1000 1
vlan mlt 1000 2	vlan mlt 1000 2
vlan mlt 1000 3	vlan mlt 1000 3
vlan members 1000 3/1,3/13,4/1,4/13,4/26 portmember	vlan members 1000 3/1,3/13,4/1,4/13,4/26 portmember
vlan mac-address-entry 1000 aging-time 21601	vlan mac-address-entry 1000 aging-time 21601
interface Vlan 1000	interface Vlan 1000
ip address 10.1.100.1 255.255.255.0 6	ip address 10.1.100.2 255.255.255.0 6
ip ospf network passive	ip ospf network passive
ip rsmlt	ip rsmlt
ip rsmlt holdup-timer 9999	ip rsmlt holdup-timer 9999
exit	exit
#	#
# RSMLT CONFIGURATION	# RSMLT CONFIGURATION
#	#
ip rsmlt edge-support	ip rsmlt edge-support
#	#
# OSPF CONFIGURATION - GlobalRouter	# OSPF CONFIGURATION - GlobalRouter
#	#
router ospf	router ospf
exit	exit
router ospf enable	router ospf enable

2.5.3 Verify RSMLT Edge Operation

2.5.3.1 RSMLT Edge Operations

Step 1 - Verify that the RSMLT instance is configured correctly and is functioning by issuing the following command:

show ip rsmlt

Results:

```
================================================================================
                        Ip Rsmlt Local Info
================================================================================

VID   IP              MAC               ADMIN   OPER  HDTMR  HUTMR
--------------------------------------------------------------------------------
1000  10.1.100.1      00:01:81:28:86:1c  Enable  Up    60     infinity

VID   SMLT ID                  SLT ID
--------------------------------------------------------------------------------
1000

================================================================================
                        Ip Rsmlt Peer Info
================================================================================

VID   IP              MAC               ADMIN   OPER  HDTMR  HUTMR

--------------------------------------------------------------------------------
1000  10.1.100.2      00:e0:7b:bc:22:02  Enable  Up    60     infinity

VID   HDT REMAIN  HUT REMAIN  SMLT ID                 SLT ID

--------------------------------------------------------------------------------
1000  60          infinity
```

Step 2 - Verify that the RSMLT-edge is enabled:

```
show ip rsmlt edge-support
```

Results:

```
RSMLT Peer Info:
        rsmlt-peer-forwarding : enable
```

On each VSP 9000 in the switch cluster verify the following information:

Option	Verify
ADMIN	Verify that the RSMLT Admin is ***Enabled*** on both VSP-1 and VSP-2. If not, there is a configuration error.
OPER	Verify that the RSMLT operation is ***up*** on both VSP-1 and VSP-2.
HUTMR	Verify that the RSMLT holdup timer is set to ***infinity*** on both VSP-1 and VSP-2. If not, there is a configuration error.
rsmlt-peer-forwarding	Verify that RSMLT-edge support is enabled; if not, enable RSMLT-edge.

2.6 Configuration – ERS 8600/8800 Layer 2 Edge Routed SMLT (RSMLT Edge) Triangle Switch Cluster Configuration

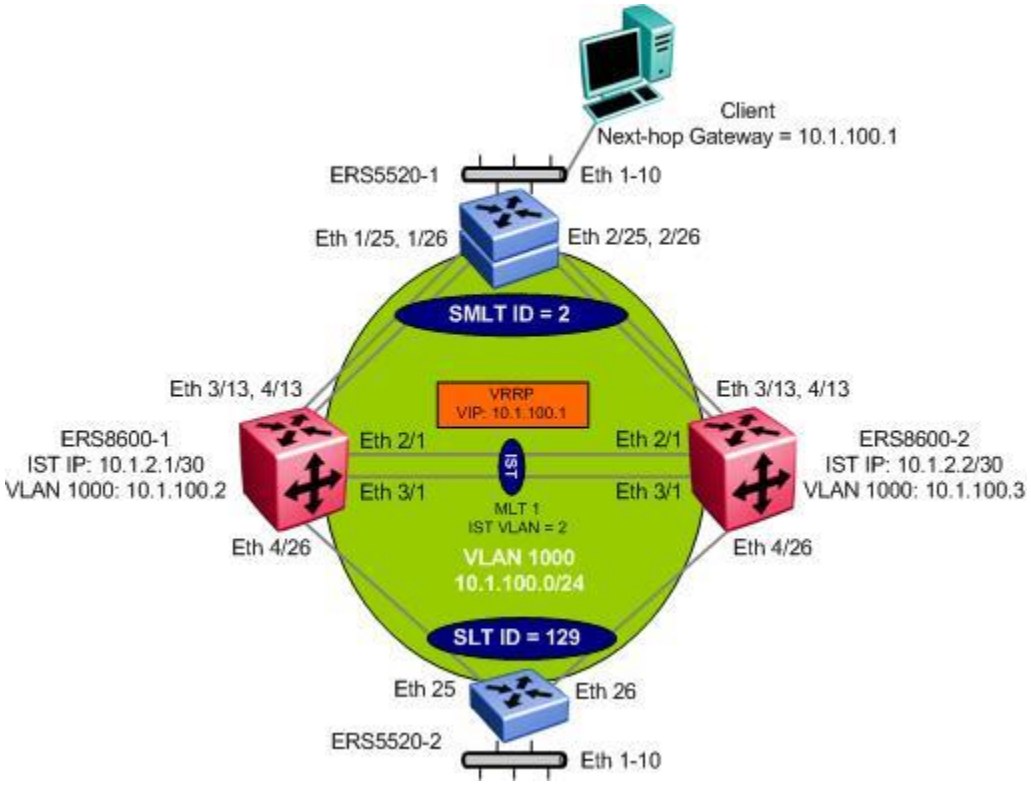


Figure 7: ERS 8600/8800 RSMLT Edge

If a redundant layer 3 triangle edge is required via a layer 2 access switch, this can be accomplished using either VRRP with backup-master enabled or RSMLT Edge. Either option will work. However, there is only a maximum of 255 VRRP instances available on the ERS 8600/8800. If there is concern about running out of VRRP instances, RSMLT Edge can be deployed.

For this configuration example, we will enable RSMLT Edge on VLAN 1000 on the ERS 8600/8800 Switch Cluster. The users connected to either ERS5520-1 or ERS5520-2 can use the IP address of either ERS 8600/8800 peer switch as the default gateway. For this example, 8000-1 will be used as the default gateway while 8000-2 will forward traffic on behalf of its peer.

In reference to the diagram above, we will configure the following:

- Overall, this configuration example will cover the configuration steps required for 8000-1 and 8000-2 assuming we take the same base setup as used in Section 2.2.1
- OSPF will be used as the IGP on VLAN 1000
- We will set the RSMLT holdup timer to infinity (value of 9999) as required for RSMLT Edge

The hold-down timer should be configured to be at least 1.5 times greater than the routing protocol convergence time, thus allowing RIP, OSPF or BGP enough time to build up the routing table of the recovering router before L3 forwarding for its peer router's MAC address is activated again. For example, if the default routing timers are

used, the hold-down timer could be set for 60 seconds for OSPF while for RIP, 180 second could be used. The default hold-down timer is set for 60 seconds and since we are using OSPF in this example, we do not have to change this setting.

The default RSMLT hold-up timer is 180 seconds, which is designed for interconnecting to Layer 3 switches. For RSMLT Edge, the hold-up timer should be set to infinity (9999), which allows the core nodes in the Switch Cluster to forward traffic indefinitely on behalf of their peers similar to the VRRP backup-master function.

2.6.1 Configuration – ERS 8600/8800 Switch Cluster using RSMLT Edge

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

2.6.1.1 Add IP address to VLAN 1000

ERS 8000 SMLT Cluster: Add IP address to VLAN 1000

8000-1:

```
8000-1:5(config)#interface vlan 1000
8000-1:5(config-if)#ip address 10.1.100.1 255.255.255.0
8000-1:5(config-if)#exit
```

8000-2:

```
8000-2:5# config vlan 1000 ip create 10.1.100.2/24
```

2.6.1.2 Enable OSPF

VLAN 1000 will be configured with OSPF passive interface on the SMLT Switch cluster.

ERS 8000 SMLT Cluster: Step 1 – Enable OSPF to VLAN 1000 with passive interface

8000-1:

```
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:

```
8000-2:5# config vlan 1000 ip ospf interface-type passive
8000-2:5# config vlan 1000 ip ospf enable
```

ERS 8000 SMLT Cluster: Step 2 – Enable OSPF globally

8000-1:

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

8000-2:

```
8000-2:5# config ip ospf enable
```

2.6.1.3 Enable RSMLT Edge

VLAN 1000 will be configured with OSPF passive interface on the SMLT Switch cluster.

ERS 8000 SMLT Cluster: Step 1 – Enable RSMLT Edge by setting the holdup timer to infinity (9999)

8000-1:

```
8000-1:5(config)#interface vlan 1000
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:

```
8000-2:5# config vlan 1000 ip rsmlt enable
8000-2:5# config vlan 1000 ip rsmlt holdup-timer 9999
```

ERS 8000 SMLT Cluster: Step 2 – Enable RSMLT Edge support

8000-1:

```
8000-1:5(config)#ip rsmlt edge-support
```

8000-2:

```
8000-2:5# config ip rsmlt rsmlt-edge-support enable
```

2.6.1.4 DHCP Option

Please see section 2.4.1.4.

2.6.2 Configuration File

8000-1	8000-2
#	#
# VLAN CONFIGURATION - PHASE I	# VLAN CONFIGURATION - PHASE I
#	#
vlan create 1000 name "Services" type port 1 color 2	vlan 1000 create byport 1 name "Services"
vlan mlt 1000 1	vlan 1000 add-mlt 1
vlan mlt 1000 2	vlan 1000 add-mlt 2
vlan members 2 2/1,3/1,3/13,4/13 portmember	vlan 1000 ports add 2/1,3/1,3/13,4/13 member portmember
vlan mac-address-entry 1000 aging-time 21601	vlan 1000 fdb-entry aging-time 21601
interface Vlan 1000	vlan 1000 ip create 10.1.100.3/255.255.255.0 mac_offset 10
ip address 10.1.100.2 255.255.255.0 6	vlan 1000 ip ospf interface-type passive
ip ospf network passive	vlan 1000 ip ospf enable
ip rsmlt	vlan 1000 ip rsmlt enable
ip rsmlt holdup-timer 9999	vlan 1000 ip rsmlt holdup-timer 9999
exit	
#	#
# RSMLT CONFIGURATION	# OSPF CONFIGURATION - GlobalRouter
#	#
ip rsmlt edge-support	ip ospf admin-state enable
	ip ospf enable
#	#
# OSPF CONFIGURATION - GlobalRouter	# RSMLT CONFIGURATION
#	#
router ospf	ip rsmlt rsmlt-edge-support enable
exit	
router ospf enable	

2.6.3 Verify RSMLT Edge Operation

2.6.3.1 RSMLT Edge Operations

Step 1 - Verify that the RSMLT instance is configured correctly and is functioning by issuing the following command:

ACLI: ***show ip rsmlt***

CLI: ***show ip rsmlt info***

Results:

```
================================================================================
                        Ip Rsmlt Local Info
================================================================================

VID   IP              MAC               ADMIN   OPER  HDTMR  HUTMR
--------------------------------------------------------------------------------
1000  10.1.100.1      00:01:81:28:86:1c  Enable  Up    60     infinity

VID   SMLT ID                  SLT ID
--------------------------------------------------------------------------------
1000                           129


================================================================================
                        Ip Rsmlt Peer Info
================================================================================

VID   IP              MAC               ADMIN   OPER  HDTMR  HUTMR

--------------------------------------------------------------------------------
1000  10.1.100.2      00:e0:7b:bc:22:02  Enable  Up    60     infinity

VID   HDT REMAIN  HUT REMAIN  SMLT ID                  SLT ID

--------------------------------------------------------------------------------
1000  60          infinity                             129
```

Step 2 - Verify that the RSMLT-edge is enabled:

```
ACLI: show ip rsmlt edge-support
CLI: config ip rsmlt info
```

Results:

```
RSMLT Peer Info:
        rsmlt-peer-forwarding : enable
```

On each ERS 8600/8800 in the switch cluster verify the following information:

Option	Verify
ADMIN	Verify that the RSMLT Admin is ***Enabled*** on both 8000-1 and 8000-2. If not, there is a configuration error.
OPER	Verify that the RSMLT operation is ***up*** on both 8000-1 and 8000-2.
HUTMR	Verify that the RSMLT holdup timer is set to ***infinity*** on both 8000-1 and 8000-2. If not, there is a configuration error.
SMLT ID	Verify the SLT ID is showing ***129***.
Ip Rsmlt Peer Info	Verify the RSMLT Peer is showing: • 8000-1: VLAN ***1000***, SLT ***129*** , IP ***10.1.100.2*** and the corresponding MAC of RSMLT cluster peer • 8000-2: VLAN ***1000*** and SLT ***129***, IP ***10.1.100.1*** and the corresponding MAC of RSMLT cluster peer
rsmlt-peer-forwarding	Verify that RSMLT-edge support is enabled; if not, enable RSMLT-edge.

2.7 Configuration – VSP 9000 Layer 3 Routed SMLT Triangle Switch Cluster Configuration

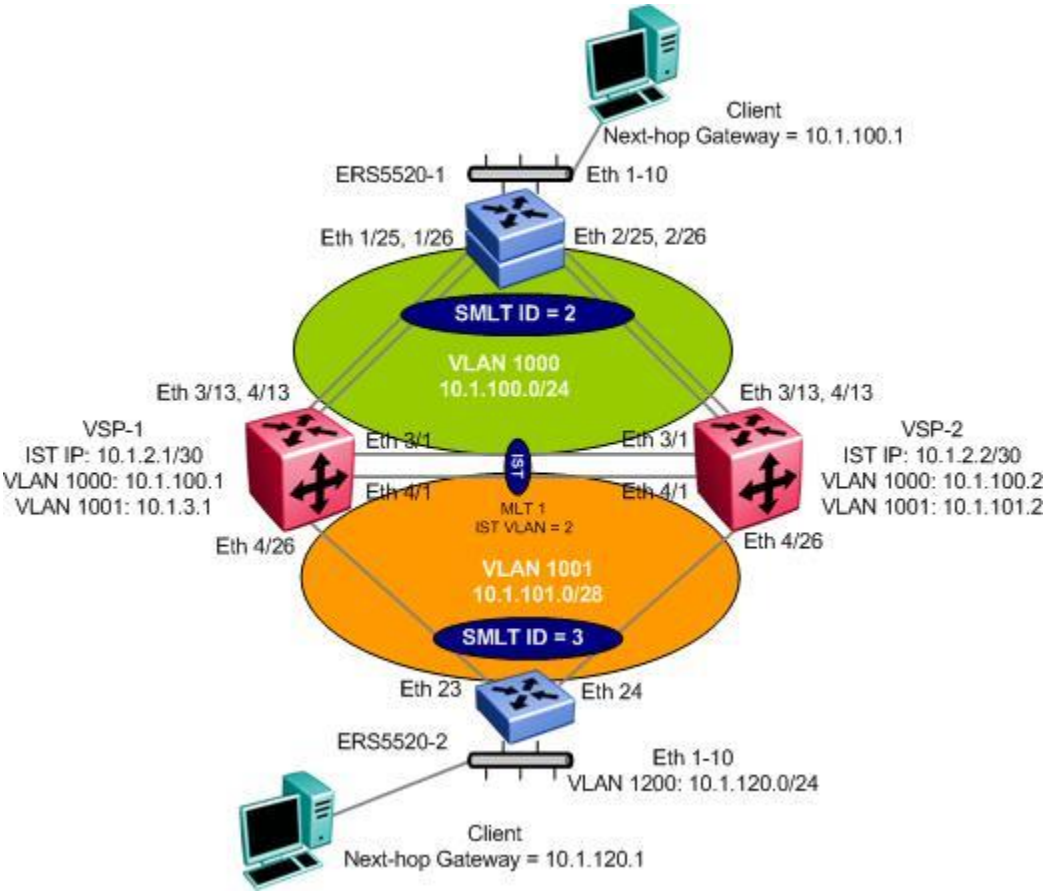


Figure 8: VSP 9000 RSMLT

If the access switch supports L3, RSMLT can be enabled. For this example, we will configure the SMLT switch cluster with the following assuming ERS5520-2 is enabled for Layer 3:

- SMLT Cluster
  - Add VLAN 1001 with IP subnet 10.1.101.0/24 and tagged port member 4/26; add IP address 10.1.101.1 to VSP-1 and 10.1.101.2 to VSP-2
  - Enable RSMLT
- Access Switch – ERS5520-2
  - Add VLAN 1001 with IP address 10.1.101.3/24 and MLT tagged trunk members 23 and 24
  - Add access VLAN 1200 with IP address 10.1.120.1/24 and user port members 1 to 10
  - Enable OSPF on both VLAN 1001 and 1200

2.7.1 Configuration – VSP 9000 Switch Cluster using RSMLT

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

2.7.1.1 Create VLAN 1001

The following port based VLANs will be configured on the SMLT Switch cluster

- VLAN 1001 to be used at a Layer 3 level to ERS5520-2

VSP 9000 SMLT Cluster: Create VLAN 1001, add port members, and change the MAC fdb timer to the recommended value of 21601 seconds

VSP-1 & VSP-2: Same configuration on both switches

```
VSP-1:1(config)#vlan create 1001 name "Vlan1001" type port-mstprstp 0
VSP-1:1(config)#vlan members remove 1000 4/26
VSP-1:1(config)#vlan members add 1001 4/26
VSP-1:1(config)#vlan mac-address-entry 1001 aging-time 21601
```

2.7.1.2 Add IP address to VLAN 1001

VSP 9000 SMLT Cluster: Add IP address to VLAN 1001

VSP-1:

```
VSP-1:1(config)#interface Vlan 1001
VSP-1:1(config-if)#ip address 10.1.101.1 255.255.255.0
VSP-1:1(config-if)#exit
```

VSP-2:

```
VSP-2:1(config)#interface Vlan 1001
VSP-2:1(config-if)#ip address 10.1.101.2 255.255.255.0
VSP-2:1(config-if)#exit
```

2.7.1.3 Enable OSPF

VLAN 1001 will be configured with OSPF on the SMLT Switch cluster.

VSP 9000 SMLT Cluster: Step 1 – Enable OSPF to VLAN 1000 with passive interface

VSP-1 & VSP-2: Same configuration on both switches

```
VSP-1:1(config)#interface Vlan 1001
VSP-1:1(config-if)#ip ospf enable
```

```
VSP-1:1(config-if)#ip ospf network passive
VSP-1:1(config-if)#exit
```

VSP 9000 SMLT Cluster: Step 2 – Enable OSPF globally

VSP-1 & VSP-2: Same configuration on both switches

```
VSP-1:1(config)#router ospf enable
```

2.7.1.4 Enable RSMLT

Enable VLAN 1001 with RSMLT using default RSMLT timers.

VSP 9000 SMLT Cluster: Enable RSMLT

VSP-1 & VSP-2: Same configuration on both switches

```
VSP-1:1(config)#interface Vlan 1001
VSP-1:1(config-if)#ip rsmlt
VSP-1:1(config-if)#exit
```

2.7.2 Configuration - Edge Switch

2.7.2.1 MSTP

Edge switch: Enable MSTP

5520-1 & 5520-2: Same configuration on both switches

```
5520-1(config)#spanning-tree mode mst
New operational mode MSTP will take effect upon reset
5520-1(config)#boot
Reboot the unit(s) (y/n) ? y
```

As the VSP 9000 uses MSTP by default, it is recommended to change the Spanning mode on the access stackable switches to also use MSTP. Even though Spanning Tree is not used and is disabled on the core ports, the Spanning Tree mode is used by some Network Management tools such as VLAN Manager in COM. VLAN Manager will regroup all VLANs per Spanning Tree group type, hence, if you leave the stackable edge switch in their default Spanning Tree mode of STPG, then VLAN Manager will not be able to display, create, delete, or sync a VLAN across the VSP and the edge stackable switches.

2.7.2.2 Create VLANs 1001 and 1200 and Delete VLAN 1000

Assuming we are using the configuration from section 2.1.2, perform the following steps:

ERS5520-2: Create VLAN 1001 and 1200

```
5520-2(config)#vlan create 1001 name rsmlt_cluster type port cist
5520-2(config)#vlan create 1200 name access type port cist
5520-2(config)#vlan delete 1000
5520-2(config)# vlan members add 1001 23,24
5520-2(config)# vlan members add 1200 2-10
```

2.7.2.3 Add IP addresses

ERS5520-2: Step 1 – Add IP address to VLAN 1001

```
5520-2(config)#interface vlan 1001
5520-2(config-if)# ip address 10.1.101.3 255.255.255.0
5520-2(config-if)# exit
```

ERS5520-2: Step 2 – Add IP address to VLAN 1200

```
5520-2(config)#interface vlan 1200
5520-2(config-if)#ip address 10.1.120.1 255.255.255.0
5520-2(config-if)#exit
```

2.7.2.4 Enable OSPF

Enable OSPF on VLANs 1001 and 1200. VLAN 1200 will be configured with OSPF passive interface.

ERS5520-2: Step 1 – Enable IP Routing

```
5520-2(config)#ip routing
```

ERS5520-2: Step 2 – Enable OSPF to VLAN 1200 with passive interface

```
5520-2(config)#interface vlan 1200
5520-2(config-if)#ip ospf network passive
5520-2(config-if)#ip ospf enable
```

ERS5520-2: Step 3 – Enable OSPF to VLAN 1001 with passive interface

```
5520-2(config)#interface vlan 1001
5520-2(config-if)#ip ospf enable
5520-2(config-if)# exit
```

ERS5520-2: Step 4 – Enable OSPF globally

```
5520-2(config)#router ospf enable
```

2.7.2.5 DHCP Option

If you wish to enable DHCP relay for VLAN 1200, please enter the following command assuming the DHCP server IP address is 172.30.30.20. By default, DHCP is enabled on all VLANs when you add an IP address.

ERS5520-2: Step 1 – Enable IP DHCP relay agent

```
5520-2(config)# ip dhcp-relay fwd-path 10.1.120.1 172.30.30.20 mode dhcp
```

2.7.3 Verify RSMLT Operation

2.7.3.1 RSMLT Operations

Please note that only the output pertaining to VID 1001 is shown below.

Verify that the RSMLT instance is configured correctly and is functioning by issuing the following command

show ip rsmlt

Results:

```
================================================================================
                          Ip Rsmlt Local Info
================================================================================

VID   IP              MAC               ADMIN   OPER  HDTMR  HUTMR
--------------------------------------------------------------------------------
1001  10.1.101.1      00:01:81:28:86:1d  Enable  Up    60     180

VID   SMLT ID                  SLT ID
--------------------------------------------------------------------------------
1001

================================================================================
                          Ip Rsmlt Peer Info
================================================================================

VID   IP              MAC               ADMIN   OPER  HDTMR  HUTMR
--------------------------------------------------------------------------------
1001  10.1.101.2      00:e0:7b:bc:22:03  Enable  Up    60     180

VID   HDT REMAIN  HUT REMAIN  SMLT ID                  SLT ID
--------------------------------------------------------------------------------
1001  60          180
```

On each VSP 9000 in the switch cluster verify the following information:

Option	Verify
ADMIN	Verify that the RSMLT Admin is ***Enabled*** on both VSP-1 and VSP-2. If not, there is a configuration error.
OPER	Verify that the RSMLT operations are ***Up*** on both VSP-1 and VSP-2.
HDTMR HUTMR	Verify that the RSMLT holdup and holddown timer is set to ***60*** and ***180*** respectively on both VSP-1 and VSP-2. If not, there is a configuration error.
Ip Rsmlt Peer Info	Verify the RSMLT Peer is showing: • VSP-1: VLAN ***1001***, IP ***10.1.101.2*** and the corresponding MAC of RSMLT cluster peer • VSP-2: VLAN ***1001***, IP ***10.1.101.1*** and the corresponding MAC of RSMLT cluster peer

2.8 Configuration – ERS 8600/8800 Layer 3 Routed SMLT Triangle Switch Cluster Configuration

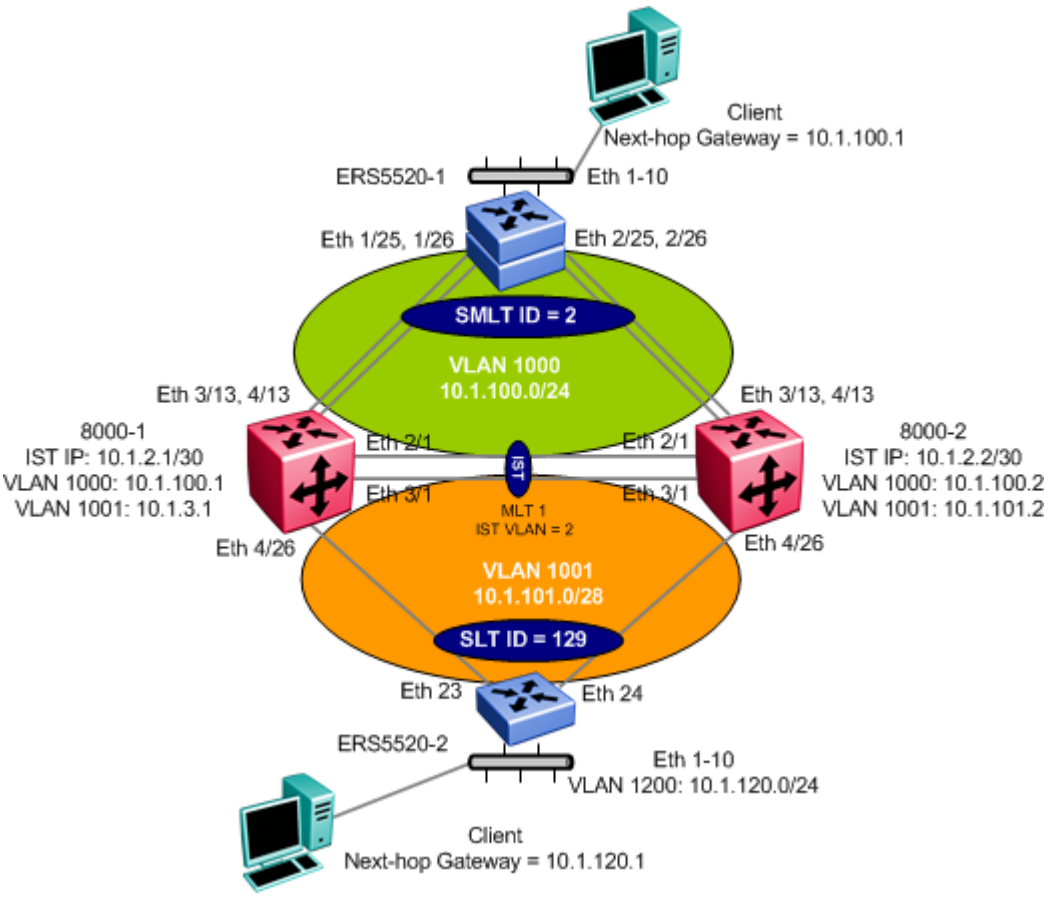


Figure 9: ERS 8600/8800 RSMLT

If the access switch supports L3, RSMLT can be enabled. For this example, we will configure the SMLT switch cluster with the following assuming ERS5520-2 is enabled for Layer 3:

- SMLT Cluster
  - Base SLT configuration is based on configuration from section 2.2.1 in regards to SLT configuration, CP Limit, Ext-CP Limit, SLPP, and VLACP
  - Add VLAN 1001 with IP subnet 10.1.101.0/24 and tagged port member 4/26; add IP address 10.1.101.1 to 8000-1 and 10.1.101.2 to 8000-2
  - Enable RSMLT on port 4/26
- Access Switch – ERS5520-2
  - Add VLAN 1001 with IP address 10.1.101.3/24 and MLT tagged trunk members 23 and 24
  - Add access VLAN 1200 with IP address 10.1.120.1/24 and user port members 1 to 10
  - Enable OSPF on both VLAN 1001 and 1200

2.8.1 Configuration – ERS 8600/8800 Switch Cluster using RSMLT

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

2.8.1.1 Create VLAN 1001

The following port based VLANs will be configured on the SMLT Switch cluster

- VLAN 1001 to be used at a Layer 3 level to ERS5520-2

ERS 8000 SMLT Cluster: Create VLAN 1001, add port members, and change the MAC fdb timer to the recommended value of 21601 seconds

8000-1:

```
8000-1:5(config)#vlan create 1001 name 5520-2 type port 1
8000-1:5(config)#vlan members remove 1000 4/26
8000-1:5(config)#vlan members add 1001 4/26
8000-1:5(config)#vlan mac-address-entry 1001 aging-time 21601
```

8000-2

```
8000-2:5# config vlan 1001 create byport 1 name 5520-2
8000-2:5# config vlan 1000 port remove 4/26
8000-2:6# config vlan 1001 port add 4/26
8000-2:5# config vlan 1001 fdb-entry aging-time 21601
```

2.8.1.2 Add IP address to VLAN 1001

ERS 8000 SMLT Cluster: Add IP address to VLAN 1001

8000-1:

```
8000-1:5(config)#interface vlan 1001
8000-1:5(config-if)#ip address 10.1.101.1 255.255.255.240
```

8000-2

```
8000-2:5# config vlan 1001 ip create 10.1.101.2/28
```

2.8.1.3 Enable OSPF

VLAN 1001 will be configured with OSPF on the SMLT Switch cluster.

ERS 8000 SMLT Cluster: Step 1 – Enable OSPF to VLAN 1000 with passive interface

8000-1:

```
8000-1:5(config)#interface vlan 1001
8000-1:5(config-if)#ip ospf enable
8000-1:5(config-if)#exit
```

8000-2

```
8000-2:5# config vlan 1001 ip ospf enable
```

ERS 8000 SMLT Cluster: Step 2 – Enable OSPF globally

8000-1:

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

8000-2

```
8000-2:5# config ip ospf enable
```

2.8.1.4 Enable RSMLT

VLAN 1001 with RSMLT using default RSMLT timers.

ERS 8000 SMLT Cluster: Enable RSMLT

8000-1:

```
8000-1:5(config)#interface vlan 1001
8000-1:5(config-if)#ip rsmlt
8000-1:5(config-if)#exit
```

8000-2

```
8000-2:5# config vlan 1001 ip rsmlt enable
```

2.8.2 Configuration - Edge Switch

2.8.2.1 Create VLANs 1001 and 1200 and Delete VLAN 1000

Assuming we are using the configuration from section 0, perform the following steps:

ERS5520-2: Create VLAN 1001 and 1200

```
5520-2(config)#vlan create 1001 name rsmlt_cluster type port
5520-2(config)#vlan create 1200 name access type port
5520-2(config)#vlan delete 1000
5520-2(config)# vlan members add 1001 23,24
5520-2(config)# vlan members add 1200 2-10
```

2.8.2.2 Add IP addresses

ERS5520-2: Step 1 – Add IP address to VLAN 1001

```
5520-2(config)# interface vlan 1001
5520-2(config-if)# ip address 10.1.101.3 255.255.255.240
5520-2(config-if)# exit
```

ERS5520-2: Step 2 – Add IP address to VLAN 1200

```
5520-2(config)#interface vlan 1200
5520-2(config-if)#ip address 10.1.120.1 255.255.255.0
5520-2(config-if)#exit
```

2.8.2.3 Enable OSPF

Enable OSPF on VLANs 3 and 1001. VLAN 1001 will be configured with OSPF passive interface.

ERS5520-2: Step 1 – Enable IP Routing

```
5520-2(config)#ip routing
```

ERS5520-2: Step 2 – Enable OSPF to VLAN 1200 with passive interface

```
5520-2(config)#interface vlan 1200
5520-2(config-if)#ip ospf network passive
5520-2(config-if)#ip ospf enable
5520-2(config-if)#exit
```

ERS5520-2: Step 3 – Enable OSPF to VLAN 1001

```
5520-2(config)#interface vlan 1001
5520-2(config-if)#ip ospf enable
```

```
5520-2(config-if)# exit
```

ERS5520-2: Step 4 – Enable OSPF globally

```
5520-2(config)#router ospf enable
```

2.8.2.4 DHCP Option

If you wish to enable DHCP relay for VLAN 1200, please enter the following command assuming the DHCP server IP address is 172.30.30.20. By default, DHCP is enabled on all VLANs when you add an IP address.

ERS5520-2: Step 4 – Enable relay agent

```
5520-2(config)#ip dhcp-relay fwd-path 10.1.120.1 172.30.30.20 mode dhcp
```

2.8.3 Verify RSMLT Operation

2.8.3.1 RSMLT Operations

Please note that only the output pertaining to VID 1001 is shown below.

Verify that the RSMLT instance is configured correctly and is functioning by issuing the following command:

ACLI

show ip rsmlt

CLI

show ip rsmlt info

Results:

8000-1:

```
================================================================================
                        Ip Rsmlt Local Info
================================================================================

VID   IP              MAC               ADMIN   OPER  HDTMR  HUTMR
--------------------------------------------------------------------------------
1001  10.1.101.1     00:01:81:28:86:1d  Enable  Up    60     180

VID   SMLT ID                  SLT ID
--------------------------------------------------------------------------------
1001                            129

================================================================================
                        Ip Rsmlt Peer Info
================================================================================

VID   IP              MAC               ADMIN   OPER  HDTMR  HUTMR
--------------------------------------------------------------------------------
1001  10.1.101.2     00:e0:7b:bc:22:03  Enable  Up    60     180

VID   HDT REMAIN  HUT REMAIN  SMLT ID                  SLT ID
--------------------------------------------------------------------------------
1001  60          180                                  129
```

On each ERS 8600/8800 in the switch cluster verify the following information:

Option	Verify
ADMIN	Verify that the RSMLT Admin is ***Enabled*** on both 8000-1 and 8000-2. If not, there is a configuration error.
OPER	Verify that the RSMLT operations is ***Up*** on both 8000-1 and 8000-2.
HDTMR HUTMR	Verify that the RSMLT holdup and holddown timer is set to ***60*** and ***180*** respectively on both 8000-1 and 8000-2. If not, there is a configuration error.
SMLT ID	Verify the SLT ID is showing ***129***.
Ip Rsmlt Peer Info	Verify the RSMLT Peer is showing: • 8000-1: VLAN ***1001***, SLT ***129*** , IP ***10.1.101.2*** and the corresponding MAC of RSMLT cluster peer • 8000-2: VLAN ***1001*** and SLT ***129***, IP ***10.1.101.1*** and the corresponding MAC of RSMLT cluster peer

2.9 Configuration – ERS 5000 Layer 2 SMLT Triangle Switch Cluster Configuration

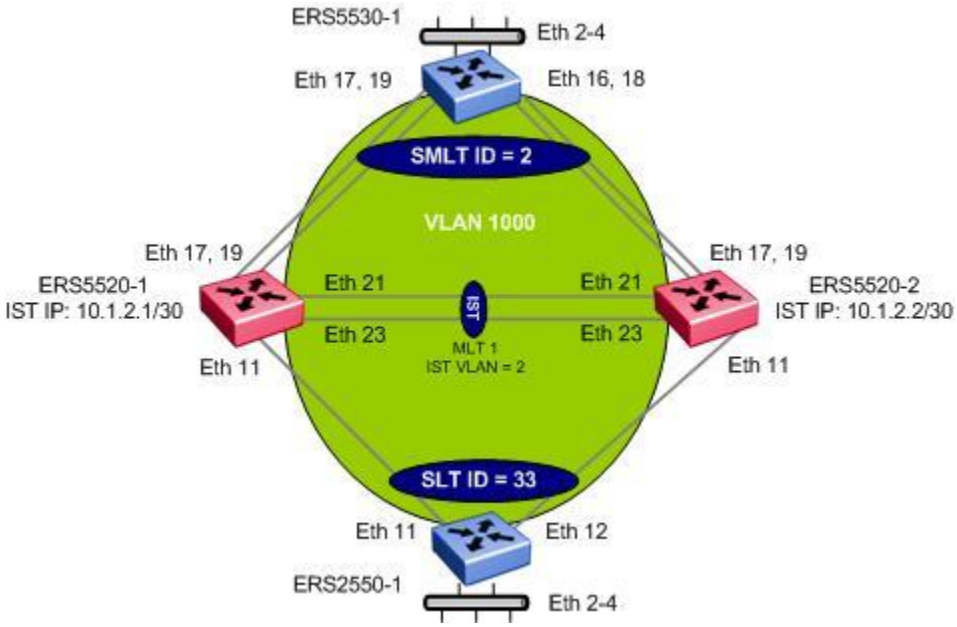


Figure 10: ERS 5000 Layer 2 Triangle SMLT Configuration

For this example, we will configure the SMLT switch cluster with the following:

- IST
  - IST VLAN 2 using MLT ID = 1
  - Tagged port members 21 and 23
  - All IST ports are Gigabit Ethernet ports using default setting of Autonegotiation enable
  - VLACP using the recommend reserved multicast MAC (01:80:C2:00:00:0F) and long timers
- SMLT and SLT
  - SMLT VLAN 1000
  - MLT and SMLT ID of 2 for ERS5530-1 with tagged port member 17 and 19
  - SLT ID of 33 for ERS2520-1 with tagged port member 11
  - Enable SLPP
  - All SMLT and SLT ports are 10/100 Mbps Ethernet ports using default setting of Autonegotiation enable
  - Enable VLACP with recommended reserved multicast MAC address, set VLACP timeout scale to 5, and use default short timers of 500ms; this is for the ERS5530-1 switch only as the ERS2550 does not support VLACP in its current release.
  - Enable “Discard Untagged Frames” on all SMLT/SLT port members
  - Disable STP on all SMLT ports
- On both ERS5530-1 and ERS2550-1, the following will be configured:

- Broadcast and multicast rate limiting with a threshold to 10%.
- Spanning Tree Fast Start on all edge ports
- BPDU filtering on all edge ports
- VLAN Tagging on SMLT access trunk ports

Presently, SMLT is supported in a standalone or stacked configuration. Square or full mesh topology is supported between ERS 5000 to ERS 5000 SMLT clusters or ERS 5000 to ERS 8600/8800 or VSP 9000 SMLT clusters. Please refer to document number NN48500-555 for more details.

You must have an Advanced Routing License to enable SMLT on the ERS 5000. Please ensure that you have obtained and installed the license prior to configuring SMLT on the ERS 5000 switch.

It is recommended to use the lowest MLT number for the IST which will be 1. In regards to the VLAN ID, it makes no difference what VLAN ID to use.

It is recommended to start the SLT numbering at 33 up to 512 even though you can use any number from 1 to 512. This is to avoid taking away a valid MLT ID that can be used for either a MLT or SMLT instance.

In a stacked configuration, when configuring a DMLT as an IST or SMLT, it is recommended that at least one port member is on the base. This help traffic recover faster in case of a base unit failure.

2.9.1 Configuration – ERS 5000 Layer 2 Switch Cluster

2.9.1.1 Configuration Mode

Go to configuration mode

```
config terminal
```

2.9.1.2 Create VLANs and enable discard untagged frames

The following port based VLANs will be configured on the SMLT Switch cluster

- VLAN 2 to be used by the Inter Switch Trunk (IST)
- VLAN 1000 to be used at a Layer 2 level to ERS5530-1 and ERS2550-1 for connecting users.

ERS 5000 SMLT Cluster – VLAN configuration

5520-1 & 5520-2: Same configuration on both switches

```
5520-1(config)#vlan create 2 name ist type port
5520-1(config)#vlan create 1000 name Services type port
5520-1(config)#vlan ports 11,17,19,21,23 tagging tagAll filter-untagged-frame enable
5520-1(config)#vlan members remove 1 11,17,19,21,23
```

```
5520-1(config)#vlan members 2 21,23
5520-1(config)#vlan members 1000 11,17,19,21,23
```

The above steps assume that the ERS 5000 switch is using the default VLAN configuration mode of *strict*. In this mode, you must first remove port members from the default VLAN 1 prior to adding these port members to a new VLAN. The VLAN configuration mode is set by using the command *vlan configcontrol <automatic|autopvid|flexible|strict>*

2.9.1.3 Enable VLACP globally and use the Reserved MAC

It is recommended to use the reserved multicast MAC address of 01:80:c2:00:00:0f for the VLACP MAC address. Via the ERS 5000, enter the hex value *180.c200.f*.

ERS5000 Cluster – Enable VLACP

5520-1 & 5520-2: Same configuration on both switches

```
5520-1(config)#vlacp macaddress 180.c200.f
5520-1(config)#vlacp enable
```

2.9.1.4 Create IST

Multilink Trunking 1 (MLT 1) will be used for the IST with port members 21 and 23. 802.1Q tagging will be enabled on all IST port members and Spanning Tree will be disabled on all IST port members via the MLT configuration. VLACP will be enabled on the IST trunk.

ERS5000 Cluster – Create IST and enable VLACP on IST port members using the recommended slow timer

5520-1:

```
5520-1(config)# mlt 1 name ist enable member 21,23 learning disable
5520-1(config)#ip routing
5520-1(config)#interface vlan 2
5520-1(config-if)#ip address 10.1.2.1 255.255.255.252
5520-1(config-if)#exit
5520-1(config)#interface mlt 1
5520-1(config-if)#ist enable peer-ip 10.1.2.2 vlan 2
5520-1(config-if)#exit
5520-1(config)#interface FastEthernet 21,23
5520-1(config-if)#vlacp slow-periodic-time 10000
5520-1(config-if)#vlacp enable
5520-1(config-if)#exit
```

5520-2: Same configuration as above except for VLAN 2 IP address and IST peer

```
5520-1(config)#interface vlan 2
```

```
5520-1(config-if)#ip address 10.1.2.2 255.255.255.252
5520-1(config-if)#exit
5520-1(config)#interface mlt 1
5520-1(config-if)#ist enable peer-ip 10.1.2.1 vlan 2
5520-1(config-if)#exit
```

2.9.1.5 SMLT-2 to ERS5530-1

ERS5000 Cluster – Create MLT 2 for SMLT 2

5520-1 & 5520-2: Same configuration on both switches

```
5520-1(config)#mlt 2 name 5530-1 enable member 17,19 learning disable
5520-1(config)#interface mlt 2
5520-1(config-if)#smlt 2
5520-1(config-if)#exit
```

2.9.1.6 SLT-33 to ERS2550-2

ERS5000 Cluster – Create SLT 33

5520-1 & 5520-2: Same configuration on both switches

```
5520-1(config)#interface FastEthernet ALL
5520-1(config-if)#smlt port 11 33
5520-1(config-if)#exit
```

2.9.1.7 SLPP

SLPP will be enabled globally and only on the SMLT access ports 17 and 19 and SLT access port 11 for VLAN 1000. On the SMLT primary switch we will set the SLPP packet-rx-threshold to 5, while on the SMLT secondary switch we will set the SLPP packet-rx-threshold to 50. For this example, we will pick ERS5520-1 as the primary switch.

The recommended SLPP receive threshold value for the primary switch is 5 and 50 for the secondary switch in an SMLT cluster.

SLPP should only be enabled on the SMLT access ports and not on the IST port members.

ERS5000 Cluster – Enable SLPP

5520-1:

```
5520-1(config)#slpp vid 1000
5520-1(config)#slpp enable
5520-1(config)#interface fastEthernet 11,17,19
```

```
5520-1(config-if)#slpp packet-rx-threshold 5
5520-1(config-if)# slpp enable
5520-1(config-if)#exit
```

5520-2: Same configuration as 5520-1 except for the SLPP packet receive threshold

```
5520-1(config-if)#slpp packet-rx-threshold 50
```

2.9.1.8 VLACP

As the access switches supports VLACP, we will enable this feature and use the short timeout option. By default the ERS 5000 uses a default short timeout of 500ms. In addition, we will use the recommended VLACP reserved MAC address and set the VLACP timeout scale to 5

Please note, software release 4.2 or higher is required on the ERS 2500 to support VLACP

ERS5000 Cluster – Enable VLACP

5520-1 & 5520-2: Same configuration on both switches

```
5520-1(config)#interface FastEthernet 11,17,19
5520-1(config-if)#vlacp timeout short
5520-1(config-if)#vlacp timeout-scale 5
5520-1(config-if)#vlacp enable
5520-1(config-if)#exit
```

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

2.9.2 Configuration - Edge Switch

2.9.2.1 Create VLAN

Create VLAN 2

5530-1:

```
5530-1(config)#vlan create 2 name core_1 type port
5530-1(config)#vlan members remove 1 2-4,16-19
5530-1(config)#vlan ports 1/25,2/25 tagging tagall
5530-1(config)#vlan members 2 2-4,16-18
```

2550-1:

```
2550-1(config)#vlan create 2 name core_1 type port
2550-1(config)#vlan members remove 1 2-4,11-12
2550-1(config)#vlan ports 11-12 tagging tagall
2550-1(config)#vlan members 2 2-4,11-12
```

2.9.2.2 Create MLT

Create MLT

5530-1:

```
5530-1(config)# mlt 1 name core_1 member 16-19 learning disable
5530-1(config)# mlt 1 enable
```

2550-1:

```
2550-1(config)#mlt 1 name core_1 member 11-12 learning disable
2550-1(config)#vlan mlt 1 enable
```

2.9.2.3 VLACP

Enable VLACP

5530-1:

```
5530-1(config)#vlacp macaddress 180.c200.f
5530-1(config)#vlacp enable
5530-1(config)#interface fastEthernet 16-19
5530-1(config-if)#vlacp timeout short
5530-1(config-if)#vlacp timeout-scale 5
5530-1(config-if)#vlacp enable
5530-1(config-if)#exit
```

2550-1:

```
2550-1(config)#vlacp macaddress 180.c200.f
2550-1(config)#vlacp enable
2550-1(config)#interface fastEthernet 11,12
2550-1(config-if)#vlacp timeout short
2550-1(config-if)#vlacp timeout-scale 5
2550-1(config-if)#vlacp enable
```

Please note that the ERS2500 requires software level 4.2 or higher to support VLACP.

2.9.2.4 Enable Spanning Tree Fast Start and BPDU filtering on all access ports

Enable STP Fast Start and BPDU filtering

5530-1 & 2550-1: Same configuration on both switches

```
5530-1(config)#interface fastEthernet 2-4
5530-1(config-if)#spanning-tree learning fast
5530-1(config-if)#spanning-tree bpdu-filtering timeout 0
5530-1(config-if)#spanning-tree bpdu-filtering enable
5530-1(config-if)#exit
```

Please note that the ERS2500 requires software level 4.2 or higher to support BPDU filtering.

2.9.2.5 Enable Rate Limiting

Enable Rate Limiting to 10% of total traffic for both broadcast and multicast traffic on 5530-1 and enable Rate Limiting to maximum value of 262143 pps for both broadcast and multicast traffic on 2550-1

5530-1:

```
5530-1(config)#interface fastEthernet all
5530-1(config-if)#rate-limit port 2-4 both 10
5530-1(config-if)#exit
```

2550-1:

```
2550-1(config)#interface fastEthernet 2-4
2550-1(config-if)#rate-limit both 262143
2550-1(config-if)#exit
```

Please note that the rate limit parameter on the ERS 5000 is expressed as percentage of total traffic whereas for the ERS2500 it is express in Packets Per Second (pps). The values used in this example are just a suggestion and may vary depending on your needs.

2.9.2.6 Discard Untagged Frames

Enable Discard Untagged Frames

5530-1:

```
5530-1(config)#vlan ports 16-18 filter-untagged-frame enable
```

2550-1:

```
2550-1(config)#vlan ports 11-12 filter-untagged-frame enable
```

2.9.3 Configuration File

ERS5520-1	ERS5520-2
enable configure terminal ! ! *** SNMP *** ! snmp-server enable snmp-server name "5520-1" ! ! *** VLAN *** ! vlan create 2,1000 type port 1 vlan name 2 "IST" vlan name 1000 "Services" vlan ports 11,17,19,21,23 tagging tagAll vlan configcontrol flexible vlan members 2 21,23 vlan members 1000 11,17,19,21,23 vlan configcontrol automatic ! ! *** MLT (Phase 1) *** ! mlt 1 name "ist" enable member 21,23 mlt 2 name "5530-1" enable member 17,19 ! ! *** STP (Phase 2) *** ! spanning-tree port-mode normal interface FastEthernet ALL spanning-tree port 11,17,19,21,23 learning disable exit ! ! *** MLT (Phase 2) *** ! mlt spanning-tree 1 stp 1 learning disable mlt spanning-tree 2 stp 1 learning disable ! ! *** L3 ***	enable configure terminal ! ! *** SNMP *** ! snmp-server enable snmp-server name "5520-2" ! ! *** VLAN *** ! vlan create 2,1000 type port 1 vlan name 2 "IST" vlan name 1000 "Services" vlan ports 11,17,19,21,23 tagging tagAll vlan configcontrol flexible vlan members 2 21,23 vlan members 1000 11,17,19,21,23 vlan configcontrol automatic ! ! *** MLT (Phase 1) *** ! mlt 1 name "ist" enable member 21,23 mlt 2 name "5530-1" enable member 17,19 ! ! *** STP (Phase 2) *** ! spanning-tree port-mode normal interface FastEthernet ALL spanning-tree port 11,17,19,21,23 learning disable exit ! ! *** MLT (Phase 2) *** ! mlt spanning-tree 1 stp 1 learning disable mlt spanning-tree 2 stp 1 learning disable ! ! *** L3 ***

```
!
ip routing
interface vlan 2
ip address 10.1.2.1 255.255.255.252 3
exit
!
! *** VLACP ***
!
vlacp enable
vlacp macaddress 180.c200.f
interface FastEthernet ALL
vlacp port 21,23 slow-periodic-time 10000
vlacp port 11,17,19 timeout short
vlacp port 11,17,19 timeout-scale 5
vlacp port 11,17,19,21,23 enable
exit
!
! *** SMLT ***
!
interface mlt 1
ist peer-ip 10.1.2.2
ist vlan 2
ist enable
exit
interface mlt 2
smlt 2
exit
interface FastEthernet all
smlt port 11 33
exit
!
! *** SLPP ***
!
slpp enable vid 1000
interface FastEthernet all
slpp port 11,17,19 enable packet-rx-threshold 5
exit
!
```

```
!
ip routing
interface vlan 2
ip address 10.1.2.2 255.255.255.252 3
exit
!
! *** VLACP ***
!
vlacp enable
vlacp macaddress 180.c200.f
interface FastEthernet ALL
vlacp port 21,23 slow-periodic-time 10000
vlacp port 11,17,19 timeout short
vlacp port 11,17,19 timeout-scale 5
vlacp port 11,17,19,21,23 enable
exit
!
! *** SMLT ***
!
interface mlt 1
ist peer-ip 10.1.2.1
ist vlan 2
ist enable
exit
interface mlt 2
smlt 2
exit
interface FastEthernet all
smlt port 11 33
exit
!
! *** SLPP ***
!
slpp enable vid 1000
interface FastEthernet all
slpp port 11,17,19 enable packet-rx-threshold
50
exit
!
```

2.9.4 Verify Operations

2.9.4.1 Verify MLT Configuration

Verify that the MLT instances is configured correctly and is functioning by issuing the following command:

show mlt

Results:

```
Id Name            Members              Bpdu   Mode          Status   Type
-- --------------- -------------------- ------ ------------- -------- -----
1  ist             21,23                All    Basic         Enabled  Trunk
2  5530-1          17,19                All    Basic         Enabled  Trunk
```

For each switch in the SMLT switch cluster, verify the following information:

Option	Verify
Members	Verify that the VLAN port members assigned to the IST and SMLT MLT are correct: • MLT 1: Port members ***21*** and ***23*** • MLT 2: Port members ***17*** and ***19***
Statues	Displays as ***Enabled***
Type	Displays as ***Trunk*** for MLT 1 and MLT 2

2.9.4.2 Virtual LANs (VLANs):

Step 1 – Verify the VLAN port assignments:

show vlan

Results:

```
Id  Name                 Type     Protocol         User PID Active IVL/SVL Mgmt
--- -------------------- -------- ---------------- -------- ------ ------- ----
1   VLAN #1              Port     None             0x0000   Yes    IVL     No
        Port Members: 2-10,12-16,18,20,22,24
2    ist                  Port     None             0x0000   Yes    IVL     No
        Port Members: 21,23
1000 vlan2                Port     None             0x0000   Yes    IVL     Yes
        Port Members: 11,17,19,21,23
```

Step 2 – Verify the VLAN port assignments and 802.1Q tagging settings by issuing the following commands:

show vlan interface info 11,17,19,21,23

Results:

```
      Filter     Filter
     Untagged Unregistered
Port  Frames     Frames    PVID PRI    Tagging    Name
---- -------- ------------ ---- --- ------------ ----------------
11   Yes      Yes          1    0   TagAll       Port 11
17   Yes      Yes          1    0   TagAll       Port 17
19   Yes      Yes          1    0   TagAll       Port 19
21   Yes      Yes          1    0   TagAll       Port 21
23   Yes      Yes          1    0   TagAll       Port 23
```

Step 3 - Verify the VLAN port assignments and 802.1Q tagging settings by issuing the following commands:

show vlan interface vids 11,17,19,21,23

Results:

```
Port VLAN VLAN Name         VLAN VLAN Name         VLAN VLAN Name
---- ---- ---------------  ---- ---------------  ---- ---------------
11   1000 vlan2
---- ---- ---------------  ---- ---------------  ---- ---------------
17   1000 vlan2
---- ---- ---------------  ---- ---------------  ---- ---------------
19   1000 vlan2
---- ---- ---------------  ---- ---------------  ---- ---------------
21   1000 vlan2            2    IST
---- ---- ---------------  ---- ---------------  ---- ---------------
23   1000 vlan2            2    IST
---- ---- ---------------  ---- ---------------  ---- ---------------
```

On each ERS 5000 in the switch cluster verify the following information:

Option	Verify
VLAN Port Members	VLAN Port Members: • VLAN 2: Port members ***21*** and ***23.*** • VLAN 1000: Port members ***11, 17, 19, 21,*** and ***23***
TAGGING	Displays as ***enable*** for all IST and SMLT ports. The value ***UntagAll*** indicates that the port is in an untagged mode. Filter Untagged Frames displays as ***Yes***.
VIDS	Displays as ***1000*** for all SMLT ports and as ***2*** for all IST ports.

2.9.4.3 Inter Switch Trunk (IST):

Verify that the IST is configured correctly and is functioning by issuing the following command:

show ist

Results:

```
=============================================================
MLT ID Enabled Running Master Peer IP Address Vlan ID
------ ------- ------- ------ --------------- -------
1      YES     YES     NO     10.1.2.2        2
```

On each ERS 5000 in the switch cluster verify the following information:

Option	Verify
MLT	Displays as ***1.*** The value ***1*** indicates that the IST is using MLT 1.
Running	Displays as ***YES***. The value ***YES*** indicates that the IST is operational.
Master	Verify that the one of the peer is Master: • 5520-1: ***NO*** • 5520- 2: ***YES***
Peer IP	Verify that the IST peer IP address is correct: • ERS5520-1: Will display the peer IP ***10.1.2.2*** • ERS5520-2: Will display the peer IP ***10.1.2.1***
Vlan ID	Displays the correct IST VLAN ID of ***2***.

2.9.4.4 Split MultiLink Trunking (SMLT):

Verify that SMLT is functioning correctly by issuing the following command:

show smlt mlt 2

Results:

```
=============================================================
                                        MLT SMLT Info
=============================================================
MLT    SMLT      ADMIN     CURRENT
ID     ID        TYPE      TYPE
-------------------------------------------------------------
2        2         smlt      smlt
```

On each ERS 5000 in the switch cluster verify the following information:

Option	Verify
MLT ID	Verify the SMLT ID ***2*** is assigned to MLT 2 is correct.
ADMIN TYPE	Displays as ***smlt***. The value ***norm*** indicates that the SMLT is not configured correctly.
CURRENT TYPE	Displays as ***smlt***. The value ***norm*** indicates that the SMLT instance is not operational. The value ***SMLT*** indicates that this SMLT instance is up and operational.

2.9.4.5 SMLT Single Link Trunking (SLT):

Verify that SLT is functioning correctly by issuing the following command:

show smlt fastethernet 33

Results:

```
                                        SLT Info
=================================================
PORT   SMLT      ADMIN     CURRENT
NUM    ID        TYPE      TYPE
-------------------------------------------------
11       33       slt       slt
```

On each ERS 5000 in the switch cluster verify the following information:

Option	Verify
Port Number	Verify the port number for SLT 33 is port ***11***.
ADMIN TYPE	Displays as ***slt***. The value ***norm*** indicates that the SLT is not configured correctly.
CURRENT TYPE	Displays as ***slt***. The value ***norm*** indicates that the SLT instance is not operational. The value ***SLT*** indicates that this SLT instance is up and operational.

The command *show smlt* will display all the current IST, SMLT, and SLT settings and state.

5520-1#***show smlt***

```
=============================================================================
                                        MLT SMLT Info
=============================================================================
MLT    SMLT      ADMIN     CURRENT
ID     ID        TYPE      TYPE
-----------------------------------------------------------------------------
1                 ist       ist
2        2        smlt      smlt
=============================================================================
                                        SLT Info
=============================================================================
PORT   SMLT      ADMIN     CURRENT
NUM    ID        TYPE      TYPE
-----------------------------------------------------------------------------
11       33       slt       slt
```

2.9.4.6 Simple Loop Prevention Protocol (SLPP):

Step 1 - Verify that SLPP is globally enabled on the switch by issuing the following command:

show slpp

Results:

```
================================================================================
                          SLPP Info
============================================================================
SLPP Enabled:  True
SLPP Transmission Interval:  500
SLPP Ether Type:  0x8104
SLPP Auto Port Re-Enable Timeout:  Disabled
SLPP Vlans:  1000
```

On each ERS 5000 in the switch cluster verify the following information:

Option	Verify
SLPP Enabled	Displays as ***True***. The value ***False*** indicates that SLPP is globally disabled on the switch.
vlan	Displays as ***1000*** indicating SLPP is enabled for VLAN 1000.

Step 2 - Verify the SLPP settings by issuing the following command:

show interfaces fastEthernet slpp 11,17,19

Results:

```
Port SLPP Enabled Pkt Rx Threshold Incoming Vlan Id Src Node Type
---- ------------ ---------------- ---------------- -------------
11   True         5                0                None
17   True         5                0                None
19   True         5                0                None
```

On each ERS 5000 in the switch cluster verify the following information:

Option	Verify
PORT	Displays the port numbers as per selected.
SLPP Enabled	Displays as ***true*** for ports where SLPP is enabled. The value ***False*** indicates that SLPP is disabled for the port.
Pkt Rx Threshold	Displays as ***5*** for each SMLT/SLT port on ERS5520-1 and ***50*** for each SMLT/SLT port on ERS5520-2.
Incoming Vlan	Displays as ***0*** as long as there is no loop. If there is a loop detected by SLPP, the corresponding VLAN will be shown under this column.
Src Node Type	Displays as ***None*** as long as there is no loop. Will be displayed as Peer if there is a loop detected.

If port 11 is disabled on either ERS5520-1 or ERS5520-2 due to either switch receiving its own SLPP-PDU, a message is logged and a trap will be issued. The following is an example of log message received on ERS5520-1 upon detecting its own SLPP-PDU caused by a loop in the network.

- 5520-1#***show logging sort-reverse***

```
I    00:02:49:45                  45       Trap:  Smlt Link Down, smlt:33
I    00:02:49:45                  44       Trap:  Smlt Link Down, smlt:33
I    00:02:49:45                  43       Link Down Trap for Port: 11
I    00:02:49:45                  42       Trap:  SLPP Port Down Event, Port:
11
I    00:02:45:23                  41       #0 Session opened from serial conne
```

Also, you view the SLPP port state by using the following command

- ERS5520-1:5#***show slpp interface 11***

```
Port SLPP Enabled Pkt Rx Threshold Incoming Vlan Id Src Node
Type
---- ------------ ---------------- ---------------- ------------
11   True         5                1000             Peer
```

2.9.4.7 Virtual Link Aggregation Control Protocol (VLACP):

Step 1 - Verify that VLACP is globally enabled by using the following command:

show vlacp

Results:

```
================================================================
                        Vlacp Global Information
================================================================
                  Multicast address :  01:80:c2:00:00:0f
                  Vlacp             :  enabled
```

On each ERS 5000 in the switch cluster verify the following information:

Option	Verify
Vlacp	Displays as ***enable***. The value ***disable*** indicates that VLACP is globally disabled on the switch.
Multicast address	Displays as ***01:80:c2:00:00:0f***. This indicates at the correct reserved address was entered correctly.

Step 2 - Verify the IST and SMLT per port VLACP settings by issuing the following command:

show vlacp interface 11,17,19,21,23

Results:

```
================================================================================
                            VLACP Information
================================================================================
PORT ADMIN   OPER    HAVE    FAST  SLOW  TIMEOUT TIMEOUT ETH  MAC
     ENABLED ENABLED PARTNER TIME  TIME  TYPE    SCALE   TYPE ADDRESS
--------------------------------------------------------------------------------
0/11  true    true    yes    500   30000 short   5       8103 01:80:c2:00:00:0f
0/17  true    true    yes    500   30000 short   5       8103 01:80:c2:00:00:0f
0/19  true    true    yes    500   30000 short   5       8103 01:80:c2:00:00:0f
0/21  true    true    yes    500   10000 long    3       8103 01:80:c2:00:00:0f
0/23  true    true    yes    500   10000 long    3       8103 01:80:c2:00:00:0f
```

On each ERS 5000 in the switch cluster verify the following information:

Option	Verify
ADMIN ENABLED	Displays as ***true*** for the IST, SMLT-2 and SLT-33 ports. The value ***false*** indicates that VLACP is disabled for the port.
OPER ENABLED	Displays as ***true*** for the IST, SMLT-2 and SLT-33 ports. The value ***false*** indicates that VLACP is not operational on the port.
TIME	Displays as ***10000*** for the IST port members. If not, please change the VLACP time value for the IST port members.
TIMEOUT TIME	Displays as ***long*** for the IST ports and ***short*** for SMLT-2 and SLT-33 ports. This value must match for each switch port in the link pair.
TIMEOUT SCALE	Display as ***5*** only for the SMLT-2 and SLT-33 port members..
MAC ADDR	The VLACP MAC address is assigned to each IST and SMLT-2: • IST ports 21 and 23: ***01:80:c2:00:00:0f*** • SMLT-2 ports 17 and 19: ***01:80:c2:00:00:0f*** • SLT-33 port 1: ***01:80:c2:00:00:0f*** The VLACP MAC address must match for each switch port in the link pair.

2.10 Configuration – ERS 5000 Triangle Switch Cluster using VRRP with Backup Master

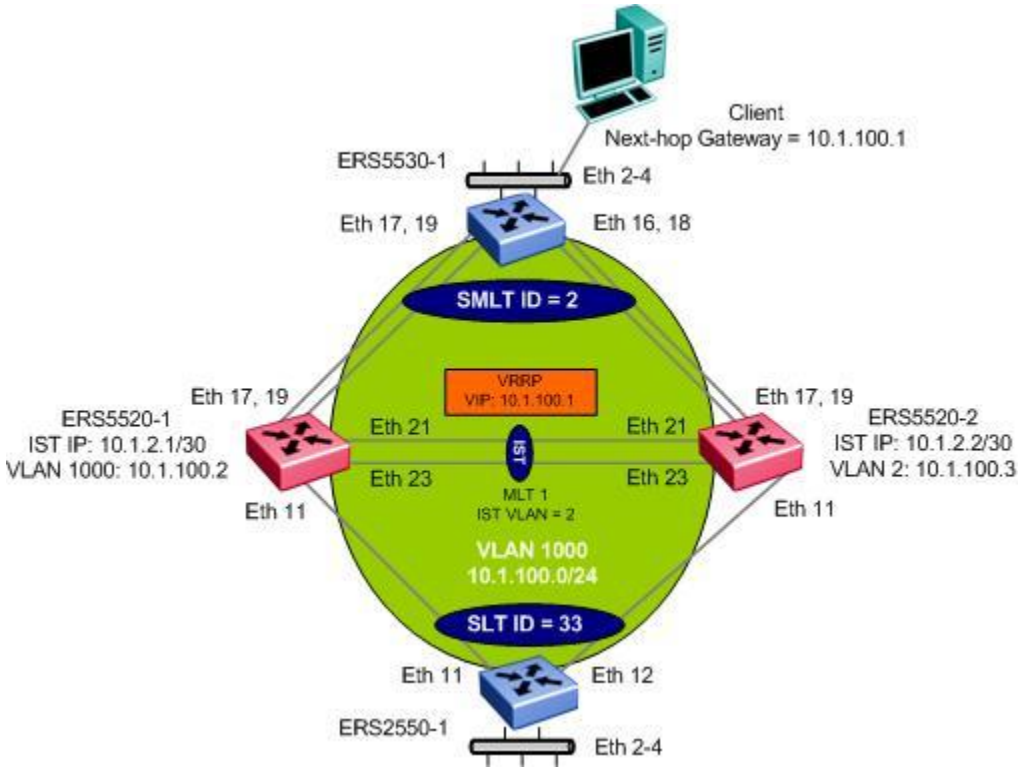


Figure 11: ERS 5000 Triangle SMLT Configuration with VRRP Backup Master

Assuming we take the same base setup as used in Section 2.9.1 but we now add a Layer 3 routing protocol with VRRP Backup Master. The configuration remains the same with the addition of enabling a routing protocol on VLAN 1000 and enabling VRRP Backup-Master.

Overall, we will use the same configuration steps as used in Section 2.9.1 and will add the following:

- Enable OSPF on VLAN 1000
  - VLAN 1000 on ERS5520-1 will be configured with IP address 10.1.100.2/24
  - VLAN 1000 on ERS5520-2 will be configured with IP address 10.1.100.3/24
  - Both ERS5520-1 and ERS5520-2 will be configured with OSPF passive interface as both switches are connected to Layer 2 access switches. This prevent OSPF messages being send to the access switches
  - Use default OSPF timers
- Enable VRRP on VLAN 2 with the following settings
  - Enable backup master
  - Set the hold down timer to 0 seconds on ERS5520-1 and ERS5520-2 – please see section 1.3.2.7
  - Set the VRRP VIP to 10.1.100.1 on both switches in the SMLT cluster
  - Set the VRRP virtual router id to 10

- Set the VRRP priority to 200 on ERS5520-1 so that it becomes the VRRP master and use the default value of 100 on ERS-5520-2 so that it becomes the VRRP backup

Normally, the VRRP hold down timer should be set long enough such that the IGP routing protocol has time to converge and update the routing table. However, for the ERS 5000 only in software releases prior to 6.2, the VRRP hold-down timer should be set to zero and the critical IP interface should not be used. For the ERS 5600 only starting with software release 6.2, the VRRP hold-down timer should be used as normal.

In Release 5.0.x, pinging the virtual IP address from the master VRRP routing switch is not supported. Please see document NN47200-400 (Release Notes — Software Release 5.0) for more detail and other VRRP/SMLT related issues. This problem has been corrected in software release 6.0, however, pinging the VRRP IP address from local console or telnet is not supported – please see Release Notes for release 6.0.

2.10.1 Configuration – ERS 5000 Layer 3 Switch Cluster using VRRP Backup Master

2.10.1.1 Add IP address to VLAN 1000

ERS5000 Cluster – Add IP address to VLAN 1000

5520-1:

```
5520-1(config)#interface vlan 1000
5520-1(config-if)#ip address 10.1.100.2 255.255.255.0
5520-1(config-if)#exit
```

5520-2:

```
5520-2(config)#interface vlan 1000
5520-2(config-if)#ip address 10.1.100.3 255.255.255.0
5520-2(config-if)#exit
```

2.10.1.2 Enable OSPF

VLAN 1000 will be configured with OSPF passive interface on the SMLT Switch cluster. As we have already enable IP routing globally when we configured the IST, we do not have to perform this step again.

ERS5000 Cluster: Step 1 – Enable OSPF to VLAN 1000 with passive interface

5520-1 & 5520-2: Same configuration on both switches

```
5520-1(config)#interface vlan 1000
5520-1(config-if)#ip ospf network passive
5520-1(config-if)#ip ospf enable
5520-1(config-if)# exit
```

ERS5000 Cluster: Step 1 – Enable OSPF globally

5520-1 & 5520-2: Same configuration on both switches

```
5520-1(config)#router ospf enable
```

2.10.1.3 Enable VRRP

ERS5000 Cluster: Step 1 – Enable VRRP Globally

5520-1 & 5520-2: Same configuration on both switches

```
5520-1(config)#router vrrp enable
```

ERS5000 Cluster: Step 2 – Add VIP, enable backup master, set the hold-down timer to 0, and enable VRRP to VLAN 1000.

5520-1:

```
5520-1(config)#interface vlan 1000
5520-1(config-if)#ip vrrp address 2 10.1.100.1
5520-1(config-if)#ip vrrp 2 backup-master enable
5520-1(config-if)#ip vrrp 2 holddown-timer 0
5520-1(config-if)#ip vrrp 2 priority 200
5520-1(config-if)#ip vrrp 2 enable
5520-1(config-if)#exit
```

5520-2: Same configuration as 5520-1 except for the VRRP priority

```
5520-2(config-if)#ip vrrp 2 priority 100
```

Please note if an ERS 5600 switch is used, starting with release 6.2, the VRRP holddown-timer should be used as normal. Hence, a holddown-timer value of 60 should be used if an ERS 5600 switch is used instead of an ERS 5520 as in this example.

2.10.1.4 DHCP Option

If you wish to enable DHCP relay for VLAN 1000, please enter the following command assuming the DHCP server IP address is 172.30.30.20. By default, DHCP is enabled on all VLANs when you add an IP address.

ERS5000 Cluster: Step 1 – Enable VRRP Globally

5520-1:

```
5520-1(config)#ip dhcp-relay fwd-path 10.1.100.2 172.30.30.20 mode dhcp
```

5520-2:

```
5520-1(config)#ip dhcp-relay fwd-path 10.1.100.3 172.30.30.20 mode dhcp
```

2.10.2 Configuration File

ERS5520-1	ERS5520-2
enable configure terminal ! ! *** L3 *** ! ip routing interface vlan 1000 ip address 10.1.100.2 255.255.255.0 4 exit ! ! *** L3 Protocols *** ! ! --- VRRP --- router vrrp enable interface vlan 1000 ip vrrp address 2 1.10.100.1 ip vrrp 2 enable ip vrrp 2 priority 200 ip vrrp 2 backup-master enable exit ! --- OSPF --- router ospf enable router ospf exit enable configure terminal interface vlan 1000 ip ospf network passive ip ospf enable exit	enable configure terminal ! ! *** L3 *** ! ip routing interface vlan 1000 ip address 10.1.100.3 255.255.255.0 4 exit ! ! *** L3 Protocols *** ! ! --- VRRP --- router vrrp enable interface vlan 1000 ip vrrp address 2 1.10.100.1 ip vrrp 2 enable ip vrrp 2 backup-master enable exit ! --- OSPF --- router ospf enable router ospf exit enable configure terminal interface vlan 1000 ip ospf network passive ip ospf enable exit

2.10.3 Verify Operations

2.10.3.1 VRRP Operations

Verify that the MLT instances is configured correctly and is functioning by issuing the following command "show ip vrrp interface <1-4094; VLAN id> verbose vrid <1-255>:

show ip vrrp interface 1000 verbose vrid 2

Results:

```
VLAN VR   Virtual                    Admin  Primary          Master
ID   ID   IP Address       State      State  IP Address       IP Address
---- ---  ---------------  ---------- -----  ---------------  ---------------
1000 2    10.1.100.1       Master     Up     10.1.100.2       10.1.100.2

VLAN VR       Adv       FastAdv  FastAdv   Critical    Critical
ID   ID   Pri Interval  Enabled  Interval  IP Enabled  IP Address
---- ---  --- --------  -------  --------  ----------  ---------------
1000 2    200 1         False    200       False       0.0.0.0

VLAN VR   BkMaster  BkMaster  Hold           Virtual            Virtual Router
ID   ID   Enabled   State     Timer  Action  MAC Address        Uptime
---- ---  --------  --------  -----  ------- -----------------  --------------
1000 2    True      Down      0      None    00:00:5e:00:01:02  0d 00:31:42

Total VRRP instances: 1
```

On each ERS 5000 in the switch cluster verify the following information:

Option	Verify
VRID	Verify that the VRRP VID is ***2*** on both ERS5520-1 and ERS5520-2. If not, there is a configuration error.
Virtual IP Address	Verify that the VRRP IP address is ***10.1.100.1*** on both ERS5520-1 and ERS5520-2. If not, there is a configuration error.
Virtual MAC Address	The VRRP MAC on both switches in the SMLT cluster should be the same.
Admin State	Verify that the VRRP administrative state is ***Up***.
State	Verify the VRRP state:

	• ERS5520-1: ***Master*** • ERS5520-2: ***Back Up***
Pri	Verify that the VRRP priority is set to ***200*** on ERS5520-1 and ***100*** on ERS5520-2. If not, configure the appropriate VRRP priority.
FastAdv Enabled	Verify that the VRRP Fast Advertise option is disabled.
Primary IP Address	Verify that VRRP master's IP address belongs to ERS5520-1 on both switches: • ERS5520-1: ***10.1.100.2*** • ERS5520-2: ***10.1.100.2***
BkMaster Enable	Verify that backup master is set to ***True*** on both switches. If not, enable VRRP backup master.
BkMaster STATE	Verify that VRRP backup master state on both switches: • ERS5520-1: ***down*** • ERS5520-2: ***up***
Hold Timer	Verify that the hold-down timer is set to ***0***.

2.11 Configuration – VSP 7000 Layer 2 SMLT Triangle Switch Cluster Configuration using Rear & Front Ports

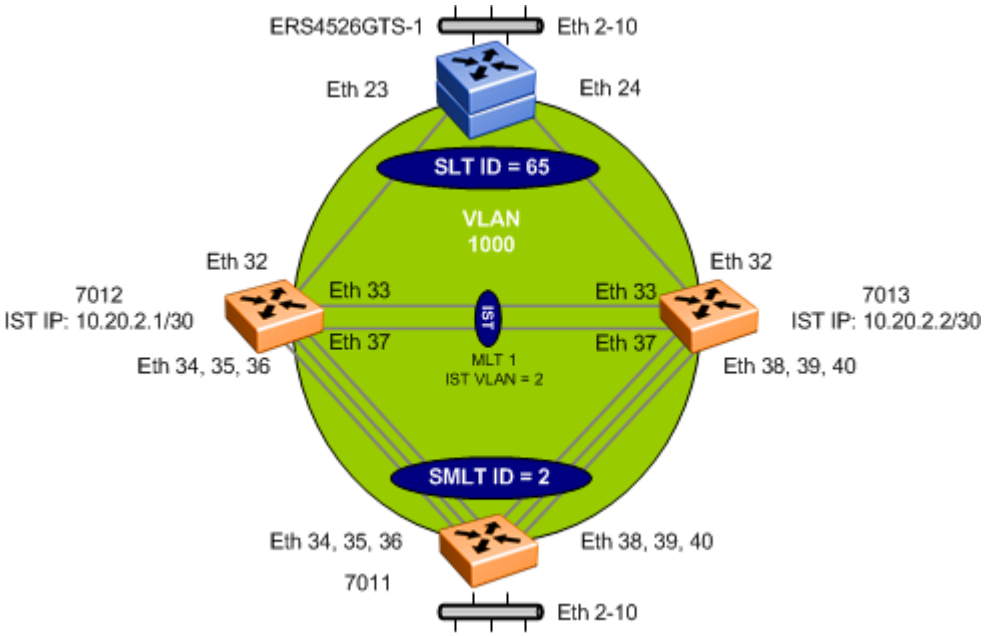


Figure 12: VSP 7000 Layer 2 Triangle SMLT Configuration

For this example, we will enable rear port mode and use the rear port for both the IST and a SMLT to another VSP 7000. Overall, we will configure the following.

- IST
  - IST VLAN 2 using MLT ID = 1
  - Tagged rear port members 33 and 37 (bottom two rear port)
  - VLACP using the recommend reserved multicast MAC (01:80:C2:00:00:0F), long timers and slow-periodic-time of 10,000ms
- SMLT and SLT
  - SMLT VLAN 1000
  - MLT and SMLT ID of 2 for switch 7011 using the rear ports – see diagram below
    - 7012 – using rear ports 34-36 to switch 7011 (top right rear port)
    - 7013 – using rear ports 38-40 to switch 7011 (top left rear port)
  - SLT ID of 65 for ERS4526GTS-1 with tagged port member 32
  - Enable “Discard Untagged Frames” on all SMLT/SLT port members
  - Enable SLPP
  - Disable STP on all SMLT ports

- Enable VLACP with recommended reserved multicast MAC address and with short timers of 500ms and set timeout scale to 5

- On both 7011 and ERS4526GTS-1, the following will be configured:
  - Broadcast and multicast rate limiting with a threshold to 10%.
  - Spanning Tree Fast Start on all edge ports
  - VLAN Tagging on SMLT access trunk ports

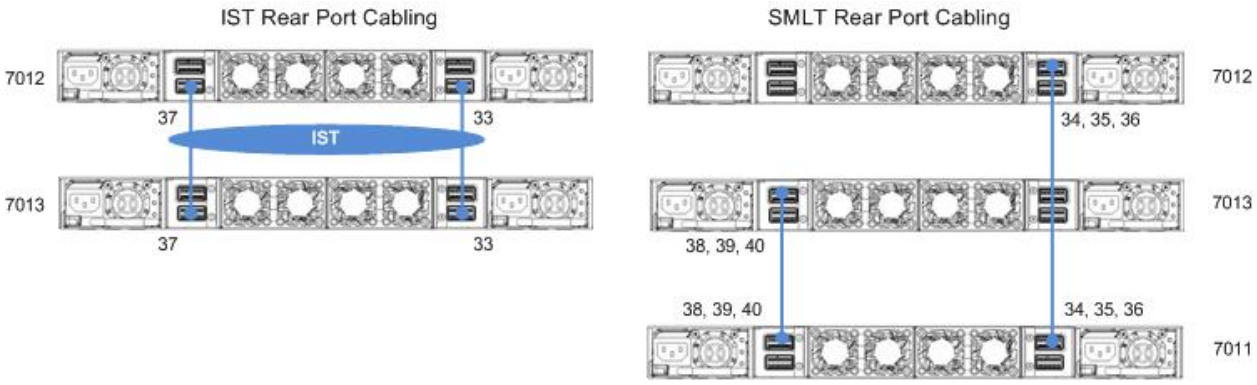


Figure 13: VSP 7000 Rear Port Cabling

You must have an Advanced Routing License to enable SMLT on the VSP 7000. Please ensure that you have obtained and installed the license prior to configuring SMLT on the VSP 7000 switch.

It is recommended to use the lowest possible MLT number for the IST which will be 1. For the SMLT, start with lowest MLT number available and work up.

It is recommended to start the SLT numbering at 65 up to 512 even though you can use any number from 1 to 512. This is to avoid taking away a valid MLT ID that can be used for either a MLT or SMLT instance. The VSP 7000 supports up to 32 MLT instances minus 1 for the IST in the 10.2.1 release, but, will support 64 MLT instances minus 1 for the IST in the 10.3 release.

2.11.1 Configuration – VSP 7000 Layer 2 Switch Cluster

2.11.1.1 Configuration Mode

Go to configuration mode

```
config terminal
```

2.11.1.2 VSP 7000 – Rear Port Mode

Switch	Parameter	Value
Rear Port		
7012, 7013	Rear port mode	Enabled
	LACP	Disable

Enable rear-port mode on switches 7012 and 7013

```
rear-port mode enable
Enabling rear port mode will disable Fabric Interconnect Stack operation.
Switch configuration will be reset to partial-defaults. Continue(yes/no)?y
```

```
show rear-port mode
Rear Port Mode:                Enabled Normal
Rear Port Operational State:   Operational Normal
```

```
interface fastEthernet 33-40
no lacp aggregation enable
lacp mode off
exit
```

Please note that by default LACP is enabled on all rear ports. For switches 7012 and 7013, we will be configuring the rear ports for SMLT with VLACP, hence, we will disable LACP.

2.11.1.3 Option: Change Spanning Tree mode to MSTP

We will change the Spanning Tree mode to MSTP. This is the default setting on the VSP 4000 and VSP 9000. When using tools such as VLAN Manager in COM, it is recommended to change the Spanning Tree mode to MSTP.

VSP 7000 Option – change spanning mode to MSTP on switches 7012 and 7013

```
spanning-tree mode mst
```

```
New operational mode MSTP will take effect upon reset
7024XLS(config)#boot
Reboot the unit(s) (y/n) ? y Rebooting . . .
--------------------------------------------------------------------------------
show spanning-tree mode
Current STP Operation Mode: MSTP
```

2.11.1.4 System Name

VSP 7000 Switches - Configure system name

```
snmp-server name <7012|7013>
```

2.11.1.5 IST Configuration

Switch	Feature	Parameter	Value
7012, 7013	IST	MLT ID	1
		VLAN	2
	VLACP (IST port members)	Timers	Long (slow)
		Time-out Scale	3
		VLACP MAC	01:80:c2:00:00:0f
		Slow periodic time	10000
	Filter Untagged Frames	Ports	33, 37
7012	IST VLAN	IP address	10.20.2.1/30
		Ports	33, 37
7013	IST VLAN	IP address	10.20.2.2/30
		Ports	33, 37

VSP 7000 SMLT Cluster – Add IST VLAN 2, add IP address, and enable VLACP

7012:

```
7012(config)#vlan create 2 name IST_vlan2 type port
```

```
7012(config)#mlt 1 name IST enable member 33,37 learning disable
7012(config)#vlan members add 2 33,37
7012(config)#vlan members remove 1 33,37
7012(config)#vlan ports 33,37 filter-untagged-frame enable
7012(config)#interface vlan 2
7012(config-if)#ip address 10.20.2.1 255.255.255.252
7012(config-if)#exit
7012(config)#interface mlt 1
7012(config-mlt)#ist peer-ip 10.20.2.2 vlan 2
7012(config-mlt)#ist enable
7012(config-mlt)#exit
7012(config)#interface fastEthernet 33,37
7012(config-if)#vlacp slow-periodic-time 10000
7012(config-if)#vlacp enable
7012(config-if)#exit
7012(config)#vlacp macaddress 01:80:c2:00:00:0f
7012(config)#vlacp enable
```

7013: Use the same configuration as 7012 except for the VLAN 2 IP address and IST peer

```
7013(config)#interface vlan 2
7013(config-if)#ip address 10.20.2.2 255.255.255.252
7013(config-if)#exit
7013(config)#interface mlt 1
7013(config-mlt)#ist peer-ip 10.20.2.1 vlan 2
7013(config-mlt)#ist enable
7013(config-mlt)#exit
```

2.11.1.6 Services VLAN configuration

Switch	Feature	Parameter	Value
7012, 7013	SMLT	MLT ID	2
		Ports	34-36, 38-40
	SLT	SLT ID	65
		Ports	32
	VLAN	VLAN ID	1000
7012		Ports	32, 34-36
7013		Ports	32, 38-70

VSP 7000 SMLT Cluster – Add SMLT 2

7012:

```
7012(config)#vlan create 1000 name services type port
7012(config)#mlt 2 name smlt_2 enable member 34-36 learning disable
7012(config)#vlan configcontrol automatic
7012(config)#vlan members add 1000 33-37
7012(config)#vlan members remove 1 34-36
7012(config)#interface mlt 2
7012(config-mlt)#smlt 2
7012(config-mlt)#exit
```

7013:

```
7013(config)#vlan create 1000 name services type port
7013(config)#mlt 2 name smlt_2 enable member 38-40 learning disable
7013(config)#vlan configcontrol automatic
7013(config)#vlan members add 1000 33,37-40
7013(config)#vlan members remove 1 38-40
7013(config)#interface mlt 2
7013(config-mlt)#smlt 2
7013(config-mlt)#exit
```

VSP 7000 SMLT Cluster – Add SLT 65

7012 & 7013: Same configuration on both switches

```
7012(config)#vlan ports 32 tagging tagall
7012(config)#vlan members add 1000 32
7012(config)#vlan members remove 1 32
7012(config)#interface fastEthernet 32
7012(config-if)#smlt 65
7012(config-if)#exit
```

2.11.1.7 Best Practices Configuration

Switch	Feature	Parameter	Value
7012, 7013	VLACP	Timers	Short (fast)
		Time-out Scale	3
		VLACP MAC	01:80:c2:00:00:0f
7012		Ports	32, 34-36
7013		Ports	32, 38-40
7012	Filter Untagged Frames	Ports	32, 34-36
7013		Ports	32, 38-40
7012, 7013	SLPP	VLAN	1000
		Operation	Enabled
7012		Threshold	5
7013		Threshold	50

VSP 7000 SMLT Cluster – Enable VLACP

7012:

```
7012(config)#interface fastEthernet 32,34-36
7012(config-if)#vlacp timeout short
7012(config-if)#vlacp timeout-scale 5
7012(config-if)#vlacp enable
7012(config-if)#exit
```

7013:

```
7013(config)#interface fastEthernet 32,38-40
7013(config-if)#vlacp timeout short
```

```
7013(config-if)#vlacp timeout-scale 5
7013(config-if)#vlacp enable
7013(config-if)#exit
```

VSP 7000 SMLT Cluster – Enable Untagged-frames-discard on all SMLT ports

7012:

```
7012(config)#vlan ports 32,34-36 filter-untagged-frame enable
```

7013:

```
7013(config)#vlan ports 32,38-40 filter-untagged-frame enable
```

VSP 7000 SMLT Cluster – Enable SLPP for VLAN 1000

7012:

```
7012(config)#slpp vid 1000
7012(config)#slpp enable
7012(config)#interface fastEthernet 32,34-36
7012(config-if)#slpp packet-rx-threshold 5
7012(config-if)#slpp enable
7012(config-if)#exit
```

7013:

```
7013(config)#slpp vid 1000
7013(config)#slpp enable
7013(config)#interface fastEthernet 32,38-40
7013(config-if)#slpp packet-rx-threshold 50
7013(config-if)#slpp enable
7013(config-if)#exit
```

2.11.2 Configuration - Edge Switch

2.11.2.1 VSP 7000 - Rear Port Mode

Enable rear-port mode on switches 7011

```
rear-port mode enable
Enabling rear port mode will disable Fabric Interconnect Stack operation.
Switch configuration will be reset to partial-defaults. Continue(yes/no)?y
```

```
show rear-port mode
Rear Port Mode:                Enabled Normal
Rear Port Operational State:   Operational Normal
```

```
interface fastEthernet 33-40
no lacp aggregation enable
lacp mode off
exit
```

Please note that by default LACP is enabled on all rear ports. For switch 7011, we will disable LACP and use VLACP.

2.11.2.2 Option: Change Spanning Tree Mode

Change spanning mode to MSTP on switches 7011 and ERS4526GTS-1

```
spanning-tree mode mst
New operational mode MSTP will take effect upon reset
7024XLS(config)#boot
Reboot the unit(s) (y/n) ? y Rebooting . . .
--------------------------------------------------------------------------------
show spanning-tree mode
Current STP Operation Mode: MSTP
```

2.11.2.3 VLAN and MLT configuration

Switch	Feature	Parameter	Value
7011, ERS4526GTS-1	MLT	MLT ID	1
7011		Ports	34-36, 38-40
ERS4526GTS-1		Ports	23-24
7011, ERS4526GTS-1	VLAN	VLAN ID	1000
7011		Ports	2-10, 34-36, 38-40
ERS4526GTS-1		Ports	2-10, 23-24

VSP 7011 & ERS4526GTS-1 – Add VLAN 1000 and enable VLACP on uplink ports

7011:

```
7011(config)#vlan create 1000 name services type port
7011(config)#mlt 1 name core enable member 34-36,38-40 learning disable
7011(config)#vlan configcontrol automatic
7011(config)#vlan members add 1000 2-10,34-36,38-40
7011(config)#vlan members remove 1 34-36,38-40
```

ERS4526GTS-1

```
ERS4526GTS-1(config)#vlan create 1000 name services type port
ERS4526GTS-1(config)#vlan ports 23-24 tagging tagall
ERS4526GTS-1(config)#mlt 1 name core enable member 23-24 learning disable
ERS4526GTS-1(config)#vlan configcontrol automatic
ERS4526GTS-1(config)#vlan members add 1000 2-10,23-24
ERS4526GTS-1(config)#vlan members remove 1 23-24
```

2.11.2.4 Best Practices Configuration

Switch	Feature	Parameter	Value
7011, ERS4526GTS-1	VLACP	Timers	Short (fast)
		Time-out Scale	5
		VLACP MAC	01:80:c2:00:00:0f
7011		Ports	34-36, 38-40
ERS4526GTS-1		Ports	23-24
7011	Filter Untagged Frames	Ports	34-36, 38-40
ERS4526GTS-1		Ports	23-24
7011, ERS4526GTS-1	Spanning Tree	Edge Port	True
		BPDU Filtering	Forever (timer = 0)
		Ports	2-10
7011, ERS4526GTS-1	Rate Limiting	Broadcast	10%
		Multicast	10%
ERS4526GTS-1	SLPP Guard	Timeout	0 (infinity)
7011	Unicast Storm Control	Action	Shutdown

Please note SLPP Guard is not available on the VSP 7000 at this time. Unicast storm control is only available on the ERS 5000 and VSP 7000.

VSP 7011 & ERS4526GTS-1

7011:

```
7011(config)#vlan ports 34-36,38-40 filter-untagged-frame enable
7011(config)#interface fastEthernet 34-36,38-40
7011(config-if)#vlacp timeout short
7011(config-if)#vlacp timeout-scale 5
7011(config-if)#vlacp enable
7011(config-if)#exit
7011(config)#interface fastEthernet 2-10
7011(config-if)#spanning-tree mstp edge-port true
7011(config-if)#spanning-tree bpdu-filtering enable timeout 0
7011(config-if)#rate-limit both 10
```

```
7011(config-if)#storm-control unicast action shutdown
7011(config-if)#exit
7011(config)#vlacp macaddress 01:80:c2:00:00:0f
7011(config)#vlacp enable
```

ERS4526GTS-1

```
ERS4526GTS-1(config)#vlan ports 23-24 filter-untagged-frame enable
ERS4526GTS-1(config)#interface fastEthernet 23-24
ERS4526GTS-1(config-if)#vlacp timeout short
ERS4526GTS-1(config-if)#vlacp timeout-scale 5
ERS4526GTS-1(config-if)#vlacp enable
ERS4526GTS-1(config-if)#exit
ERS4526GTS-1(config)#interface fastEthernet 2-10
ERS4526GTS-1(config-if)#spanning-tree mstp edge-port true
ERS4526GTS-1(config-if)#spanning-tree bpdu-filtering enable timeout 0
ERS4526GTS-1(config-if)#slpp-guard timeout 0 enable
ERS4526GTS-1(config-if)#rate-limit both 10
ERS4526GTS-1(config-if)#exit
ERS4526GTS-1(config)#vlacp macaddress 01:80:c2:00:00:0f
ERS4526GTS-1(config)#vlacp enable
```

2.11.3 Configuration File

7012	7013
enable configure terminal ! ! *** SNMP *** ! snmp-server name "7012" ! ! *** MSTP (Phase 1) *** ! spanning-tree mode mst ! ! *** LACP (Phase 1) *** ! interface fastEthernet ALL lacp mode port ALL off exit ! ! *** VLAN *** ! vlan create 2,1000 type port cist vlan name 2 "IST_vlan2" vlan name 1000 "services" vlan ports 32-37 tagging tagAll filter-untagged-frame enable vlan ports 38-40 tagging tagAll vlan configcontrol flexible vlan members 1 1-31 vlan members 2 33,37 vlan members 1000 32-37 vlan configcontrol strict ! ! *** LACP (Phase 2) *** ! interface fastEthernet ALL lacp mode port 33-40 off no lacp aggregation port 33-40 enable	enable configure terminal ! ! *** SNMP *** ! snmp-server name "7013" ! ! *** MSTP (Phase 1) *** ! spanning-tree mode mst ! ! *** LACP (Phase 1) *** ! interface fastEthernet ALL lacp mode port ALL off exit ! ! *** VLAN *** ! vlan create 2,1000 type port cist vlan name 2 "IST_vlan2" vlan name 1000 "services" vlan ports 32 tagging tagAll filter-untagged-frame enable vlan ports 33-37 tagging tagAll vlan ports 38-40 tagging tagAll filter-untagged-frame enable vlan configcontrol flexible vlan members 1 1-31 vlan members 2 33,37 vlan members 1000 32-33,37-40 vlan configcontrol automatic ! ! *** LACP (Phase 2) *** ! interface fastEthernet ALL lacp mode port 33-40 off no lacp aggregation port 33-40 enable

```
exit
!
! *** MSTP (Phase 2) ***
!
interface FastEthernet ALL
spanning-tree mstp port 32-40 learning disable
exit
!
! *** MLT (Phase 2) ***
!
mlt spanning-tree 1 stp 0 learning disable
!
! *** L3 ***
!
ip routing force
!
interface vlan 2
ip address 10.20.2.1 255.255.255.252 2
exit
!
! *** VLACP ***
!
vlacp enable
vlacp macaddress 180.c200.f
interface FastEthernet ALL
vlacp port 33,37 slow-periodic-time 10000
vlacp port 32,34-36,38-40 timeout short
vlacp port 32,34-36,38-40 timeout-scale 5
vlacp port 32-40 enable
exit
!
! *** SMLT ***
!
interface mlt 1
ist peer-ip 10.20.2.2
ist vlan 2
ist enable
exit
interface mlt 2
smlt 2
exit
```

```
exit
!
! *** MSTP (Phase 2) ***
!
interface FastEthernet ALL
spanning-tree mstp port 33-40 learning disable
exit
!
! *** MLT (Phase 2) ***
!
mlt spanning-tree 1 stp 0 learning disable
!
! *** L3 ***
!
ip routing force
!
interface vlan 2
ip address 10.20.2.2 255.255.255.252 2
exit
!
! *** VLACP ***
!
vlacp enable
vlacp macaddress 180.c200.f
interface FastEthernet ALL
vlacp port 33,37 slow-periodic-time 10000
vlacp port 32,34-36,38-40 timeout short
vlacp port 32,34-36,38-40 timeout-scale 5
vlacp port 32-40 enable
exit
!
! *** SMLT ***
!
interface mlt 1
ist peer-ip 10.20.2.1
ist vlan 2
ist enable
exit
interface mlt 2
smlt 2
exit
```

interface FastEthernet all smlt port 32 65 exit ! ! *** SLPP *** ! slpp enable slpp vid 1000 interface FastEthernet all slpp port 32,34-36 enable packet-rx-threshold 5 exit !	interface FastEthernet all smlt port 32 65 exit ! ! *** SLPP *** ! slpp enable slpp vid 1000 interface FastEthernet all slpp port 32,38-40 enable packet-rx-threshold 50 exit !

2.11.4 Verify Operations

2.11.4.1 VLACP Operations

Verify VLACP operation

show vlacp

show vlacp interface <ports>

Results:

7012:

```
7012(config)#show vlacp
================================================================================
                          Vlacp Global Information
================================================================================
                  Multicast address :  01:80:c2:00:00:0f
                  Vlacp             :  enabled
                  Vlacp hold time   :  0
7012#show vlacp interface 32-40
================================================================================================
                           VLACP Information
================================================================================================
PORT ADMIN   OPER    HAVE    FAST  SLOW  TIMEOUT TIMEOUT ETH  MAC
     ENABLED ENABLED PARTNER TIME  TIME  TYPE    SCALE   TYPE ADDRESS
------------------------------------------------------------------------------------------------
  32  true    true    yes     500   30000 short   5       8103 00:00:00:00:00:00
  33  true    true    yes     500   10000 long    3       8103 00:00:00:00:00:00
  34  true    true    yes     500   30000 short   5       8103 00:00:00:00:00:00
  35  true    true    yes     500   30000 short   5       8103 00:00:00:00:00:00
  36  true    true    yes     500   30000 short   5       8103 00:00:00:00:00:00
  37  true    true    yes     500   10000 long    3       8103 00:00:00:00:00:00
  38  true    false   no      500   30000 short   5       8103 00:00:00:00:00:00
  39  true    false   no      500   30000 short   5       8103 00:00:00:00:00:00
  40  true    false   no      500   30000 short   5       8103 00:00:00:00:00:00
7013#show vlacp interface 32-40
================================================================================================
                           VLACP Information
================================================================================================
PORT ADMIN   OPER    HAVE    FAST  SLOW  TIMEOUT TIMEOUT ETH  MAC
```

```
     ENABLED ENABLED PARTNER TIME  TIME  TYPE    SCALE   TYPE ADDRESS
-------------------------------------------------------------------------------
  32  true    true    yes     500   30000 short   5       8103 00:00:00:00:00:00
  33  true    true    yes     500   10000 long    3       8103 00:00:00:00:00:00
  34  true    false   no      500   30000 short   5       8103 00:00:00:00:00:00
  35  true    false   no      500   30000 short   5       8103 00:00:00:00:00:00
  36  true    false   no      500   30000 short   5       8103 00:00:00:00:00:00
  37  true    true    yes     500   10000 long    3       8103 00:00:00:00:00:00
  38  true    true    yes     500   30000 short   5       8103 00:00:00:00:00:00
  39  true    true    yes     500   30000 short   5       8103 00:00:00:00:00:00
  40  true    true    yes     500   30000 short   5       8103 00:00:00:00:00:00
```

On each VSP 7000 in the switch cluster verify the following information:

Option	Verify
ADMIN ENABLED	Displays as ***true*** for the IST (ports 33 and 37), SMLT (ports 34-36 on 7012 and ports 38-40 on 7013), and SLT-32 port (port 32). The value ***false*** indicates that VLACP is disabled for the port.
HAVE PARTNER	Displays as ***yes*** for the IST, SMLT, and SLT-32 ports. The value ***no*** indicates that VLACP is not operational on the port.
FAST TIME	Displays as ***500*** for the ports for the SMLT and SLT ports. The value must match for each switch port in the link pair.
SLOW TIME	Displays as ***10000*** for the IST ports 33 and 37, the IST port members. The value must match for each switch port in the link pair.
TIMEOUT TIME	Displays as ***long*** for the IST ports and ***short*** for the SMLT and SLT ports. This value must match for each switch port in the link pair.
MAC ADDR	The VLACP global should be displayed as ***01:80:c2:00:00:0f.***

2.11.4.2 Verify VLAN Configuration

Step 1 – Verify VLAN Tagging and Filter Untagged Frames

show vlan interface info <port>

Results:

7012:

```
7012#show vlan interface info 32-37
      Filter     Filter
     Untagged Unregistered
Port  Frames     Frames    PVID PRI    Tagging    Name
```

```
---- -------- ------------ ---- --- ------------- --------------
32   Yes      Yes          1    0   TagAll        Port 32
33   Yes      Yes          1    0   TagAll        Port 33
34   Yes      Yes          1    0   TagAll        Port 34
35   Yes      Yes          1    0   TagAll        Port 35
36   Yes      Yes          1    0   TagAll        Port 36
37   Yes      Yes          1    0   TagAll        Port 37
```

Step 2 – Verify VLAN Port Membership

show vlan interface vids <port>

Results:

```
7012#show vlan interface vids 32-37
Port VLAN VLAN Name          VLAN VLAN Name          VLAN VLAN Name
---- ---- ----------------  ---- ----------------  ---- ----------------
32   1000 services
---- ---- ----------------  ---- ----------------  ---- ----------------
33   2    IST_vlan2         1000 services
---- ---- ----------------  ---- ----------------  ---- ----------------
34   1000 services
---- ---- ----------------  ---- ----------------  ---- ----------------
35   1000 services
---- ---- ----------------  ---- ----------------  ---- ----------------
36   1000 services
---- ---- ----------------  ---- ----------------  ---- ----------------
37   2    IST_vlan2         1000 services
---- ---- ----------------  ---- ----------------  ---- ----------------
7013#show vlan interface vids 32-33,37-40
Port VLAN VLAN Name          VLAN VLAN Name          VLAN VLAN Name
---- ---- ----------------  ---- ----------------  ---- ----------------
32   1000 services
---- ---- ----------------  ---- ----------------  ---- ----------------
33   2    IST_vlan2         1000 services
---- ---- ----------------  ---- ----------------  ---- ----------------
37   2    IST_vlan2         1000 services
---- ---- ----------------  ---- ----------------  ---- ----------------
38   1000 services
---- ---- ----------------  ---- ----------------  ---- ----------------
39   1000 services
```

```
---- ---- ---------------  ---- ---------------  ---- ---------------
40   1000 services
---- ---- ---------------  ---- ---------------  ---- ---------------
```

On each VSP 7000 in the switch cluster verify the following information:

Option	Verify
VLAN IDS	Verify that the VLAN ids assigned to the IST and SMLT ports are correct: • IST Ports 33 & 37: Member of VLANs ***2*** & ***1000*** • SMLT 2 Ports: Member of VLAN ***1000*** • SLT 65 Ports: Member of VLAN ***1000***
TAGGING	Displays as ***TagAll*** for all IST and SMLT ports. The value ***untagAll*** indicates that the port is in an untagged mode and is the default value.
Filter Untagged Frames	Displays as ***Yes*** for all IST and SMLT ports. The value ***No*** indicates that the port will pass untagged frames and is the default value.

2.11.4.3 Verify MLT configuration

Step 1 – Verify MLT

show mlt

Results:

```
7012#show mlt
Id Name             Members               Bpdu   Mode           Status  Type
-- ---------------- --------------------- ------ -------------- ------- ------
1  IST              33,37                 All    Basic          Enabled Trunk
2  smlt_2           34-36                 All    Basic          Enabled Trunk
7013#show mlt
Id Name             Members               Bpdu   Mode           Status  Type
-- ---------------- --------------------- ------ -------------- ------- ------
1  IST              33,37                 All    Basic          Enabled Trunk
2  smlt_2           38-40                 All    Basic          Enabled Trunk
```

On each VSP 7000 in the switch cluster verify the following information:

Option	Verify
Members	Verify that the VLAN ids assigned to the IST and SMLT MLT are correct: • IST MLT 1: Port members ***33*** and ***37***

	• MLT 2: Port member ***34-36*** for switch 7012 and ***38-40*** for switch 7013
Status	Displays as ***Enabled*** indicating the MLT instance has been enabled
Type	Displays as ***Trunk*** for all IST and SMLT ports and will pass tagged frames. The value ***access*** indicates that the port will pass untagged frames.

2.11.4.4 Inter Switch Trunk (IST)

Step 1 – Verify IST

```
show ist
```

Results:

7012:

```
MLT ID Enabled Running Master Peer IP Address Vlan ID
------ ------- ------- ------ --------------- -------
1      YES     YES     NO     10.20.2.2       2
```

7013:

```
MLT ID Enabled Running Master Peer IP Address Vlan ID
------ ------- ------- ------ --------------- -------
1      YES     YES     YES    10.20.2.1       2
```

On each VSP 7000 in the switch cluster verify the following information:

Option	Verify
Enable	Displays as ***YES*** to indicate the IST is enabled.
Running	Displays as ***YES*** to indicate the IST is up and operational
Peer IP Address	Verify that the IST peer IP address is correct: • 7012: Will display the peer IP ***10.20.2.2*** • 7013: Will display the peer IP ***10.20.2.1***
Vlan ID	Displays as ***2***, indicating that VLAN 2 has been provisioned as the IST VLAN ID.

2.11.4.5 Split MultiLink Trunking (SMLT)

Step 1 – Verify SMLT

show smlt

Results:

7012 & 7013:

```
================================================================================
                                      MLT SMLT Info
================================================================================
MLT    SMLT      ADMIN     CURRENT
ID     ID        TYPE      TYPE
--------------------------------------------------------------------------------
1                 ist       ist
2        2        smlt      smlt
================================================================================
                                      SLT Info
================================================================================
PORT   SMLT      ADMIN     CURRENT
NUM    ID        TYPE      TYPE
--------------------------------------------------------------------------------
32       65       slt       slt
```

On each VSP 7000 in the switch cluster verify the following information:

Option	Verify
ADMIN TYPE	Displays as ***ist*** for MLT 1***, smlt*** for SMLT 2***,*** and ***slt*** for SLT 65 (SLT 65 on port 32) indicating the SMLT type provisioned
CURRENT TYPE	Displays as ***ist*** for MLT 1***, smlt*** for SMLT 2***,*** and ***slt*** for SLT 65 (SLT 65 on port 32) indicating that the IST, SMLT and/or SLT is up and operational. If not operational, ***Norm*** will be displayed indicating either mis-configuration or networking problems.

2.11.4.6 Virtual Link Aggregation Control Protocol (VLACP):

Step 1 – Verify VLACP global configuration

show vlacp

Results:

7012 & 7013:

```
================================================================================
                          Vlacp Global Information
================================================================================
                  Multicast address :  01:80:c2:00:00:0f
                  Vlacp             :  enabled
                  Vlacp hold time   :  0
```

On each VSP 7000 in the switch cluster verify the following information:

Option	Verify
Multicast address	Displays as ***01:80:c2:00:00:0f***.
Vlacp	Displays as ***enable***. The value ***disable*** indicates that VLACP is globally disabled on the switch.

Step 2 – Verify VLACP at interface level

show vlacp interface 32-40

Results:

7012:

```
================================================================================
                          VLACP Information
================================================================================
PORT ADMIN   OPER    HAVE    FAST  SLOW  TIMEOUT TIMEOUT ETH  MAC
     ENABLED ENABLED PARTNER TIME  TIME  TYPE    SCALE   TYPE ADDRESS
--------------------------------------------------------------------------------
  32  true    true    yes    500   30000 short   5       8103 00:00:00:00:00:00
  33  true    true    yes    500   10000 long    3       8103 00:00:00:00:00:00
  34  true    true    yes    500   30000 short   5       8103 00:00:00:00:00:00
  35  true    true    yes    500   30000 short   5       8103 00:00:00:00:00:00
  36  true    true    yes    500   30000 short   5       8103 00:00:00:00:00:00
```

```
  37  true    true    yes    500   10000 long    3       8103 00:00:00:00:00:00
  38  true    false   no     500   30000 short   5       8103 00:00:00:00:00:00
  39  true    false   no     500   30000 short   5       8103 00:00:00:00:00:00
  40  true    false   no     500   30000 short   5       8103 00:00:00:00:00:00
```

7013:

```
================================================================================
                          VLACP Information
================================================================================
PORT ADMIN   OPER    HAVE    FAST  SLOW  TIMEOUT TIMEOUT ETH  MAC
     ENABLED ENABLED PARTNER TIME  TIME  TYPE    SCALE   TYPE ADDRESS
--------------------------------------------------------------------------------
  32  true    true    yes    500   30000 short   5       8103 00:00:00:00:00:00
  33  true    true    yes    500   10000 long    3       8103 00:00:00:00:00:00
  34  true    false   no     500   30000 short   5       8103 00:00:00:00:00:00
  35  true    false   no     500   30000 short   5       8103 00:00:00:00:00:00
  36  true    false   no     500   30000 short   5       8103 00:00:00:00:00:00
  37  true    true    yes    500   10000 long    3       8103 00:00:00:00:00:00
  38  true    true    yes    500   30000 short   5       8103 00:00:00:00:00:00
  39  true    true    yes    500   30000 short   5       8103 00:00:00:00:00:00
  40  true    true    yes    500   30000 short   5       8103 00:00:00:00:00:00
```

On each VSP 7000 in the switch cluster verify the following information:

Option	Verify
ADMIN ENABLED	Displays as ***true*** for the IST (ports 33 and 37), SMLT-2 (ports 34—36 for 7012 and port 38-40 for 7013), and SLT-65 port (port 32). The value ***false*** indicates that VLACP is disabled for the port.
OPER ENABLED	Displays as ***true*** for the IST, SMLT-2, and SLT-65 ports. The value ***false*** indicates that VLACP is not operational on the port.
FAST TIME	Displays as ***500*** for the ports 32 & 34-36 for 7012 and port 32 & 38-40 for 7013. The value must match for each switch port in the link pair.
SLOW TIME	Displays as ***10000*** for the ports 33 and 37, the IST port members. The value must match for each switch port in the link pair.
TIMEOUT TIME	Displays as ***long*** for the IST ports and ***short*** for SMLT-2 and SLT-65 ports. This value must match for each switch port in the link pair.

2.11.4.7 SLPP

Step 1 – Verify SLPP globally

show slpp

Results:

7012 & 7013:

```
SLPP Enabled:  True
SLPP Transmission Interval:  500
SLPP EtherType:  0x8102
SLPP Auto Port Re-Enable Timeout:  Disabled
SLPP Vlans:  1000
```

On each VSP 7000 in the switch cluster verify the following information:

Option	Verify
SLPP Enabled	Displays as ***True*** indicating that SLPP is globally enabled on the switch.
SLPP Vlans	Displays as ***1000*** as we only enable SLPP for this one VLAN**.**

Step 1 – Verify the SLPP Packet Receive and Packet Threshold settings

show slpp interface 32-40

Results:

7012:

```
7012#show slpp interface 32-40
Port SLPP Enabled Pkt Rx Threshold Incoming Vlan Id Src Node Type
---- ------------ ---------------- ---------------- -------------
32   True         5                0                None
33   False        5                0                None
34   True         5                0                None
35   True         5                0                None
36   True         5                0                None
37   False        5                0                None
38   False        5                0                None
39   False        5                0                None
40   False        5                0                None
```

7013:

```
7013#show slpp interface 32-40
Port SLPP Enabled Pkt Rx Threshold Incoming Vlan Id Src Node Type
---- ------------ ---------------- ---------------- -------------
32   True         50               0                None
33   False        5                0                None
34   False        5                0                None
35   False        5                0                None
36   False        5                0                None
37   False        5                0                None
38   True         50               0                None
39   True         50               0                None
40   True         50               0                None
```

On each VSP 7000 in the switch cluster verify the following information:

Option	Verify
SLPP	Displays as ***True*** for SLT port 32 and SMLT ports 34-36 on 7012 and SMLT port 38-40 on 7013. The value ***False*** indicates that SLPP is disabled for the port.
Pkt Rx Threshold	Displays as ***5*** for primary switch 7012 and ***50*** for the secondary switch 7013
Incoming Vlan Id	Displays as ***0*** for normal operations. If there is a loop, the VLAN ID will be shown, i.e. ***1000*** will be shown on the Secondary SMLT cluster switch if there is a loop
Src Node Type	Displays as ***None*** for normal operations. If there is a loop, ***Peer*** will be shown on the Primary SMLT cluster switch

2.12 Configuration – VSP 7000 Triangle Switch Cluster using VRRP with Backup Master and OSPF

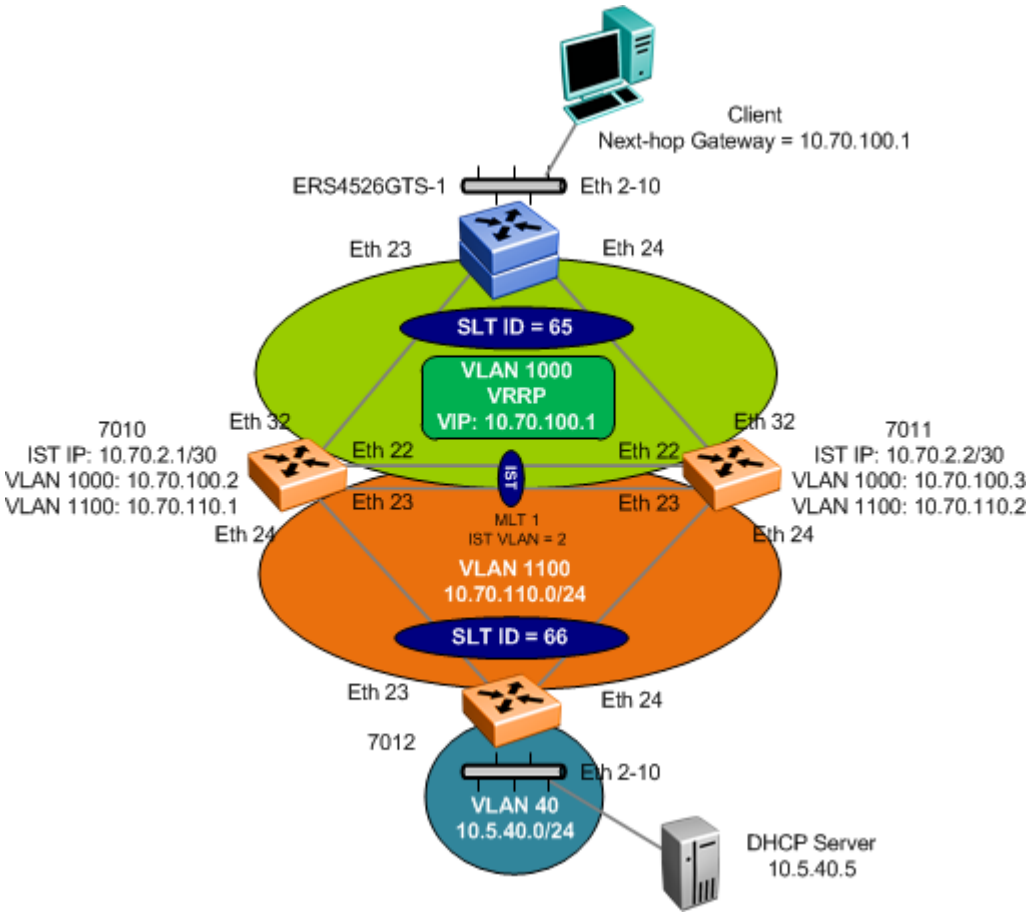


Figure 14: VSP 7000 Triangle SMLT Configuration with VRRP Backup Master

Please note that OSPF over SMLT in the 10.2.1 release is only supported in standalone mode and no rear port support.

For this example, we now add an OSPF passive interface with VRRP Backup Master to an edge ERS 4000 switch and enable OSPF to an edge VSP 7000.

Overall, we will add the following:

- Enable OSPF & VRRP Backup Master on VLAN 1000
  - VLAN 1000 on 7010 will be configured with IP address 10.70.100.2/24
  - VLAN 1000 on 7011 will be configured with IP address 10.70.100.3/24
  - Both 7010 and 7013 will be configured with OSPF passive interface as both switches are connected to Layer 2 access switches. This prevent OSPF messages being send to the access switches
  - Use default OSPF timers

- Enable VRRP backup master
- Set the hold down timer to 60 seconds on 7002 & 7013
- Set the VRRP VIP to 10.70.100.1 on both switches in the SMLT cluster
- Set the VRRP virtual router id to 100
- Set the VRRP priority to 150 on 7010 so that it becomes the VRRP master and use the default value of 100 on 7011 so that it becomes the VRRP backup

The VRRP hold down timer should be set long enough such that the IGP routing protocol has time to converge and update the routing table. In some cases, setting the VRRP hold down timer a minimum of 1.5 times the IGP convergence time should be sufficient. For OSPF, it is suggested to use a value of 60 seconds if using the default OSPF timers.

- Enable DHCP Relay for VLAN 1000
- Enable OSPF on VLAN 1100 to edge VSP 7000 switch 7012
  - VLAN 1100 on 7010 with be configured with IP address 10.70.110.1/24 and setup to be the OSPF DR with an OSPF priority of 200
  - VLAN 1100 on 7011 with be configured with IP address 10.70.110.2/24 and setup to be the OSPF BDR with an OSPF priority of 150

2.12.1 Configuration – VSP 7000 Layer 3 Switch Cluster using VRRP Backup Master

2.12.1.1 Configuration Mode

Go to configuration mode

```
config terminal
```

2.12.1.2 Option: Change Spanning Tree mode to MSTP

We will change the Spanning Tree mode to MSTP. This is the default setting on the VSP 4000 and VSP 9000. When using tools such as VLAN Manager in COM, it is recommended to change the Spanning Tree mode to MSTP.

VSP 7000 Option – change spanning mode to MSTP on switches 7012 and 7013

```
spanning-tree mode mst
New operational mode MSTP will take effect upon reset
7024XLS(config)#boot
Reboot the unit(s) (y/n) ? y Rebooting . . .
--------------------------------------------------------------------------------
show spanning-tree mode
Current STP Operation Mode: MSTP
```

2.12.1.3 System Name

VSP 7000 Switches - Configure system name

```
snmp-server name <7010|7011>
```

2.12.1.4 IST Configuration

Switch	Feature	Parameter	Value
7010, 7011	IST	MLT ID	1
		VLAN	2
	VLACP (IST port members)	Timers	Long (slow)
		Time-out Scale	3
		VLACP MAC	01:80:c2:00:00:0f
		Slow periodic time	10000
	Filter Untagged Frames	Ports	22, 23
7010	IST VLAN	IP address	10.70.2.1/30
		Ports	22, 23
7011	IST VLAN	IP address	10.70.2.2/30
		Ports	22, 23

VSP 7000 SMLT Cluster – Add IST VLAN 2, add IP address, and enable VLACP

7010:

```
7010(config)#vlan create 2 name IST_vlan2 type port
7010(config)#vlan ports 22-23 tagging tagall
7010(config)#mlt 1 name IST enable member 22-23 learning disable
7010(config)#vlan configcontrol automatic
7010(config)#vlan members add 2 22-23
7010(config)#vlan members remove 1 22-23
7010(config)#vlan ports 22-23 filter-untagged-frame enable
7010(config)#interface vlan 2
7010(config-if)#ip address 10.70.2.1 255.255.255.252
```

```
7010(config-if)#exit
7010(config)#interface mlt 1
7010(config-mlt)#ist peer-ip 10.20.2.2 vlan 2
7010(config-mlt)#ist enable
7010(config-mlt)#exit
7010(config)#interface fastEthernet 22,23
7010(config-if)#vlacp slow-periodic-time 10000
7010(config-if)#vlacp enable
7010(config-if)#exit
7010(config)#vlacp macaddress 01:80:c2:00:00:0f
7010(config)#vlacp enable
```

7011: Use the same configuration as 7010 except for VLAN 2 IP address and IST peer

```
7011(config)#interface vlan 2
7011(config-if)#ip address 10.20.2.2 255.255.255.252
7011(config-if)#exit
7011(config)#interface mlt 1
7011(config-mlt)#ist peer-ip 10.70.2.1 vlan 2
7011(config-mlt)#ist enable
7011(config-mlt)#exit
```

2.12.1.5 Services VLAN configuration

Switch	Feature	Parameter	Value
7010, 7011	SLT	SLT ID	65
		Port	32
	SLT	SLT ID	66
		Port	24
	VLAN	VLAN ID	1000
		Ports	22-23, 32
	VLAN	VLAN ID	1100
		Ports	22-24

VSP 7000 SMLT Cluster – Add SLT 33

7010 & 7011: Same configuration on both switches

```
7010(config)#vlan ports 24,32 tagging tagall
7010(config)#vlan create 1000,1100
7010(config)#vlan members add 1000 22-23,32
7010(config)#vlan members add 1000 22-24
7010(config)#vlan members remove 1 24,32
7010(config)#interface fastEthernet 32
7010(config-if)#smlt 65
7010(config-if)#exit
7010(config)#interface fastEthernet 24
7010(config-if)#smlt 66
7010(config-if)#exit
```

2.12.1.6 Best Practices Configuration

Switch	Feature	Parameter	Value
7010, 7011	VLACP	Timers	Short (fast)
		Time-out Scale	3
		VLACP MAC	01:80:c2:00:00:0f
		Ports	24, 32
7010, 7011	Filter Untagged Frames	Ports	24, 32
7010, 7011	SLPP	VLAN	1000
		Operation	Enabled
7011		Threshold	5
7011		Threshold	50

VSP 7000 SMLT Cluster – Enable VLACP

7010 & 7011: Same configuration on both switches

```
7010(config)#interface fastEthernet 24,32
7010(config-if)#vlacp timeout short
7010(config-if)#vlacp timeout-scale 5
7010(config-if)#vlacp enable
7010(config-if)#exit
```

VSP 7000 SMLT Cluster – Enable Untagged-frames-discard on all SMLT ports

7010 & 7011: Same configuration on both switches

```
7010(config)#vlan ports 24,32 filter-untagged-frame enable
```

VSP 7000 SMLT Cluster – Enable SLPP for VLAN 1000

7010:

```
7010(config)#slpp vid 1000
7010(config)#slpp enable
7010(config)#interface fastEthernet 32
7010(config-if)#slpp packet-rx-threshold 5
7010(config-if)#slpp enable
7010(config-if)#exit
```

7011: Same configuration as 7011 except for the SLPP packet receive threshold

```
7011(config-if)#slpp packet-rx-threshold 50
```

2.12.1.7 IP configuration

Step1: VSP 7000 SMLT Cluster – Add IP Address to VLAN 1000, enable OSPF, and enable VRRP Backup Master using a VIP 100 using a VRRP priority of 150 on switch 7010

7010:

```
7010(config)#interface vlan 1000
7010(config-if)#ip address 10.70.100.2 255.255.255.0
7010(config-if)#ip ospf network passive
7010(config-if)#ip ospf enable
7010(config-if)#ip vrrp address 100 10.70.100.1
7010(config-if)#ip vrrp 100 backup-master enable priority 150
7010(config-if)#ip vrrp 100 holddown-timer 60
7010(config-if)#ip vrrp 100 enable
7010(config-if)#exit
```

7011: Same configuration as 7010 except for VLAN 1000 IP address and VRRP priority

```
7011(config-if)#ip address 10.70.100.3 255.255.255.0
7011(config-if)#ip vrrp 100 backup-master enable
```

Step 2: VSP 7000 SMLT Cluster – Add IP Address to VLAN 1100, enable OSPF, and setup OSPF priority to 200 on 7010 and 150 on 7011

7010:

```
7010(config)#interface vlan 1100
7010(config-if)#ip address 10.70.110.1 255.255.255.0
7010(config-if)#ip ospf priority 200
7010(config-if)#ip ospf enable
7010(config-if)#exit
```

7011: Same configuration as 7010 except for VLAN 1100 IP address

```
7011(config-if)#ip address 10.70.110.2 255.255.255.0
7011(config-if)#ip ospf priority 150
```

2.12.1.8 Enable OSPF and VRRP Globally

VSP 7000 SMLT Cluster – Enable OSPF globally

7010 & 7011: Same configuration on both switches

```
7010(config)#router ospf enable
7010(config)#router vrrp enable
```

2.12.1.9 Add DHCP Relay Agent

VSP 7000 SMLT Cluster – Add DHCP relay agent for VLAN 1000

7010:

```
7010(config)#ip dhcp-relay fwd-path 10.70.100.2 10.5.40.5 mode dhcp
```

7011:

```
7011(config)#ip dhcp-relay fwd-path 10.70.100.3 10.5.40.5 mode dhcp
```

2.12.1.10 Option – Add loopback address as OSPF router id

Assuming we wish to add lpbk addresses of 10.70.1.1/32 to 7010 and 10.70.1.2/32 to 7011 and also use the lpbk addresses as the OSPF router id.

VSP 7000 SMLT Cluster – Add lpbk address and OSPF router id

7010:

```
7010(config)#interface loopback 1
7010(config-if)#ip address 10.70.1.1 255.255.255.255
7010(config-if)#ip ospf
```

```
7010(config-if)#exit
7010(config)#router ospf
7010(config-router)#router-id 10.70.1.1
7010(config-router)#exit
```

7011:

```
7011(config)#interface loopback 1
7011(config-if)#ip address 10.70.1.2 255.255.255.255
7011(config-if)#ip ospf
7011(config-if)#exit
7011(config)#router ospf
7011(config-router)#router-id 10.70.1.2
7011(config-router)#exit
```

2.12.2 Configuration – Edge Switch

2.12.2.1 Option: Change Spanning Tree Mode

Change spanning mode to MSTP on switches 7011 and ERS4526GTS-1

```
spanning-tree mode mst
New operational mode MSTP will take effect upon reset
7024XLS(config)#boot
Reboot the unit(s) (y/n) ? y Rebooting . . .
--------------------------------------------------------------------------------
show spanning-tree mode
Current STP Operation Mode: MSTP
```

2.12.2.2 VLAN and MLT configuration

Switch	Feature	Parameter	Value
7012, ERS4526GTS-1	MLT	MLT ID	1
		Ports	23-34
ERS4526GTS-1	VLAN	VLAN ID	1000
		Ports	2-10, 23-24
7012	VLAN	VLAN ID	1100
		Ports	23-34
	VLAN	VLAN ID	40
		Ports	2-10

VSP 7011 & ERS4526GTS-1 – Add VLAN 1000 and enable VLACP on uplink ports

7012:

```
7012(config)#vlan create 40,1100 type port
7012(config)#vlan ports 23-24 tagging tagall
7012(config)#mlt 1 name core enable member 23-24 learning disable
7012(config)#vlan configcontrol automatic
7012(config)#vlan members add 1100 23-24
7012(config)#vlan members add 40 2-10
7012(config)#vlan members remove 1 23-24
```

ERS4526GTS-1

```
ERS4526GTS-1(config)#vlan create 1000 name services type port
ERS4526GTS-1(config)#vlan ports 23-24 tagging tagall
ERS4526GTS-1(config)#mlt 1 name core enable member 23-24 learning disable
ERS4526GTS-1(config)#vlan configcontrol automatic
ERS4526GTS-1(config)#vlan members add 1000 2-10,23-24
ERS4526GTS-1(config)#vlan members remove 1 23-24
```

2.12.2.3 Best Practices Configuration

Switch	Feature	Parameter	Value
7012, ERS4526GTS-1	VLACP	Timers	Short (fast)
		Time-out Scale	5
		VLACP MAC	01:80:c2:00:00:0f
		Ports	23-24
7012, ERS4526GTS-1	Filter Untagged Frames	Ports	23-24
7012, ERS4526GTS-1	Spanning Tree	Edge Port	True
		BPDU Filtering	Forever (timer = 0)
		Ports	2-10
7012, ERS4526GTS-1	Rate Limiting	Broadcast	10%
		Multicast	10%
ERS4526GTS-1	SLPP Guard	Timeout	0 (infinity)
7012	Unicast Storm Control	Action	Shutdown

Please note SLPP Guard is not available on the VSP 7000 at this time.

VSP 7011 & ERS4526GTS-1

7012:

```
7012(config)#vlan ports 23-24 filter-untagged-frame enable
7012(config)#interface fastEthernet 23-24
7012(config-if)#vlacp timeout short
7012(config-if)#vlacp timeout-scale 5
7012(config-if)#vlacp enable
```

```
7012(config-if)#exit
7012(config)#interface fastEthernet 2-10
7012(config-if)#spanning-tree mstp edge-port true
7012(config-if)#spanning-tree bpdu-filtering enable timeout 0
7012(config-if)#rate-limit both 10
7012(config-if)#storm-control unicast action shutdown
7012(config-if)#exit
7012(config)#vlacp macaddress 01:80:c2:00:00:0f
7012(config)#vlacp enable
```

ERS4526GTS-1

```
ERS4526GTS-1(config)#vlan ports 23-24 filter-untagged-frame enable
ERS4526GTS-1(config)#interface fastEthernet 23-24
ERS4526GTS-1(config-if)#vlacp timeout short
ERS4526GTS-1(config-if)#vlacp timeout-scale 5
ERS4526GTS-1(config-if)#vlacp enable
ERS4526GTS-1(config-if)#exit
ERS4526GTS-1(config)#interface fastEthernet 2-10
ERS4526GTS-1(config-if)#spanning-tree mstp edge-port true
ERS4526GTS-1(config-if)#spanning-tree bpdu-filtering enable timeout 0
ERS4526GTS-1(config-if)#slpp-guard timeout 0 enable
ERS4526GTS-1(config-if)#rate-limit both 10
ERS4526GTS-1(config-if)#exit
ERS4526GTS-1(config)#vlacp macaddress 01:80:c2:00:00:0f
ERS4526GTS-1(config)#vlacp enable
```

2.12.2.4 IP Configuration

Step 1: 7012 – Add IP Address to VLAN 1100 and enable OSPF

7012:

```
7012(config)#interface vlan 1100
7012(config-if)#ip address 10.70.110.3 255.255.255.0
7012(config-if)#ip ospf enable
7012(config-if)#exit
```

Step 2: 7012 – Add IP Address to VLAN 40 and enable OSPF

7012:

```
7012(config)#interface vlan 1100
7012(config-if)#ip address 10.5.40.1 255.255.255.0
```

```
7012(config-if)#ip ospf enable
7012(config-if)#exit
```

2.12.2.5 Enable OSPF Globally

7012 – Enable OSPF globally

7012:

```
7012(config)#router ospf enable
```

2.12.2.6 Option – Add loopback address as OSPF router id

Assuming we wish to add lpbk addresses of 10.70.1.3/32 to 7012 and also use the lpbk addresses as the OSPF router id.

7012 – Add lpbk address and OSPF router id

7012:

```
7012(config)#interface loopback 1
7012(config-if)#ip address 10.70.1.3 255.255.255.255
7012(config-if)#ip ospf
7012(config-if)#exit
7012(config)#router ospf
7012(config-router)#router-id 10.70.1.3
7012(config-router)#exit
```

2.12.3 Configuration File

7010	7011
enable	enable
configure terminal	configure terminal
!	!
! *** SNMP ***	! *** SNMP ***
!	!
snmp-server name "7010"	snmp-server name "7011"
!	!
!	!
! *** MSTP (Phase 1) ***	! *** MSTP (Phase 1) ***
!	!
spanning-tree mode mst	spanning-tree mode mst
!	!
! *** VLAN ***	! *** VLAN ***
!	!
vlan create 2,1000,1100 type port cist	vlan create 2,1000,1100 type port cist
vlan name 2 "IST"	vlan name 2 "IST"
vlan name 1000 "services"	vlan name 1000 "services"
vlan ports 22-24,32 tagging tagAll filter-untagged-frame enable	vlan ports 22-24,32 tagging tagAll filter-untagged-frame enable
vlan configcontrol flexible	vlan configcontrol flexible
vlan members 1 1-21,25-31	vlan members 1 1-21,25-31
vlan members 2 22-23	vlan members 2 22-23
vlan members 1000 22-23,32	vlan members 1000 22-23,32
vlan members 1100 22-24	vlan members 1100 22-24
vlan configcontrol automatic	vlan configcontrol automatic
!	!
! *** Rate-Limit ***	! *** Rate-Limit ***
!	!
interface FastEthernet ALL	interface FastEthernet ALL
rate-limit port 2-10 both 10	rate-limit port 2-10 both 10
exit	exit
!	!
! *** MLT (Phase 1) ***	! *** MLT (Phase 1) ***
!	!
mlt 1 name "IST" enable member 22-23	mlt 1 name "IST" enable member 22-23
!	!
! *** MSTP (Phase 2) ***	! *** MSTP (Phase 2) ***
!	!

interface FastEthernet ALL	interface FastEthernet ALL
spanning-tree mstp port 22-24,32 learning disable	spanning-tree mstp port 22-24,32 learning disable
spanning-tree mstp port 2-10 edge-port true	spanning-tree mstp port 2-10 edge-port true
spanning-tree bpdu-filtering port 2-10 enable timeout 0	spanning-tree bpdu-filtering port 2-10 enable timeout 0
exit	exit
!	!
! *** L3 ***	! *** L3 ***
!	!
!	!
ip routing force	ip routing force
!	!
interface vlan 2	interface vlan 2
ip address 10.70.2.1 255.255.255.252 2	ip address 10.70.2.2 255.255.255.252 2
exit	exit
interface vlan 1000	interface vlan 1000
ip address 10.70.100.2 255.255.255.0 5	ip address 10.70.100.3 255.255.255.0 5
exit	exit
interface vlan 1100	interface vlan 1100
ip address 10.70.110.1 255.255.255.0 3	ip address 10.70.110.2 255.255.255.0 3
exit	exit
interface loopback 1	interface loopback 1
ip address 10.70.1.1 255.255.255.255	ip address 10.70.1.2 255.255.255.255
exit	exit
!	!
! *** VLACP ***	! *** VLACP ***
!	!
vlacp enable	vlacp enable
vlacp macaddress 180.c200.f	vlacp macaddress 180.c200.f
interface FastEthernet ALL	interface FastEthernet ALL
vlacp port 22-23 slow-periodic-time 10000	vlacp port 22-23 slow-periodic-time 10000
vlacp port 24-25,32 timeout short	vlacp port 24,32 timeout short
vlacp port 24-25,32 timeout-scale 5	vlacp port 24,32 timeout-scale 5
vlacp port 22-25,32 enable	vlacp port 22-24,32 enable
exit	exit
!	!
! *** DHCP Relay ***	! *** DHCP Relay ***
!	!
ip dhcp-relay fwd-path 10.70.100.2 10.5.40.5	ip dhcp-relay fwd-path 10.70.100.3 10.5.40.5
ip dhcp-relay fwd-path 10.70.100.2 10.5.40.5 mode dhcp	ip dhcp-relay fwd-path 10.70.100.3 10.5.40.5 mode dhcp

```
!
! *** L3 Protocols ***
!
! --- VRRP ---

router vrrp enable
interface vlan 1000
ip vrrp address 100 10.70.100.1
ip vrrp 100 enable
ip vrrp 100 priority 150
ip vrrp 100 holddown-timer 60
ip vrrp 100 backup-master enable
exit
! --- OSPF ---

router ospf enable
router ospf
router-id 10.70.1.1
exit
interface vlan 1000
ip ospf network passive
ip ospf priority 150
ip ospf enable
exit
interface vlan 1100
ip ospf priority 200
ip ospf enable
exit
interface loopback 1
ip ospf
exit
!
! *** SMLT ***
!
interface mlt 1
ist peer-ip 10.70.2.2
ist vlan 2
ist enable
exit
interface FastEthernet all
smlt port 24 66
```

```
!
! *** L3 Protocols ***
!
! --- VRRP ---

router vrrp enable
interface vlan 1000
ip vrrp address 100 10.70.100.1
ip vrrp 100 enable
ip vrrp 100 holddown-timer 60
ip vrrp 100 backup-master enable
exit

! --- OSPF ---

router ospf enable
router ospf
router-id 10.70.1.2
exit
interface vlan 1000
ip ospf network passive
ip ospf priority 200
ip ospf enable
exit
interface vlan 1100
ip ospf priority 150
ip ospf enable
exit
interface loopback 1
ip ospf
exit
!
! *** SMLT ***
!
interface mlt 1
ist peer-ip 10.70.2.1
ist vlan 2
ist enable
exit
interface FastEthernet all
smlt port 24 66
```

smlt port 32 65 exit ! ! *** SLPP *** ! slpp enable slpp vid 1000 interface FastEthernet all slpp port 32 enable packet-rx-threshold 5 exit	smlt port 32 65 exit ! ! *** SLPP *** ! slpp enable slpp vid 1000 interface FastEthernet all slpp port 32 enable packet-rx-threshold 50 exit

2.12.4 Verify Operations

2.12.4.1 VRRP Operations

Step 1 – Verify VLACP global setting

show ip vrrp

Results:

7010 & 7011:

```
VRRP Version:  2
VRRP Notifications Enabled:  Yes
VRRP Enabled:  Yes
VRRP Ping Virtual Address Enabled:  Yes
```

Step 2 – Verify VLACP operation

show ip vrrp interface verbose vrid 100

Results:

7010:

```
VLAN VR   Virtual                    Admin  Primary         Master
ID   ID   IP Address       State      State  IP Address      IP Address
---- ---  ---------------  ---------- -----  --------------- ---------------
1000 100  10.70.100.1      Master     Up     10.70.100.2     10.70.100.2

VLAN VR       Adv       FastAdv  FastAdv   Critical    Critical
ID   ID   Pri  Interval  Enabled  Interval  IP Enabled  IP Address
---- ---  ---  --------  -------  --------  ----------  ---------------
1000 100  150  1         False    200       False       0.0.0.0

VLAN VR   BkMaster  BkMaster  Hold           Virtual            Virtual Router
ID   ID   Enabled   State     Timer  Action  MAC Address        Uptime
---- ---  --------  --------  -----  ------- -----------------  --------------
1000 100  True      Down      0      None    00:00:5e:00:01:64  3d 21:24:45

Total VRRP instances: 1
```

7011:

```
VLAN VR   Virtual                    Admin  Primary         Master
ID   ID   IP Address       State      State  IP Address      IP Address
---- ---  ---------------  ---------- -----  --------------- ---------------
```

```
1000 100  10.70.100.1      Backup      Up     10.70.100.3      10.70.100.2

VLAN VR        Adv       FastAdv  FastAdv   Critical    Critical
ID   ID   Pri  Interval  Enabled  Interval  IP Enabled  IP Address
---- ---  ---  --------  -------  --------  ----------  ---------------
1000 100  100  1         False    200       False       0.0.0.0

VLAN VR   BkMaster  BkMaster  Hold            Virtual            Virtual Router
ID   ID   Enabled   State     Timer  Action   MAC Address        Uptime
---- ---  --------  --------  -----  -------  -----------------  --------------
1000 100  True      Up        0      None     00:00:5e:00:01:64  3d 21:26:07

Total VRRP instances: 1
```

On each VSP 7000 in the switch cluster verify the following information:

Option	Verify
VR ID	Verify that the VRRP VID is ***100*** on both 7010 and 7011. If not, there is a configuration error.
Virtual IP Address	Verify that the VRRP IP address is ***10.70.100.1*** on both 7010 and 7011. If not, there is a configuration error.
Virtual MAC Address	The VRRP MAC on both switches in the SMLT cluster should be the same.
State	Verify the VRRP state: • 7010: ***Master*** • 7011: ***Back Up***
Pri	Verify that the VRRP priority is set to ***150*** on 7010 and ***100*** on 7011. If not, configure the appropriate VRRP priority.
Master IP Address	Verify that VRRP master's IP address belongs to 7010 on both switches: • 7010: ***10.70.100.2*** • 7011: ***10.70.100.2***
BkMaster Enable	Verify that backup master is set to ***True*** on both switches. If not, enable VRRP backup master.
BkMaster State	Verify that VRRP backup master state on both switches: • 7010: ***Down***

	• 7011: ***Up***

2.12.4.2 Verify DHCP Relay

Step 1 – Verify DHCP relay agent

show ip vrrp interface verbose vrid 100

Results:

7010:

```
==============================================================
                        DHCP Fwd-path
==============================================================
VLAN     INTERFACE         SERVER            ENABLE     MODE
--------------------------------------------------------------
1000     10.70.100.2       10.5.40.5         TRUE       DHCP
```

7011:

```
==============================================================
                        DHCP Fwd-path
==============================================================
VLAN     INTERFACE         SERVER            ENABLE     MODE
--------------------------------------------------------------
1000     10.70.100.3       10.5.40.5         TRUE       DHCP
```

2.12.4.3 Verify OSPF operations

Step 1 – Verify OSPF interface

show ip ospf interface enabled

Results:

7010:

```
Interface:  10.70.1.1
    Area ID:  0.0.0.0
    Admin State:  Enabled
    Type:  Passive
    Priority:  1
    Designated Router:  10.70.1.1
    Backup Designated Router:  0.0.0.0
    Authentication Type:  None
    MTU Ignore:  Yes
```

```
    Advertise When Down:  No
    Metric Value:  10
Interface:  10.70.100.2
    Area ID:  0.0.0.0
    Admin State:  Enabled
    Type:  Passive
    Priority:  150
    Designated Router:  10.70.100.2
    Backup Designated Router:  0.0.0.0
    Authentication Type:  None
    MTU Ignore:  Yes
    Advertise When Down:  No
    Metric Value:  10
Interface:  10.70.110.1
    Area ID:  0.0.0.0
    Admin State:  Enabled
    Type:  Broadcast
    Priority:  200
    Designated Router:  10.70.110.2
    Backup Designated Router:  10.70.110.3
    Authentication Type:  None
    MTU Ignore:  Yes
    Advertise When Down:  No
    Metric Value:  10
```

7011:

```
Interface:  10.70.1.2
    Area ID:  0.0.0.0
    Admin State:  Enabled
    Type:  Passive
    Priority:  1
    Designated Router:  10.70.1.2
    Backup Designated Router:  0.0.0.0
    Authentication Type:  None
    MTU Ignore:  Yes
    Advertise When Down:  No
    Metric Value:  10
Interface:  10.70.100.3
    Area ID:  0.0.0.0
    Admin State:  Enabled
    Type:  Passive
```

```
    Priority:  200
    Designated Router:  10.70.100.3
    Backup Designated Router:  0.0.0.0
    Authentication Type:  None
    MTU Ignore:  Yes
    Advertise When Down:  No
    Metric Value:  10
Interface:  10.70.110.2
    Area ID:  0.0.0.0
    Admin State:  Enabled
    Type:  Broadcast
    Priority:  150
    Designated Router:  10.70.110.2
    Backup Designated Router:  10.70.110.3
    Authentication Type:  None
    MTU Ignore:  Yes
    Advertise When Down:  No
    Metric Value:  10
```

Step 2– Verify OSPF neighbors

```
show ip ospf neighbor
```

Results:

7010:

```
Interface       Nbr Router ID   Nbr IP Address  Pri State     RetransQLen Perm
--------------- --------------- --------------- --- --------- ----------- ----
10.70.110.1     10.70.1.2       10.70.110.2     150 Full      0           Dyn
10.70.110.1     10.70.1.3       10.70.110.3     1   Full      0           Dyn

Total OSPF Neighbors:  2
```

7011:

```
Interface       Nbr Router ID   Nbr IP Address  Pri State     RetransQLen Perm
--------------- --------------- --------------- --- --------- ----------- ----
10.70.110.2     10.70.1.1       10.70.110.1     200 Full      0           Dyn
10.70.110.2     10.70.1.3       10.70.110.3     1   Full      0           Dyn

Total OSPF Neighbors:  2
```

2.12.4.4 Verify IP Routes

Step 1 – Verify IP routes

show ip ospf interface enabled

Results:

7010:

```
================================================================================
                                Ip Route
================================================================================
DST             MASK            NEXT            COST  VLAN PORT PROT TYPE PREF
--------------------------------------------------------------------------------
10.5.40.0       255.255.255.0   10.70.110.3     20    1100 24      O  IB    20
10.70.1.1       255.255.255.255 10.70.1.1       1     0    ----    C  DB    0
10.70.1.2       255.255.255.255 10.70.110.2     20    1100 T#1     O  IB    20
10.70.1.3       255.255.255.255 10.70.110.3     20    1100 24      O  IB    20
10.70.2.0       255.255.255.252 10.70.2.1       1     2    ----    C  DB    0
10.70.100.0     255.255.255.0   10.70.100.2     1     1000 ----    C  DB    0
10.70.110.0     255.255.255.0   10.70.110.1     1     1100 ----    C  DB    0
```

7011:

```
================================================================================
                                Ip Route
================================================================================
DST             MASK            NEXT            COST  VLAN PORT PROT TYPE PREF
--------------------------------------------------------------------------------
10.5.40.0       255.255.255.0   10.70.110.3     20    1100 24      O  IB    20
10.70.1.1       255.255.255.255 10.70.110.1     20    1100 T#1     O  IB    20
10.70.1.2       255.255.255.255 10.70.1.2       1     0    ----    C  DB    0
10.70.1.3       255.255.255.255 10.70.110.3     20    1100 24      O  IB    20
10.70.2.0       255.255.255.252 10.70.2.2       1     2    ----    C  DB    0
10.70.100.0     255.255.255.0   10.70.100.3     1     1000 ----    C  DB    0
10.70.110.0     255.255.255.0   10.70.110.2     1     1100 ----    C  DB    0
```

3. Configuring SMLT – Square and Full Mesh Topology Examples

3.1 Configuration – ERS 8600/8800 Layer 2 Square SMLT with Cisco at Edge Using EtherChannel

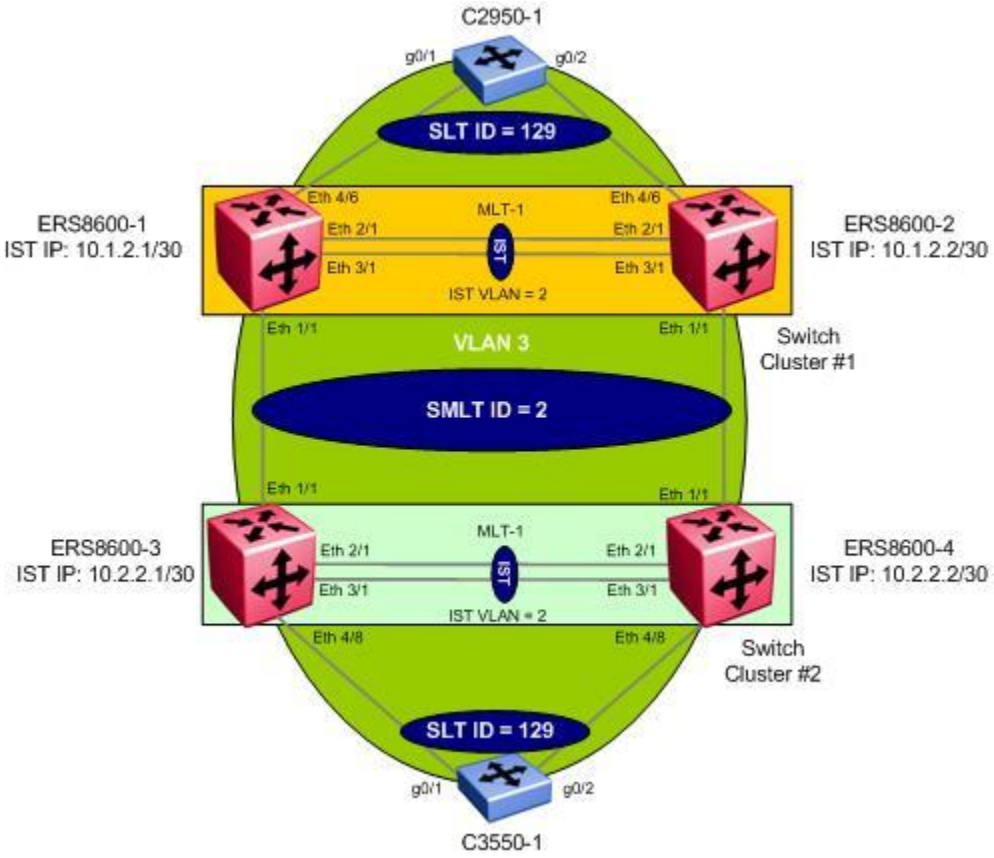


Figure 15: Square SMLT Configuration

The Square SMLT configuration procedure is repeating the triangle configuration steps twice. The Full Mesh SMLT configuration is the same as the square configuration with the addition of adding connections between the Switch Clusters – e.g. 8000-1 to 8600-3 and 8000-2 to 8600-4.

The main rule for a square configuration is that the IST pairs, Switch Cluster #1 and Switch Cluster #2, each must have matching SMLT IDs. The SMLT IDs can be different between the two SMLT Clusters as they only have local significance within the cluster. For example, we could use SMLT ID = 2 with port member 1/1 in Switch Cluster #1 and use SMLT ID = 15 with port member 1/1 in Switch Cluster #2. However, this is not recommended as it is best to use the same SMLT ID for ease of configuration and trouble-shooting problems.

In regards to SLPP, as this is a bridged network end-to-end, it is recommended to use a SLPP Packet Receive Threshold of 300 on the primary switches core ports connecting the two SMLT clusters. In our example, this is in reference to port 1/1 on switches 8000-1 and 8000-2.

For this configuration example, Cisco switches are used at the SMLT access layer using EtherChannel to connect to the SMLT Cluster. Please note that any local proprietary load-balance mechanism or 802.3ad can be used to connect to an SMLT Cluster.

It is recommended to use the same SMLT ID's between the two SMLT clusters for ease in configuration and trouble-shooting.

It is recommended to use a unique IP subnet between the SMLT Cluster.

As illustrated in the diagram above, the SMLT or SLT ID is local to an SMLT Cluster. Hence the reason we are using SLT-129 in both Switch Cluster #1 and Switch Cluster #2. Please not that this is not a requirement; it just illustrates the flexibility of the solution.

3.1.1 Switch Cluster

3.1.1.1 Create VLANs

The following port based VLANs will be configured on the SMLT Switch cluster

- VLAN 2 to be used by the Inter Switch Trunk (IST)
- VLAN 3 to be used at a Layer 2 level to C2950-1 and C3550-2 for connecting users.

ERS 8000 SMLT Cluster: Create VLAN 2 and 3

8000-1, 8000-2, 8000-3 & 8000-4: Same configuration on all switches

```
8000-1:5# config vlan 2 create byport 1 name IST
8000-1:5# config vlan 3 create byport 1 name Services
```

3.1.1.2 Change fdb aging timer for VLAN 3

ERS 8000 SMLT Cluster: Change fdb aging timer for VLAN 3

8000-1, 8000-2, 8000-3 & 8000-4: Same configuration on all switches

```
8000-1:5# config vlan 3 fdb-entry aging-time 21601
```

3.1.1.3 Create IST

Multilink Trunking 1 (MLT 1) will be used for the IST with port members 2/1 and 3/1. 802.1Q tagging will be enabled on all IST port members and Spanning Tree will be disabled on all IST port members by default. VLACP will be enabled on the IST trunk.

It is recommended to use the reserved multicast MAC address of 01:80:c2:00:00:0f for the VLACP MAC address.

ERS 8000 SMLT Cluster: Step 1 – Create MLT 1 for IST

8000-1, 8000-2, 8000-3 & 8000-4: Same configuration on all switches

```
8000-1:5# config mlt 1 create
8000-1:5# config mlt 1 name IST
8000-1:5# config mlt 1 add port 2/1,3/1
8000-1:5# config vlan 2 add-mlt 1
```

ERS 8000 SMLT Cluster: Step 2 – Create IST

8000-1:

```
8000-1:5# config vlan 2 ip create 10.1.2.1/30
8000-1:5# config mlt 1 ist create ip 10.1.2.2 vlan-id 2
8000-1:5# config mlt 1 ist enable
```

8000-2:

```
8000-2:5# config vlan 2 ip create 10.1.2.2/30
8000-2:5# config mlt 1 ist create ip 10.1.2.1 vlan-id 2
8000-2:5# config mlt 1 ist enable
```

8000-3:

```
8000-3:5# config vlan 2 ip create 10.2.2.1/30
8000-3:5# config mlt 1 ist create ip 10.2.2.2 vlan-id 2
8000-3:5# config mlt 1 ist enable
```

8000-4:

```
8000-4:5# config vlan 2 ip create 10.2.2.2/30
8000-4:5# config mlt 1 ist create ip 10.2.2.1 vlan-id 2
8000-4:5# config mlt 1 ist enable
```

ERS 8000 SMLT Cluster: Step 3 – Enable VLACP

8000-1, 8000-2, 8000-3 & 8000-4: Same configuration on all switches

```
8000-1:5# ethernet 2/1,3/1 vlacp macaddress 01:80:c2:00:00:0f
```

```
8000-1:5# ethernet 2/1,3/1 vlacp slow-periodic-time 10000
8000-1:5# ethernet 2/1,3/1 vlacp enable
8000-1:5# config vlacp enable
```

3.1.1.4 SMLT-2

ERS 8000 SMLT Cluster: Create SMLT-2

8000-1, 8000-2, 8000-3 & 8000-4: Same configuration on all switches

```
8000-1:5# config mlt 2 create
8000-1:5# config mlt 2 name CORE
8000-1:5# config mlt 2 perform-tagging enable
8000-1:5# config mlt 2 add port 1/1
8000-1:5# config vlan 2 add-mlt 2
8000-1:5# config mlt 2 smlt create smlt-id 2
```

Please note that although we used the same SMLT ID in the core for SMLT cluster 1 and 2, it is not a requirement. The SMLT and IST ID's are local to each SMLT cluster. In the core, it is best practice to use the same SMLT ID's for ease of configuration and trouble-shooting purposes.

3.1.1.5 Add VLAN 3 to IST

ERS 8000 SMLT Cluster: Add VLAN 3 to IST MLT

8000-1, 8000-2, 8000-3 & 8000-4: Same configuration on all switches

```
8000-1:5# config vlan 3 add-mlt 1
```

3.1.1.6 SLT-129 to C2950-1

ERS 8000 SMLT Cluster: Create SLT-129

8000-1, 8000-2: Same configuration on all switches

```
8000-1:5# config ethernet 4/6 perform-tagging enable
8000-1:5# config vlan 1 ports remove 4/6
8000-1:5# config vlan 3 ports add 4/6
8000-1:5# config ethernet 4/6 smlt 129 create
```

3.1.1.7 SLT-129 to C3550-1

ERS 8000 SMLT Cluster: Create SLT-129

8000-3, 8000-4: Same configuration on all switches

```
8000-3:5# config ethernet 4/8 perform-tagging enable
8000-3:5# config vlan 1 ports remove 4/8
```

```
8000-3:5# config vlan 3 ports add 4/8
8000-3:5# config ethernet 4/8 smlt 129 create
```

3.1.1.8 CP Limit – SMLT port members

CP Limit will be enabled on all the SMLT Access port members. For this example, we will select the moderate recommendations for CP-Limit.

ERS 8000 SMLT Cluster: CP Limit for SMLT Access ports

8000-1, 8000-2: Same configuration on both switches

```
8000-1:5# config ethernet 4/6 cp-limit enable multicast-limit 2500 broadcast-limit 2500
8000-1:5# config ethernet 1/1 cp-limit enable multicast-limit 5000 broadcast-limit 5000
```

8000-3 & 8000-4: Same configuration on both switches

```
8000-3:5# config ethernet 4/8 cp-limit enable multicast-limit 2500 broadcast-limit 2500
8000-3:5# config ethernet 1/1 cp-limit enable multicast-limit 5000 broadcast-limit 5000
```

3.1.1.9 SLPP

For this example, we will pick 8000-1 as the primary switch for switch cluster 1 and 8000-3 as primary for switch cluster 2. SLPP will be enabled globally and on the SMLT access ports 4/6 on switch cluster 1 and 4/8 on switch cluster 2 and on core port member 1/1 on both cluster 1 and cluster 2. On the SMLT primary switch, we will set the SLPP packet-rx-threshold to 5 while on the SMLT secondary switch, we will set the SLPP packet-rx-threshold to 50 for the access ports. As this is a bridged network end-to-end, on the SMLT primary switch only, we will set the SLPP packet-rx-threshold to 300 for the core ports

SLPP should only be enabled on the SMLT access or core ports and not on the IST port members.

ERS 8000 SMLT Cluster: Enable SLPP and in regards to the core port on the primary switch only, set the SLPP Rx-Threshold with a value of 300

8000-1:

```
8000-1:5# config slpp add 3
8000-1:5# config slpp operation enable
8000-1:5# config ethernet 1/1,4/6 slpp packet-rx enable
8000-1:5# config ethernet 4/6 slpp packet-rx-threshold 5
8000-1:5# config ethernet 1/1 slpp packet-rx-threshold 300
```

8000-2:

```
8000-2:5# config slpp add 3
```

```
8000-2:5# config slpp operation enable
8000-2:5# ethernet 4/6 slpp packet-rx enable
8000-2:5# ethernet 4/6 slpp packet-rx-threshold 50
```

8000-3:

```
8000-3:5# config slpp add 3
8000-3:5# config slpp operation enable
8000-3:5# config ethernet 1/1,4/8 slpp packet-rx enable
8000-3:5# config ethernet 4/8 slpp packet-rx-threshold 5
8000-3:5# config ethernet 1/1 slpp packet-rx-threshold 300
```

8000-4:

```
8000-4:5# config slpp add 3
8000-4:5# config slpp operation enable
8000-4:5# ethernet 4/8 slpp packet-rx enable
8000-4:5# ethernet 4/8 slpp packet-rx-threshold 50
```

3.1.1.10 VLACP – SMLT Core

We will enable VLACP and use the short timeout option with a timeout setting of 500ms on the SMLT core port 1/1.

ERS 8000 SMLT Cluster: Enable VLACP

8000-1, 8000-2, 8000-3 & 8000-4: Same configuration on all switches

```
8000-1:5# config ethernet 1/1 vlacp fast-periodic-time 500
8000-1:5# config ethernet 1/1 vlacp timeout short
8000-1:5# config ethernet 1/1 vlacp timeout-scale 5
8000-1:5# config ethernet 1/1 vlacp macaddress 01:80:c2:00:00:0f
8000-1:5# config ethernet 1/1 vlacp enable
```

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

3.1.1.11 Ext-CP Limit

Ext-CP Limit will be enable globally and on the SMLT access ports in the SMLT switch cluster. The SoftDown option will be used with the bandwidth utilization threshold set to 10%.

ERS 8000 SMLT Cluster: Enable EXT-CP-Limit

8000-1, 8000-2: Same configuration on both switches

```
8000-1:5# config sys ext-cp-limit extcplimit enable
8000-1:5# config sys ext-cp-limit max-ports-to-check 5
8000-1:5# config sys ext-cp-limit trap-level Normal
8000-1:5# config ethernet 4/6 ext-cp-limit SoftDown threshold-util-rate 10
```

8000-3 & 8000-4: Same configuration on both switches

```
8000-3:5# config sys ext-cp-limit extcplimit enable
8000-3:5# config sys ext-cp-limit max-ports-to-check 5
8000-3:5# config sys ext-cp-limit trap-level Normal
8000-3:5# config ethernet 4/8 ext-cp-limit SoftDown threshold-util-rate 10
```

3.1.1.12 Discard Untagged Frames

It is recommended to enable discard untagged frames on all IST and SMLT ports.

ERS 8000 SMLT Cluster: Enable Discard Untagged Frames

8000-1, 8000-2: Same configuration on both switches

```
8000-1:5# config ethernet 2/1,3/1,4/6 untagged-frames-discard enable
```

8000-3 & 8000-4: Same configuration on both switches

```
8000-3:5# config ethernet 2/1,3/1,3/13,4/8 untagged-frames-discard enable
```

3.1.2 Configuration - Edge Switch

3.1.2.1 C3550

Note: Spanning Tree, PVST+, is enabled by default on a Cisco switch. Spanning Tree should be left enabled on all user ports and set for portfast, but disabled on the trunk EtherChannel ports. This can be accomplished on the Port-channel ports using the command ‘spanning-tree bpdufilter enable’ command.

```
!
spanning-tree mode pvst
spanning-tree extend system-id
no spanning-tree vlan 3
!
vlan dot1q tag native
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3
 switchport mode trunk
 spanning-tree bpdufilter enable
!
interface FastEthernet0/3
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/4
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3
 switchport mode trunk
 channel-group 1 mode on
!
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3
 switchport mode trunk
 channel-group 1 mode on
!
```

3.1.2.2 C2950

```
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
interface Port-channel1
 switchport trunk allowed vlan 3
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 3
 switchport mode access
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 3
 switchport mode trunk
 channel-group 1 mode on
!
interface GigabitEthernet0/2
 switchport trunk allowed vlan 3
 switchport mode trunk
 channel-group 1 mode on
!
```

3.2 Configuration – VSP 7000 OSPF Routed SMLT in SMLT Square Core

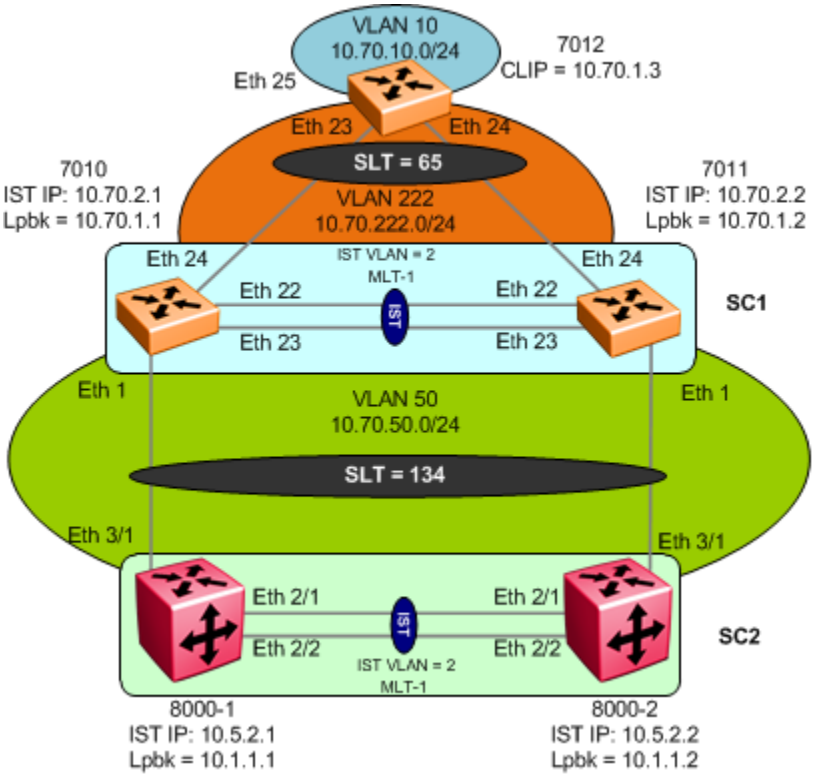


Figure 16: VSP 7000 OSPF SMLT Square

The following example is based on a square SMLT core using OSPF between a VSP 7000 SMLT cluster and ERS 8800 SMLT cluster. For simplicity, we will use OSPF area 0. Please note that RSMLT will only be provisioned on the ERS 8800 SMLT cluster as it is not supported on the VSP 7000.

In reference to the diagram above, we will configure the following:

- Overall, this configuration example will cover the configuration steps required for 7010, 7011, 8000-1, and 8000-2.
- Via Switch Cluster #1, we will configure
  - VLAN 2 for the IST VLAN using MLT ID = 1
  - IST IP subnet = 10.70.2.0/30
  - VLAN 50 for the core VLANs using SLT ID = 134
  - VLAN 222 for the edge VLAN using SLT ID = 65
  - OSPF as the IGP using area 0
  - Enable VLACP using recommended reserved MAC
  - Using the loopback address as the OSPF router ID
  - Enable SLPP on the core VLAN with a SLPP Packet Receive threshold of 5 on 7010 assuming 7010 is the primary switch and a threshold of 50 on 7011 assuming it is the secondary switch

- Via Switch Cluster #2, we will configure
  - ERS 8800 configured in ACLI mode
  - VLAN 2 for the IST VLAN using MLT ID = 1
  - IST IP subnet = 10.5.2.0/30
  - VLAN 50 for the core VLAN using SLT ID =134
  - OSPF as the IGP using area 0
  - 8000-1 (DR) OSPF priority to 100 for VLAN 50
  - 8000-2 (BDR) OSPF priority to 150 for VLAN 50
  - Enable VLACP using recommended reserved MAC
  - Using the loopback address as the OSPF router ID
  - Enable SLPP on the core VLAN with a SLPP Packet Receive threshold of 5 on 8000-1 assuming 8000-1 is the primary switch and a threshold of 50 on 8000-2 assuming it is the secondary switch

3.2.1.1 Configuration Mode

Go to configuration mode

```
config terminal
```

3.2.1.2 Change Spanning Tree mode to MSTP

We will change the Spanning Tree mode to MSTP. This is the default setting on the VSP 4000 and VSP 9000. When using tools such as VLAN Manager in COM, it is recommended to change the Spanning Tree mode to MSTP.

VSP 7000 Option – change spanning mode to MSTP on switches 7010 and 7011

VSP 7000:

```
spanning-tree mode mst
New operational mode MSTP will take effect upon reset
7024XLS(config)#boot
Reboot the unit(s) (y/n) ? y Rebooting . . .
--------------------------------------------------------------------------------
show spanning-tree mode
```

ERS 8800:

```
boot config flags spanning-tree-mode mstp
Warning: Please save boot configuration and reboot the switch
         for this to take effect.
Warning: Please carefully save your configuration files before
         starting configuring the switch in RSTP or MSTP mode.
```

```
        The syntax used to create VLANs in any of these new
        modes is NOT COMPATIBLE with the default mode (STP)
save boot
boot -y
```

3.2.1.3 System Name

SMLT Cluster switches - Configure system name

VSP 7000

```
snmp-server name <7010|7011>
```

ERS 8800

```
prompt <8000-1|8000-2>
```

3.2.1.4 Create VLANs

The following port based VLANs will be configured on the SMLT Switch cluster

- VLAN 2 to be used by the Inter Switch Trunk (IST)
- VLAN 50 to be used in the core level to 7010, 7011, 8000-1, and 8000-2.

SMLT Cluster: Create VLANs

7010 & 7011: Same configuration both switches

```
7010(config)#vlan create 2 name IST_vlan2 type port
7010(config)#vlan create 50 name core_vlan50 type port
7010(config)#vlan create 222 type port
```

8000-1 & 8000-2: Same configuration on both switches

```
8000-1:5(config)#vlan create 2 name IST_vlan2 type port-mstprstp 0
8000-1:5(config)#vlan create 50 name core_vlan50 type port-mstprstp 0
```

3.2.1.5 IST Configuration

SMLT Cluster: Step 1 - Create MLT 1 for IST

7010 & 7011: Same configuration both switches

```
7010(config)#vlan ports 22-23 tagging tagall
7010(config)#mlt 1 name IST enable member 22-23 learning disable
7010(config)#vlan members add 2 22-23
7010(config)#vlan members remove 1 22-23
```

8000-1 & 8000-2: Same configuration both switches

```
8000-1:5(config)#mlt 1 enable name IST
8000-1:5(config)#mlt 1 member 2/1-2/2
8000-1:5(config)#mlt 1 encapsulation dot1q
8000-1:5(config)#vlan mlt 2 1
8000-1:5(config)#vlan members remove 1 2/1-2/2
8000-1:5(config)#interface gigabitEthernet 2/1-2/2
8000-1:5(config-if)#untagged-frames-discard
8000-1:5(config-if)#exit
```

SMLT Cluster: Step 2 - Create IST

7010:

```
7010(config)#interface vlan 2
7010(config-if)#ip address 10.50.2.1 255.255.255.252
7010(config-if)#exit
7010(config)#interface mlt 1
7010(config-mlt)#ist peer-ip 10.20.2.2 vlan 2
7010(config-mlt)#ist enable
7010(config-mlt)#exit
```

7011:

```
7011(config)#interface vlan 2
7011(config-if)#ip address 10.70.2.2 255.255.255.252
7011(config-if)#exit
7011(config)#interface mlt 1
7011(config-mlt)#ist peer-ip 10.70.2.1 vlan 2
7011(config-mlt)#ist enable
7011(config-mlt)#exit
```

8000-1:

```
8000-1:5(config)#interface Vlan 2
8000-1:5(config-if)#ip address 10.5.2.1 255.255.255.252 3
8000-1:5(config-if)#exit
8000-1:5(config)#interface mlt 1
8000-1:5(config-mlt)#ist peer-ip 10.5.2.2 vlan 2
8000-1:5(config-mlt)#ist enable
8000-1:5(config-mlt)#exit
```

8000-2:

```
8000-2:5(config)#interface Vlan 2
8000-2:5(config-if)#ip address 10.5.2.2 255.255.255.252 3
8000-2:5(config-if)#exit

8000-1:5(config)#interface mlt 1
8000-1:5(config-mlt)#ist peer-ip 10.5.2.1 vlan 2
8000-1:5(config-mlt)#ist enable
8000-1:5(config-mlt)#exit
```

SMLT Cluster: Step 3 - Enable VLACP and discard untagged frames

7010 & 7011: Same configuration both switches

```
7010(config)#vlan ports 22-23 filter-untagged-frame enable
7010(config)#interface fastEthernet 22-23
7010(config-if)#vlacp slow-periodic-time 10000
7010(config-if)#vlacp enable
7010(config-if)#exit
7010(config)#vlacp macaddress 01:80:c2:00:00:0f
7010(config)#vlacp enable
```

8000-1 & 8000-2: Same configuration on both switches

```
8000-1:5(config)#interface GigabitEthernet 2/1-2/2
8000-1:5(config-if)#untagged-frames-discard
8000-1:5(config-if)#vlacp slow-periodic-time 10000 timeout-scale 5 funcmac-addr
01:80:c2:00:00:0f
8000-1:5(config-if)#vlacp enable
8000-1:5(config-if)#exit
8000-1:5(config)#vlacp enable
```

3.2.1.6 SLT 134 - Core between VSP 7000 SMLT Cluster and ERS 8800 SMLT Cluster

SMLT Cluster – Step 1: Add core SLT 134 and add VLAN 50 port members

7010 & 7011: Same configuration on both switches

```
7010(config)#vlan configcontrol automatic
7010(config)#vlan ports 1 tagging tagall
7010(config)#interface fastEthernet 1
7010(config-if)#smlt 134
7010(config-if)#exit
7010(config)#vlan members add 50 1,22-23
7010(config)#vlan members remove 1 1
```

8000-1 & 8000-2: Same configuration on both switches

```
8000-1:5(config)#vlan ports 3/1 tagging tagAll
8000-1:5(config)#vlan members add 50 3/1
8000-1:5(config)#vlan members remove 1 3/1
8000-1:5(config)#interface gigabitEthernet 3/1
8000-1:5(config-if)#smlt 134
8000-1:5(config-if)#exit
8000-1:5(config)#vlan mlt 50 1
```

3.2.1.7 SLT 65 to edge switch 7012

SMLT Cluster: Create SLT 33 and add VLAN 222 port members

7010 & 7011: Same configuration on both switches

```
7010(config)#vlan ports 24 tagging tagall
7010(config)#interface fastEthernet 24
7010(config-if)#smlt 65
7010(config-if)#exit
7010(config)#vlan members add 222 22-24
7010(config)#vlan members remove 1 24
```

3.2.1.8 Loopback Address

By default, the VSP 7000 and ERS 8600/8800 automatically adds an OSPF router-id. For trouble-shooting proposes, you may wish to set the OSPF router-id.

For this configuration example, assuming no exiting circuitless-ip address have already been configured, we will configure the following

- use loopback ID 1 with the following IP addresses
  - 7010 : 10.70.1.1/32
  - 7011 : 10.70.1.2/32
  - 8000-1 : 10.1.1.1/32
  - 8000-2 : 10.1.1.2/32
- Enable OSPF on loopback 1

Although you can use any mask with a Circuitless-IP address, it is recommended to use a 32-bit IP subnet mask.

Please note that by default, the loopback address uses OSPF area 0.

SMLT Cluster: Create CLIP 1 and enable OSPF

7010:

```
7010(config)#interface loopback 1
7010(config-if)#ip address 10.70.1.1 255.255.255.255
7010(config-if)#ip ospf
7010(config-if)#exit
```

7011:

```
7011(config)#interface loopback 1
7011(config-if)#ip address 10.70.1.2 255.255.255.255
7011(config-if)#ip ospf
7011(config-if)#exit
```

8000-1:

```
8000-1:5(config)#interface loopback 1
8000-1:5(config-if)#ip address 1 10.1.1.1/32
8000-1:5(config-if)#ip ospf 1
8000-1:5(config-if)#exit
```

8000-2:

```
8000-2:5(config)#interface loopback 1
8000-2:5(config-if)#ip address 1 10.1.1.2/32
8000-2:5(config-if)#ip ospf 1
8000-2:5(config-if)#exit
```

3.2.1.9 Add IP address to VLAN 50 and 222

SMLT Cluster: Add IP address to VLAN 3

7010:

```
7010(config)#interface vlan 50
7010(config-if)#ip address 10.50.50.1 255.255.255.0
7010(config-if)#exit
7010(config)#interface vlan 222
7010(config-if)#ip address 10.70.222.1 255.255.255.0
7010(config-if)#exit
```

7011:

```
7011(config)#interface vlan 50
7011(config-if)#ip address 10.50.50.2 255.255.255.0
7011(config-if)#exit
7011(config)#interface vlan 222
```

```
7011(config-if)#ip address 10.70.222.2 255.255.255.0
7011(config-if)#exit
```

8000-1:

```
8000-1:5(config)#interface vlan 50
8000-1:5(config-if)#ip address 10.50.50.3 255.255.255.0
8000-1:5(config-if)#ip ospf 1
8000-1:5(config-if)#exit
```

8000-2:

```
8000-2:5(config)#interface vlan 50
8000-2:5(config-if)#ip address 10.50.50.4 255.255.255.0
8000-2:5(config-if)#ip ospf 1
8000-2:5(config-if)#exit
```

3.2.1.10 Enable OSPF

VLAN 50 will be configured with OSPF on the SMLT Switch cluster. For this example, we will make 8000-1 the OSPF DR for VLAN 50 and make 8000-2 the BDR for VLAN 50.

SMLT Cluster: Enable OSPF for VLAN 3, make VSP-1 the DR, VSP-2 the BDR, and enable OSPF globally

7010:

```
7010(config)#interface vlan 50
7010(config-if)#ip ospf priority 0
7010(config-if)#ip ospf enable
7010(config-if)#exit
7010(config)#interface vlan 222
7010(config-if)#ip ospf enable
7010(config-if)#exit
7010(config)#router ospf
7010(config-router)#router-id 10.70.1.1
7010(config-router)#exit
7010(config)#router ospf enable
```

7011: Same configuration as 7010 except for the OSPF router-id

```
7011(config)#router ospf
7011(config-router)#router-id 10.70.1.2
```

8000-1:

```
8000-1:5(config)#interface vlan 50
```

```
8000-1:5(config-if)#ip ospf priority 150
8000-1:5(config-if)#ip ospf enable
8000-1:5(config-if)#exit
8000-1:5(config)#router ospf
8000-1:5(config-ospf)#router-id 10.1.1.1
8000-1:5(config-ospf)#exit
8000-1:5(config)#router ospf enable
```

8000-2:

```
8000-2:5(config)#interface vlan 50
8000-2:5(config-if)#ip ospf priority 200
8000-2:5(config-if)#ip ospf enable
8000-2:5(config-if)#exit
8000-2:5(config)#router ospf
8000-2:5(config-ospf)#router-id 10.1.1.2
8000-2:5(config-ospf)#exit
8000-2:5(config)#router ospf enable
```

3.2.1.11 Enable RSMLT

VLAN 3 with RSMLT using default timers

SMLT Cluster: Enable RSMLT

8000-1 & 8000-2: Same configuration both switches

```
8000-1:5(config)#interface vlan 50
8000-1:5(config-if)#ip rsmlt
8000-1:5(config-if)#exit
```

3.2.1.12 CP Limit – SMLT port members

CP Limit will be enabled on all the SMLT core port members. For this example, we will select the moderate recommendations for CP-Limit.

SMLT Cluster: CP Limit

8000-1 & 8000-2: Same configuration both switches

```
8000-1:5(config)#interface GigabitEthernet 3/1
8000-1:5(config-if)#cp-limit multicast 9000 broadcast 9000
8000-1:5(config-if)#exit
```

3.2.1.13 SLPP

SLPP will be enabled globally and on the SMLT access ports and core port members. In this example, we only show the configuration for the core ports. On the SMLT primary switch, we will set the SLPP packet-rx-threshold to 5 while on the SMLT secondary switch, we will set the SLPP packet-rx-threshold to 50 for the core ports.

SLPP should only be enabled on the SMLT access or core ports and not on the IST port members.

SMLT Cluster: Enable SLPP

7010:

```
7010(config)#slpp enable
7010(config)#slpp vid 50,222
7010(config)#interface fastEthernet 1,24
7010(config-if)#slpp packet-rx-threshold 5
7010(config-if)#slpp enable
7010(config-if)#exit
```

7011: Same configuration as 7001 except for the SLPP packet receive threshold

```
7011(config-if)#slpp packet-rx-threshold 50
```

8000-1:

```
8000-1:5(config)#slpp enable
8000-1:5(config)#slpp vid 50
8000-1:5(config)#interface gigabitEthernet 3/1
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: Same configuration as 8000-1 except for the SLPP packet receive threshold

```
8000-2:5(config-if)#slpp packet-rx-threshold 50
```

3.2.1.14 VLACP

We will enable VLACP in the core using VLACP short timers and with the recommended reserved MAC.

SMLT Cluster: Enable VLACP

7010 & 7011: Same configuration both switches

```
7010(config)#interface fastEthernet 1,24
7010(config-if)#vlacp timeout short
7010(config-if)#vlacp timeout-scale 5
```

```
7010(config-if)#vlacp enable
7010(config-if)#exit
```

8000-1 & 8000-2: Same configuration on both switches

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

3.2.1.15 Discard Untagged Frames

It is recommended to enable discard untagged frames on all IST and SMLT ports.

SMLT Cluster: Enable Discard Untagged Frames

7010 & 7011: Same configuration both switches

```
7010(config)#vlan ports 1,22-24 filter-untagged-frame enable
```

8000-1 & 8000-2: Same configuration on both switches

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

3.2.2 Configuration - Edge Switch

3.2.2.1 Configuration Mode

Go to configuration mode

```
config terminal
```

3.2.2.2 Change Spanning Tree mode to MSTP

VSP 7000 Option – change spanning mode to MSTP on switch 7012

```
spanning-tree mode mst
New operational mode MSTP will take effect upon reset
7024XLS(config)#boot
Reboot the unit(s) (y/n) ? y
Rebooting . . .
```

3.2.2.3 Create VLANs 10 and 222

7012: Create VLAN 10 and 222 and add VLAN 10 port members

```
7012(config)#vlan create 222 type port
7012(config)#vlan create 10 type port
7012(config)#vlan configcontrol automatic
7012(config)# vlan members add 10 25
```

3.2.2.4 Add MLT

7012: Create MLT 1 and add port members

```
7012(config)#vlan ports 23-24 tag tagall
7012(config)#mlt 1 enable member 23-24 learning disable
7012(config)#vlan members add 222 23-24
7012(config)#vlan members remove 1 23-24
```

3.2.2.5 Add IP addresses

7012: Step 1 – Add IP address to VLAN 10

```
7012(config)#interface vlan 10
7012(config-if)#ip address 10.70.10.1 255.255.255.0
7012(config-if)#exit
```

7012: Step 2 – Add IP address to VLAN 222

```
7012(config)#interface vlan 222
7012(config-if)#ip address 10.70.222.3 255.255.255.0
7012(config-if)#exit
```

3.2.2.6 Loopback Address

7012: Create CLIP 1 and enable OSPF

```
7012(config)#interface loopback 1
7012(config-if)#ip address 10.70.1.3 255.255.255.255
7012(config-if)#ip ospf
7012(config-if)#exit
```

3.2.2.7 Enable OSPF

Enable OSPF on VLANs 10 and 222. VLAN 10 will be configured with OSPF passive interface.

7012: Step 1 – Enable OSPF to VLAN 10 with passive interface

```
7012(config)#interface vlan 10
7012(config-if)#ip ospf network passive
7012(config-if)#ip ospf enable
7012(config-if)#exit
```

7012: Step 2 – Enable OSPF to VLAN 222

```
7012(config)#interface vlan 222
7012(config-if)#ip ospf priority 0
7012(config-if)#ip ospf enable
7012(config-if)#exit
```

7012: Step 4 – Enable OSPF globally

```
7012(config)#router ospf
7012(config-router)#router-id 10.70.1.3
7012(config-router)#exit
7012(config)#router ospf enable
```

3.2.2.8 VLACP

We will enable VLACP in the core using VLACP short timers and with the recommended reserved MAC.

7012: Enable VLACP

```
7012(config)#interface fastEthernet 23-24
7012(config-if)#vlacp timeout short
7012(config-if)#vlacp timeout-scale 5
7012(config-if)#vlacp enable
7012(config-if)#exit
7012(config)#vlacp macaddress 01:80:c2:00:00:0f
7012(config)#vlacp enable
```

3.2.2.9 Discard Untagged Frames

It is recommended to enable discard untagged frames on all ports to an SMLT cluster.

7012: Enable Discard Untagged Frames

```
7012(config)#vlan ports 23-24 filter-untagged-frame enable
```

3.2.3 Configuration File

7010	7011
enable configure terminal ! ! *** SNMP *** ! snmp-server name "7010" ! ! *** MSTP (Phase 1) *** ! spanning-tree mode mst ! ! *** VLAN *** ! vlan create 2,50,222 type port cist vlan name 2 "IST" vlan name 50 "core_vlan50" vlan ports 1,22-24 tagging tagAll filter-untagged-frame enable vlan configcontrol flexible vlan members 2 22-23 vlan members 50 1,22-23 vlan members 222 22-24 vlan configcontrol automatic ! ! *** MLT (Phase 1) *** ! mlt 1 name "IST" enable member 22-23 ! ! *** L3 *** ! ! ip routing force ! interface vlan 2 ip address 10.70.2.1 255.255.255.252 2 exit interface vlan 50 ip address 10.70.50.1 255.255.255.0 4	enable configure terminal ! ! *** SNMP *** ! snmp-server name "7011" ! ! *** MSTP (Phase 1) *** ! spanning-tree mode mst ! ! *** VLAN *** ! vlan create 2,50,222 type port cist vlan name 2 "IST" vlan name 50 "core_vlan50" vlan ports 1,22-24 tagging tagAll filter-untagged-frame enable vlan configcontrol flexible vlan members 2 22-23 vlan members 50 1,22-23 vlan members 222 22-24 vlan configcontrol automatic ! ! *** MLT (Phase 1) *** ! mlt 1 name "IST" enable member 22-23 ! ! *** L3 *** ! ! ip routing force ! interface vlan 2 ip address 10.70.2.2 255.255.255.252 2 exit interface vlan 50 ip address 10.70.50.2 255.255.255.0 4

```
exit
interface vlan 222
ip address 10.70.222.1 255.255.255.0 6
exit
interface loopback 1
ip address 10.70.1.1 255.255.255.255
exit
!
! *** VLACP ***
!
vlacp enable
vlacp macaddress 180.c200.f
interface FastEthernet ALL
vlacp port 22-23 slow-periodic-time 10000
vlacp port 1,24 timeout short
vlacp port 1,24 timeout-scale 5
vlacp port 1,22-24 enable
exit
!
! *** L3 Protocols ***
!
! --- OSPF ---

router ospf enable
router ospf
router-id 10.70.1.1
exit
interface vlan 50
ip ospf priority 0
ip ospf enable
exit
interface vlan 222
ip ospf enable
exit
interface loopback 1
ip ospf
exit
!
! *** SMLT ***
!
interface mlt 1
```

```
exit
interface vlan 222
ip address 10.70.222.2 255.255.255.0 6
exit
interface loopback 1
ip address 10.70.1.2 255.255.255.255
exit
!
! *** VLACP ***
!
vlacp enable
vlacp macaddress 180.c200.f
interface FastEthernet ALL
vlacp port 22-23 slow-periodic-time 10000
vlacp port 1,24 timeout short
vlacp port 1,24 timeout-scale 5
vlacp port 1,22-24 enable
exit
!
! *** L3 Protocols ***
!
! --- OSPF ---

router ospf enable
router ospf
router-id 10.70.1.2
exit
interface vlan 50
ip ospf priority 0
ip ospf enable
exit
interface vlan 222
ip ospf enable
exit
interface loopback 1
ip ospf
exit
!
! *** SMLT ***
!
interface mlt 1
```

ist peer-ip 10.70.2.2 ist vlan 2 ist enable exit interface FastEthernet all smlt port 1 134 smlt port 24 65 exit ! ! *** SLPP *** ! slpp enable slpp vid 50,222 interface FastEthernet all slpp port 1,24 enable packet-rx-threshold 5 exit	ist peer-ip 10.70.2.1 ist vlan 2 ist enable exit interface FastEthernet all smlt port 1 134 smlt port 24 65 exit ! ! *** SLPP *** ! slpp enable slpp vid 50,222 interface FastEthernet all slpp port 1,24 enable packet-rx-threshold 50 exit

3.2.4 Verify OSPF Operations

3.2.4.1 OSPF Interfaces

VSP 7000: Step 1 - Verify OSPF interfaces

show ip ospf interface enabled

Results:

7010:

```
Interface:  10.70.1.1
    Area ID:  0.0.0.0
    Admin State:  Enabled
    Type:  Passive
    Priority:  1
    Designated Router:  10.70.1.1
    Backup Designated Router:  0.0.0.0
    Authentication Type:  None
    MTU Ignore:  Yes
    Advertise When Down:  No
    Metric Value:  10
Interface:  10.70.50.1
    Area ID:  0.0.0.0
    Admin State:  Enabled
    Type:  Broadcast
    Priority:  0
    Designated Router:  10.70.50.3
    Backup Designated Router:  10.70.50.4
    Authentication Type:  None
    MTU Ignore:  Yes
    Advertise When Down:  No
    Metric Value:  10
Interface:  10.70.222.1
    Area ID:  0.0.0.0
    Admin State:  Enabled
    Type:  Broadcast
    Priority:  1
    Designated Router:  10.70.222.1
    Backup Designated Router:  10.70.222.2
```

```
    Authentication Type:  None
    MTU Ignore:  Yes
    Advertise When Down:  No
    Metric Value:  10
```

7011:

```
Interface:  10.70.1.2
    Area ID:  0.0.0.0
    Admin State:  Enabled
    Type:  Passive
    Priority:  1
    Designated Router:  10.70.1.2
    Backup Designated Router:  0.0.0.0
    Authentication Type:  None
    MTU Ignore:  Yes
    Advertise When Down:  No
    Metric Value:  10
Interface:  10.70.50.2
    Area ID:  0.0.0.0
    Admin State:  Enabled
    Type:  Broadcast
    Priority:  0
    Designated Router:  10.70.50.3
    Backup Designated Router:  10.70.50.4
    Authentication Type:  None
    MTU Ignore:  Yes
    Advertise When Down:  No
    Metric Value:  10
Interface:  10.70.222.2
    Area ID:  0.0.0.0
    Admin State:  Enabled
    Type:  Broadcast
    Priority:  1
    Designated Router:  10.70.222.1
    Backup Designated Router:  10.70.222.2
    Authentication Type:  None
    MTU Ignore:  Yes
    Advertise When Down:  No
    Metric Value:  10
```

On each VSP 7000 in the switch cluster verify the following information:

Option	Verify
Interface	The IP address for the loopback interface, VLAN 10, and VLAN 222 should be disabled
Admin State	Verify that the OSPG Admin state is ***Enabled*** on the loopback address and IP addresses associated with VLANs 10 and 222
Designated Router	For VLAN 222, the core VLAN used between the VSP 7000 and ERS 8000 SMLT cluster switches, verify the OSPF DR is the IP address from switch 8000-1
Backup Designated Router	For VLAN 222, the core VLAN used between the VSP 7000 and ERS 8000 SMLT cluster switches, verify the OSPF BDR is the IP address from switch 8000-2

VSP 7000: Step 2 - Verify OSPF neighbors

show ip ospf neighbor

Results:

7010:

```
Interface       Nbr Router ID   Nbr IP Address  Pri State     RetransQLen Perm
--------------- --------------- --------------- --- --------- ----------- ----
10.70.50.1      10.70.1.2       10.70.50.2      0   Two Way   0           Dyn
10.70.50.1      10.1.1.1        10.70.50.3      150 Full      0           Dyn
10.70.50.1      10.1.1.2        10.70.50.4      200 Full      0           Dyn
10.70.222.1     10.70.1.2       10.70.222.2     1   Full      0           Dyn
10.70.222.1     10.70.1.3       10.70.222.3     0   Full      0           Dyn
```

7011:

```
Interface       Nbr Router ID   Nbr IP Address  Pri State     RetransQLen Perm
--------------- --------------- --------------- --- --------- ----------- ----
10.70.50.2      10.70.1.1       10.70.50.1      0   Two Way   0           Dyn
10.70.50.2      10.1.1.1        10.70.50.3      150 Full      0           Dyn
10.70.50.2      10.1.1.2        10.70.50.4      200 Full      0           Dyn
10.70.222.2     10.70.1.1       10.70.222.1     1   Full      0           Dyn
10.70.222.2     10.70.1.3       10.70.222.3     0   Full      0           Dyn
```

On each VSP 7000 in the switch cluster verify the following information:

Option	Verify
State	For switch 7010, should be displayed as ***Full*** between the OSPF Router-id's for switches 8000-1, 8000-2, 7011, and 7012. For switch 7011, should be displayed as ***Full*** between the OSPF Router-id's for switches 8000-1, 8000-2, 7010, and 7012. If the state is not Full, check the switch configuration, port status, link state, and VLACP status

3.3 Configuration – VSP 9000 Layer 3 Routed SMLT in SMLT Full Mesh Core

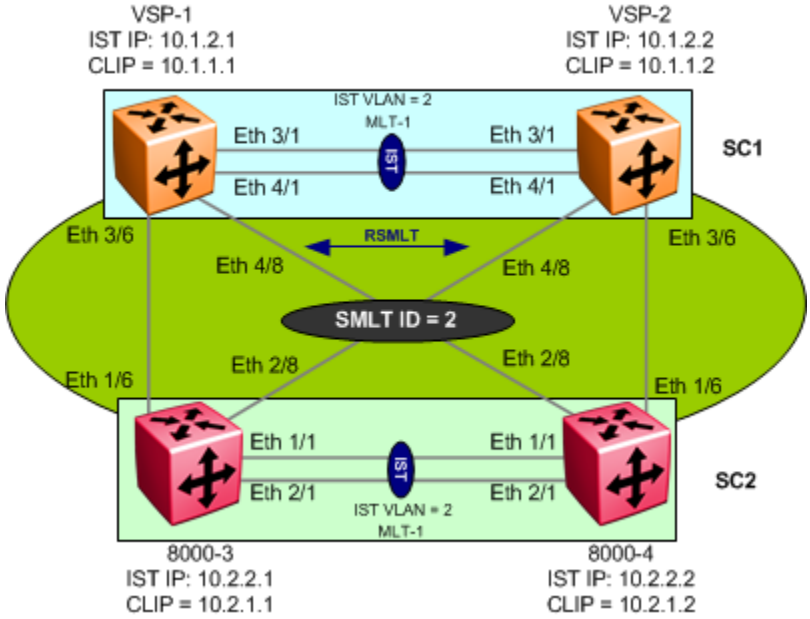


Figure 17: RSMLT Full Mesh Core Configuration

The following example is based on a full mesh SMLT core using Routed SMLT (RSMLT) in the core. Please see configuration example 0 for configuring RSMLT at the SMLT access layer. For this example, we will use OSPF as the routing protocol. For simplicity, we will use OSPF area 0.

In reference to the diagram above, we will configure the following:

- Overall, this configuration example will cover the configuration steps required for VSP-1, VSP-1, 8000-3, and 8000-4.
- Via Switch Cluster #1, we will configure
  - VLAN 2 for the IST VLAN using MLT ID = 1
  - VLAN 3 for the core VLANs using MLT and SMLT ID = 2
  - OSPF as the IGP using area 0
  - VSP-1 (DR) OSPF priority to 100 for VLAN 3
  - VSP-2 (BDR) OSPF priority to 150 for VLAN 3 IST IP subnet 10.1.2.0/30
  - Enable VLACP using recommended reserved MAC
  - Using the CLIP address as the OSPF router ID
  - Enable SLPP on the core VLANs with a SLPP Packet Receive threshold of 5 on VSP-1 assuming VSP-1 is the primary switch and a threshold of 50 on VSP-2 assuming it is the secondary switch
- Via Switch Cluster #2, we will configure
  - VLAN 2 for the IST VLAN using MLT ID = 1
  - VLAN 3 for the core VLAN using MLT and SMLT ID = 2
  - OSPF as the IGP using area 0
  - 8000-3 and 8000-4 OSPF priority to 0 for VLAN 3
  - IST IP subnet 10.2.2.0/30
  - Enable VLACP using recommended reserved MAC

- Using the CLIP address as the OSPF router ID
- Enable SLPP on the core VLAN with a SLPP Packet Receive threshold of 5 on 8000-3 assuming VSP-1 is the primary switch and a threshold of 50 on 8000-4 assuming it is the secondary switch

3.3.1 RSMLT Configuration

3.3.1.1 MSTP

ERS 8000 SMLT Cluster – Enable MSTP

8000-3 & 8000-4: Same configuration on both switches

```
8000-3:5# config boot flags spanning-tree-mode mstp
Warning: Please save boot configuration and reboot the switch
         for this to take effect.
Warning: Please carefully save your configuration files before
         starting configuring the switch in RSTP or MSTP mode.
         The syntax used to create VLANs in any of these new
         modes is NOT COMPATIBLE with the default mode (STP)
8000-3:5# save boot
8000-3:5# boot -y
```

As the VSP 9000 uses MSTP by default, it is recommended to change the Spanning mode on the access stackable switches to also use MSTP. Even though Spanning Tree is not used and is disabled on the core ports, the Spanning Tree mode is used by some Network Management tools such as VLAN Manager in COM. VLAN Manager will regroup all VLANs per Spanning Tree group type, hence, if you leave the stackable edge switch in their default Spanning Tree mode of STPG, then VLAN Manager will not be able to display, create, delete, or sync a VLAN across the VSP and the edge stackable switches.

3.3.1.2 Create VLANs

The following port based VLANs will be configured on the SMLT Switch cluster

- VLAN 2 to be used by the Inter Switch Trunk (IST)
- VLAN 3 to be used in the RSMLT core level to VSP-1, VSP-2, 8000-3, and 8000-4.

SMLT Cluster: Create VLANs 2 and 3

VSP-1 & VSP-2: Same configuration both switches

```
VSP-1:1(config)#vlan create 2 name "IST" type port-mstprstp 0
VSP-1:1(config)#vlan create 3 name "RSMLT_Core" type port-mstprstp 0
```

8000-3 & 8000-4: Same configuration on both switches

```
8000-3:5#config vlan 2 create byport-mstprstp 0 name IST
8000-3:5#config vlan 3 create byport-mstprstp 0 name "RSMLT_Core"
```

3.3.1.3 Create IST

Multilink Trunking 1 (MLT 1) will be used for the IST with port members 2/1 and 3/1 for SMLT cluster 1. We will also use MLT 1 for the IST for SMLT cluster 2 with port members 1/1 and 2/1. 802.1Q tagging will be enabled on all IST port members and Spanning Tree will be disabled on all IST port members by default. VLACP will be enabled on the IST trunk.

It is recommended to use the reserved multicast MAC address of 01:80:c2:00:00:0f for the VLACP MAC address.

SMLT Cluster: Step 1 - Create MLT 1 for IST

VSP-1 & VSP-2: Same configuration both switches

```
VSP-1:1(config)#mlt 1 enable name "IST"
VSP-1:1(config)#mlt 1 member 3/1,4/1
VSP-1:1(config)#mlt 1 encapsulation dot1q
VSP-1:1(config)#vlan mlt 2 1
```

8000-3 & 8000-4: Same configuration on both switches

```
8000-3:5# config mlt 1 create
8000-3:5# config mlt 1 name IST
8000-3:5# config mlt 1 add port 1/1,2/1
8000-3:5# config vlan 2 add-mlt 1
```

SMLT Cluster: Step 2 - Create IST

VSP-1:

```
VSP-1:1(config)#interface vlan 2
VSP-1:1(config-if)#ip address 10.1.2.1 255.255.255.252
VSP-1:1(config-if)#exit
VSP-1:1(config)#interface mlt 1
VSP-1:1(config-if)#ist peer-ip 10.1.2.2 vlan 2
VSP-1:1(config-if)#ist enable
VSP-1:1(config-if)#exit
```

VSP-2:

```
VSP-2:1(config)#interface vlan 2
VSP-2:1(config-if)#ip address 10.1.2.2 255.255.255.252
VSP-2:1(config-if)#exit
VSP-2:1(config)#interface mlt 1
VSP-2:1(config-if)#ist peer-ip 10.1.2.1 vlan 2
VSP-2:1(config-if)#ist enable
VSP-2:1(config-if)#exit
```

8000-3:

```
8000-3:5# config vlan 2 ip create 10.2.2.1/30
8000-3:5# config mlt 1 ist create ip 10.2.2.2 vlan-id 2
8000-3:5# config mlt 1 ist enable
```

8000-4:

```
8000-4:5# config vlan 2 ip create 10.2.2.2/30
8000-4:5# config mlt 1 ist create ip 10.2.2.1 vlan-id 2
8000-4:5# config mlt 1 ist enable
```

SMLT Cluster: Step 3 - Enable VLACP

VSP-1 & VSP-2: Same configuration both switches

```
VSP-1:1(config)#interface GigabitEthernet 3/1,4/1
VSP-1:1(config-if)#vlacp timeout long timeout-scale 3 funcmac-addr 01:80:c2:00:00:0f
VSP-1:1(config-if)#vlacp enable
VSP-1:1(config-if)#exit
```

8000-3 & 8000-4: Same configuration on both switches

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

3.3.1.4 SMLT-2 for RSMLT Core

SMLT Cluster: Create SMLT-2

VSP-1 & VSP-2: Same configuration both switches

```
VSP-1:1(config)#mlt 2 enable name "RSMLT_Core"
VSP-1:1(config)#mlt 2 member 3/6,4/8
VSP-1:1(config)#mlt 2 encapsulation dot1q
VSP-1:1(config)#vlan mlt 3 2
VSP-1:1(config)#interface mlt 2
VSP-1:1(config-if)#smlt
VSP-1:1(config)#exit
```

8000-3 & 8000-4: Same configuration on both switches

```
8000-3:5# config mlt 2 create
8000-3:5# config mlt 2 name RSMLT_Core
8000-3:5# config mlt 2 perform-tagging enable
8000-3:5# config mlt 2 add port 1/6,2/8
8000-3:5# config vlan 3 add-mlt 2
8000-3:5# config vlan 3 add-mlt 2
8000-3:5# config mlt 2 smlt create smlt-id 2
```

3.3.1.5 Add VLAN 3 to IST

SMLT Cluster: Add VLAN 3 to IST

VSP-1 & VSP-2: Same configuration both switches

```
VSP-1:1(config)#vlan mlt 3 1
```

8000-3 & 8000-4: Same configuration on both switches

```
8000-3:5# config vlan 3 add-mlt 1
```

3.3.1.6 Add IP address to VLAN 3

SMLT Cluster: Add IP address to VLAN 3

VSP-1:

```
VSP-1:1(config)#interface vlan 3
VSP-1:1(config-if)#ip address 10.1.3.1 255.255.255.248
VSP-1:1(config-if)#exit
```

VSP-2:

```
VSP-2:1(config)#interface vlan 3
VSP-2:1(config-if)#ip address 10.1.3.2 255.255.255.248
VSP-2:1(config-if)#exit
```

8000-3:

```
8000-3:5# config vlan 3 ip create 10.1.3.3/29
```

8000-4:

```
8000-4:5# config vlan 3 ip create 10.1.3.4/29
```

3.3.1.7 Loopback/Circuitless IP (Lpbk/CLIP)

By default, the VSP 9000 and ERS 8600/8800 automatically adds an OSPF router-id. For trouble-shooting proposes or if you are using BGP-4, you may wish to set the OSPF router-id; please note that by default, the BGP router-id is derived from the OSPF router-id.

For this configuration example, assuming no exiting circuitless-ip address have already been configured, we will configure the following

- use Lpbk/CLIP ID 1 with the following IP addresses
  - VSP-1 : 10.1.1.1/32
  - VSP-2 : 10.1.1.2/32
  - 8000-3 : 10.2.1.1/32
  - 8000-4 : 10.2.1.2/32
- Enable OSPF on Lpbk/CLIP 1

Although you can use any mask with a Circuitless-IP address, it is recommended to use a 32-bit IP subnet mask.

Please note that by default, the Lpbk/CLIP address uses OSPF area 0. If the CLIP is used in a different OSPF area, please use the command '*config ip circuitless-ip-int <1..32> area <ipaddr>*' to change the OSPF area.

SMLT Cluster: Create CLIP 1 and enable OSPF

VSP-1:

```
VSP-1:1(config)#interface loopback 1
VSP-1:1(config-if)#ip address 10.1.1.1/32
VSP-1:1(config-if)#ip ospf 1
VSP-1:1(config-if)#exit
```

VSP-2:

```
VSP-2:1(config)#interface loopback 1
VSP-2:1(config-if)#ip address 10.1.1.2/32
VSP-2:1(config-if)#ip ospf 1
VSP-2:1(config-if)#exit
```

8000-3:

```
8000-3:5# config ip circuitless-ip-int 1 create 10.2.1.1/32
8000-3:5# config ip circuitless-ip-int 1 ospf enable
```

8000-4:

```
8000-4:5# config ip circuitless-ip-int 1 create 10.2.1.2/32
8000-4:5# config ip circuitless-ip-int 1 ospf enable
```

3.3.1.8 Change the OSPF Router-ID

SMLT Cluster: Change the OSPF router-id with the CLIP address

VSP-1:

```
VSP-1:1(config)#router ospf
VSP-1:1(config-ospf)#router-id 10.1.1.1
VSP-1:1(config-ospf)#exit
```

VSP-2:

```
VSP-2:1(config)#router ospf
VSP-2:1(config-ospf)#router-id 10.1.1.2
VSP-2:1(config-ospf)#exit
```

8000-3:

```
8000-3:5# config ip ospf router-id 10.2.1.1
```

8000-4:

```
8000-4:5# config ip ospf router-id 10.2.1.2
```

3.3.1.9 Enable OSPF

VLAN 3 will be configured with OSPF on the SMLT Switch cluster. For this example, we will make VSP-1 the OSPF DR for VLAN 3 and make VSP-2 the BDR for VLAN 3.

SMLT Cluster: Enable OSPF for VLAN 3, make VSP-1 the DR, VSP-2 the BDR, and enable OSPF globally

VSP-1:

```
VSP-1:1(config)#interface vlan 3
VSP-1:1(config-if)#ip ospf enable
VSP-1:1(config-if)#ip ospf priority 100
VSP-1:1(config-if)#exit
VSP-1:1(config)#router ospf enable
```

VSP-2:

```
VSP-2:1(config)#interface vlan 3
VSP-2:1(config-if)#ip ospf enable
VSP-2:1(config-if)#ip ospf priority 150
VSP-2:1(config-if)#exit
VSP-2:1(config)#router ospf enable
```

8000-3 & 8000-4: Same configuration on both switches

```
8000-3:5# config vlan 3 ip ospf priority 0
8000-3:5# config vlan 3 ip ospf enable
8000-3:5# config ip ospf enable
```

3.3.1.10 Enable RSMLT

VLAN 3 with RSMLT using default timers

SMLT Cluster: Enable RSMLT

VSP-1 & VSP-2: Same configuration both switches

```
VSP-1:1(config)#interface vlan 3
VSP-1:1(config-if)#ip rsmlt
VSP-1:1(config-if)#exit
```

8000-3 & 8000-4: Same configuration on both switches

```
8000-3:5# config vlan 3 ip rsmlt enable
```

3.3.1.11 CP Limit – SMLT port members

CP Limit will be enabled on all the SMLT core port members. For this example, we will select the moderate recommendations for CP-Limit.

SMLT Cluster: CP Limit

VSP-1 & VSP-2: Same configuration both switches

```
VSP-1:1(config)#interface GigabitEthernet 3/6,4/8
VSP-1:1(config-if)#cp-limit 9000 shutdown
VSP-1:1(config-if)#exit
```

8000-3 & 8000-4: Same configuration on both switches

```
8000-3:5# config ethernet 1/6,2/8 cp-limit enable multicast-limit 9000 broadcast-limit 9000
```

3.3.1.12 SLPP

SLPP will be enabled globally and on the SMLT access ports and core port members. In this example, we only show the configuration for the core ports. On the SMLT primary switch, we will set the SLPP packet-rx-threshold to 5 while on the SMLT secondary switch, we will set the SLPP packet-rx-threshold to 50 for the core ports.

SLPP should only be enabled on the SMLT access or core ports and not on the IST port members.

SMLT Cluster: Enable SLPP for VLAN 3

VSP-1:

```
VSP-1:1(config)#slpp enable
VSP-1:1(config)#slpp vid 3
VSP-1:1(config)#interface GigabitEthernet 3/6,4/8
VSP-1:1(config-if)#slpp packet-rx
VSP-1:1(config-if)#slpp packet-rx-threshold 5
VSP-1:1(config-if)#exit
```

VSP-2: Same configuration as VSP-1 except for the SLPP packet receive threshold

```
VSP-2:1(config-if)#slpp packet-rx-threshold 50
```

8000-3:

```
8000-3:5# config slpp add 3
8000-3:5# config slpp operation enable
8000-3:5# config ethernet 1/6,2/8 slpp packet-rx enable
8000-3:5# config ethernet 1/6,2/8 slpp packet-rx-threshold 5
```

8000-4: Same configuration as 8000-3 except for the SLPP packet receive threshold

```
8000-4:5# ethernet 1/6,2/8 slpp packet-rx-threshold 50
```

3.3.1.13 VLACP

We will enable VLACP in the core using VLACP short timers and with the recommended reserved MAC.

SMLT Cluster: Enable VLACP

VSP-1 & VSP-2: Same configuration both switches

```
VSP-1:1(config)#interface GigabitEthernet 3/6,4/8
VSP-1:1(config-if)#vlacp timeout short timeout-scale 5 funcmac-addr 01:80:c2:00:00:0f
VSP-1:1(config-if)#vlacp enable
VSP-1:1(config-if)#exit
```

8000-3 & 8000-4: Same configuration on both switches

```
8000-3:5# config ethernet 1/6,2/8 vlacp fast-periodic-time 500
8000-3:5# config ethernet 1/6,2/8 vlacp timeout short
8000-3:5# config ethernet 1/6,2/8 vlacp timeout-scale 5
8000-3:5# config ethernet 1/6,2/8 vlacp enable
8000-3:5# config ethernet 1/6,2/8 vlacp macaddress 01:80:c2:00:00:0f
```

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

3.3.1.14 Discard Untagged Frames

It is recommended to enable discard untagged frames on all IST and SMLT ports.

SMLT Cluster: Enable Discard Untagged Frames

VSP-1 & VSP-2: Same configuration both switches

```
VSP-1:1(config)#interface GigabitEthernet 3/1,3/6,4/1,4/8
VSP-1:1(config-if)#untagged-frames-discard
VSP-1:1(config-if)#exit
```

8000-3 & 8000-4: Same configuration on both switches

```
8000-3:5# config ethernet 1/1,2/1,1/6,2/8 untagged-frames-discard enable
```

3.3.2 Verify Layer 3 RSMLT Operations

3.3.2.1 OSPF Operations

Verify that all the switches in the RSMLT core are peered:

ACLI and CLI

show ip ospf neighbors

Results:

VSP-1:

```
==============================================================================
                        Ospf Neighbors
==============================================================================
INTERFACE       NBRROUTERID     NBRIPADDR       PRIO_STATE    RTXQLEN PERMANENCE
------------------------------------------------------------------------------
10.1.3.1        10.2.1.1        10.1.3.3        0    Full     0       Dynamic
10.1.3.1        10.2.1.2        10.1.3.4        0    Full     0       Dynamic
10.1.3.1        10.1.1.2        10.1.3.2        0    Full     0       Dynamic
```

VSP-2:

```
==============================================================================
                        Ospf Neighbors
==============================================================================
INTERFACE       NBRROUTERID     NBRIPADDR       PRIO_STATE    RTXQLEN PERMANENCE
------------------------------------------------------------------------------
10.1.3.2        10.2.1.1        10.1.3.3        0    TwoWay   0       Dynamic
10.1.3.2        10.2.1.2        10.1.3.4        0    TwoWay   0       Dynamic
10.1.3.2        10.1.1.1        10.1.3.1        100  Full     0       Dynamic
```

8000-3:

```
==============================================================================
                        Ospf Neighbors
==============================================================================
INTERFACE       NBRROUTERID     NBRIPADDR       PRIO_STATE    RTXQLEN PERMANENCE
------------------------------------------------------------------------------
10.1.3.3        10.1.1.1        10.1.3.1        100  Full     0       Dynamic
10.1.3.3        10.2.1.2        10.1.3.4        0    TwoWay   0       Dynamic
10.1.3.3        10.1.1.2        10.1.3.2        0    TwoWay   0       Dynamic
```

8000-4:

```
==============================================================================
```

```
                        Ospf Neighbors
================================================================================
INTERFACE       NBRROUTERID     NBRIPADDR       PRIO_STATE    RTXQLEN PERMANENCE
--------------------------------------------------------------------------------
10.1.3.4        10.2.1.1        10.1.3.3        0    TwoWay   0       Dynamic
10.1.3.4        10.1.1.1        10.1.3.1        100  Full     0       Dynamic
10.1.3.4        10.1.1.2        10.1.3.2        0    TwoWay   0       Dynamic
```

On each VSP 9000 & ERS 8000 in the switch cluster verify the following information:

Option	Verify
INTERFACE	The local IP address should be displayed as follows: • VSP-1: ***10.1.3.1*** • VSP-2: ***10.1.3.2*** • 8000-3: ***10.1.3.3*** • 8000-4: ***10.1.3.4***
NBRIPADDR PRIO_STATE	Verify that switches VSP-2, 8000-3, 8000-4 peering state is displayed as ***Full*** pointing to 8000-1 VLAN 3's NBRIPADDR of 10.1.3.1 as it is the OSPF DR for VLAN 3.

3.3.2.2 RSMLT Operations

Verify that the RSMLT instance is configured correctly and is functioning by issuing the following command:

ACLI

show ip rsmlt

CLI

show ip rsmlt info

Results:

VSP-1:

```
================================================================================
                          Ip Rsmlt Local Info
================================================================================

VID   IP              MAC               ADMIN   OPER  HDTMR  HUTMR
--------------------------------------------------------------------------------
3     10.1.3.1        00:01:81:28:86:13 Enable  Up    60     180

VID   SMLT ID                  SLT ID
--------------------------------------------------------------------------------
3       2
================================================================================
                          Ip Rsmlt Peer Info
================================================================================

VID   IP              MAC               ADMIN   OPER  HDTMR  HUTMR
--------------------------------------------------------------------------------
3     10.1.3.2        00:e0:7b:bc:22:01 Enable  Up    60     180

VID   HDT REMAIN  HUT REMAIN  SMLT ID                  SLT ID
--------------------------------------------------------------------------------
3     60          180         2
```

On each VSP 9000 and ERS 8000 in the switch cluster verify the following information:

Option	Verify
VID	The VID should be displayed as ***3*** and ***30*** for SMLT 2.
IP	Verify the correct IP address for each switch: • VSP-1: ***10.1.3.1*** • VSP-2: ***10.1.3.2*** • 8000-3: ***10.1.3.3*** • 8000-4: ***10.1.3.4***
ADMIN	Verify that the RSMLT Admin is ***Enabled*** on both clusters. If not, there is a configuration error.
OPER	Verify that the RSMLT operation is ***Up*** on both clusters.
HUTMR HDRMR	Verify that the RSMLT holdup and holddown timer is set to ***60*** and ***180*** respectively on both clusters. If not, there is a configuration error.
SMLT ID	Verify the SMLT ID is showing ***2***.

Ip Rsmlt Peer Info	Verify the RSMLT Peer is showing:
	• VSP-1:
	  ○ VLAN 3: SMLT ***2***, IP ***10.1.3.2***
	• VSP-2:
	  ○ VLAN 30, SMLT ***2***, IP ***10.1.3.1***
	• 8000-3:
	  ○ VLAN 3, SMLT ***2***, IP ***10.1.3.4***
	• 8000-4:
	  ○ VLAN 3, SMLT ***2***, IP ***10.1.3.3***

3.3.2.3 Lpbk/CLIP Address

Verify that the RSMLT instance is configured correctly and is functioning by issuing the following command:

ACLI

show interfaces loopback

CLI

show ip circuitless-ip-int info

Results:

VSP-1:

```
================================================================================
                          Circuitless Ip Interface
================================================================================
INTERFACE    IP_ADDRESS      NET_MASK        OSPF_STATUS  PIM_STATUS   AREA_ID
ID
--------------------------------------------------------------------------------
1            10.1.1.1        255.255.255.255 enable       enable       0.0.0.0
```

On each VSP 9000 and ERS 8800/8600 in the switch cluster verify the following information:

Option	Verify
INTERFACE	The Lpbk/CLIP IP address should be displayed as follows: • VSP-1: ***10.1.1.1*** • VSP-2: ***10.1.1.2*** • 8000-3: ***10.2.1.1*** • 8000-4: ***10.2.1.2***

3.4 Configuration – ERS 8600/8800 Layer 3 Routed SMLT in SMLT Full Mesh Core

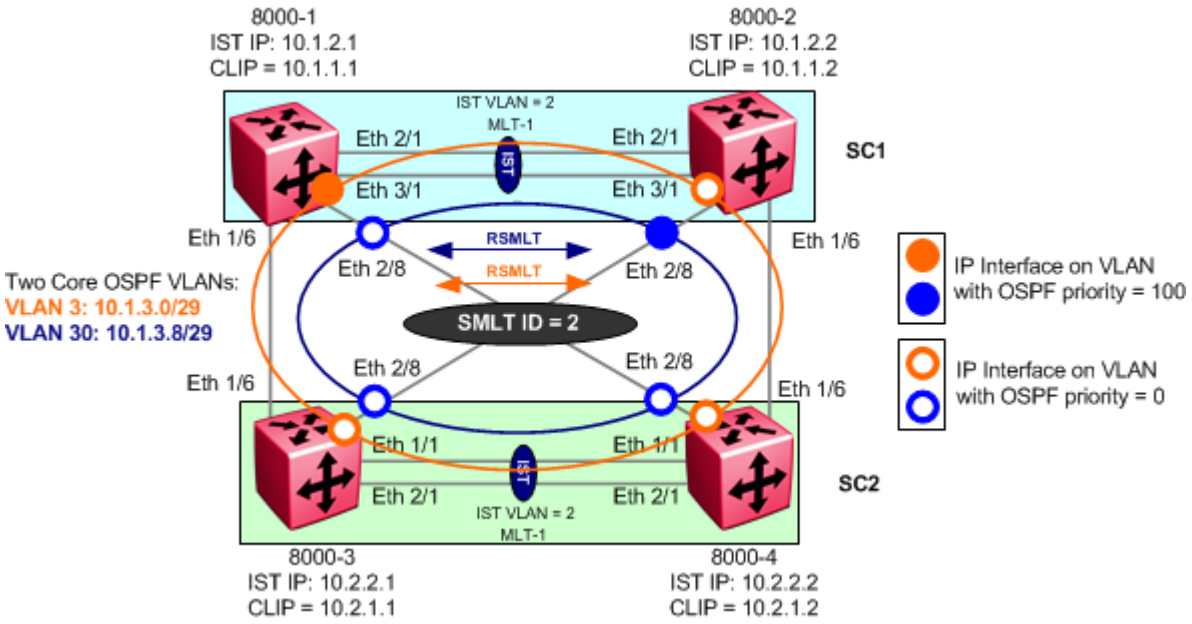


Figure 18: RSMLT Full Mesh Core Configuration

The following example is based on a full mesh SMLT core using Routed SMLT (RSMLT) in the core. Please see configuration example 0 for configuring RSMLT at the SMLT access layer. For this example, we will use OSPF as the routing protocol. For simplicity, we will use OSPF area 0.

In reference to the diagram above, we will configure the following:

- Overall, this configuration example will cover the configuration steps required for 8000-1, 8000-1, 8000-3, and 8000-4.
- Via Switch Cluster #1, we will configure
  - VLAN 2 for the IST VLAN using MLT ID = 1
  - VLAN 3 and 30 for the core VLANs using MLT and SMLT ID = 2
  - OSPF as the IGP using area 0
  - 8000-1 OSPF priority to 100 for VLAN 3 and 0 for VLAN 30
  - 8000-2 OSPF priority to 0 for VLAN 3 and 100 for VLAN 30
  - IST IP subnet 10.1.2.0/30
  - Enable VLACP using recommended reserved MAC
  - Using the CLIP address as the OSPF router ID
  - Enable SLPP on the core VLANs with a SLPP Packet Receive threshold of 5 on 8000-1 assuming 8000-1 is the primary switch and a threshold of 50 on 8000-2 assuming it is the secondary switch
- Via Switch Cluster #2, we will configure
  - VLAN 2 for the IST VLAN using MLT ID = 1

- VLAN 3 and 30 for the core VLANs using MLT and SMLT ID = 2
- OSPF as the IGP using area 0
- 8000-3 and 8000-4 OSPF priority to 0 for VLAN 3 and VLAN 30
- IST IP subnet 10.2.2.0/30
- Enable VLACP using recommended reserved MAC
- Using the CLIP address as the OSPF router ID
- Enable SLPP on the core VLANs with a SLPP Packet Receive threshold of 5 on 8000-3 assuming 8000-1 is the primary switch and a threshold of 50 on 8000-4 assuming it is the secondary switch

3.4.1 RSMLT Configuration

3.4.1.1 Create VLANs

The following port based VLANs will be configured on the SMLT Switch cluster

- VLAN 2 to be used by the Inter Switch Trunk (IST)
- VLAN 3 and VLAN 30 to be used in the RSMLT core level to 8000-1, 8000-2, 8000-3, and 8000-4.

ERS 8000 SMLT Cluster: Create VLAN 2, 3, and 30

8000-1, 8000-2, 8000-3 & 8000-4: Same configuration on all switches

```
8000-1:5# config vlan 2 create byport 1 name IST
8000-1:5# config vlan 3 create byport 1 name RSMLT_Core_1
8000-1:5# config vlan 30 create byport 1 name RSMLT_Core_2
```

3.4.1.2 Change fdb aging timer for VLAN 3 and 30

ERS 8000 SMLT Cluster: Change fdb aging timer for VLAN 3 and 30

8000-1, 8000-2, 8000-3 & 8000-4: Same configuration on all switches

```
8000-1:5# config vlan 3 fdb-entry aging-time 21601
8000-1:5# config vlan 30 fdb-entry aging-time 21601
```

3.4.1.3 Create IST

Multilink Trunking 1 (MLT 1) will be used for the IST with port members 2/1 and 3/1 for SMLT cluster 1. We will also use MLT 1 for the IST for SMLT cluster 2 with port members 1/1 and 2/1. 802.1Q tagging will be enabled on all IST port members and Spanning Tree will be disabled on all IST port members by default. VLACP will be enabled on the IST trunk.

It is recommended to use the reserved multicast MAC address of 01:80:c2:00:00:0f for the VLACP MAC address.

ERS 8000 SMLT Cluster: Step 1 – Create MLT 1 for IST

8000-1, 8000-2: Same configuration on both switches

```
8000-1:5# config mlt 1 create
8000-1:5# config mlt 1 name IST
8000-1:5# config mlt 1 add port 2/1,3/1
8000-1:5# config vlan 2 add-mlt 1
```

8000-3 & 8000-4: Same configuration on both switches

```
8000-3:5# config mlt 1 create
8000-3:5# config mlt 1 name IST
8000-3:5# config mlt 1 add port 1/1,2/1
8000-3:5# config vlan 2 add-mlt 1
```

ERS 8000 SMLT Cluster: Step 2 – Create IST

8000-1:

```
8000-1:5# config vlan 2 ip create 10.1.2.1/30
8000-1:5# config mlt 1 ist create ip 10.1.2.2 vlan-id 2
8000-1:5# config mlt 1 ist enable
```

8000-2:

```
8000-2:5# config vlan 2 ip create 10.1.2.2/30
8000-2:5# config mlt 1 ist create ip 10.1.2.1 vlan-id 2
8000-2:5# config mlt 1 ist enable
```

8000-3:

```
8000-3:5# config vlan 2 ip create 10.2.2.1/30
8000-3:5# config mlt 1 ist create ip 10.2.2.2 vlan-id 2
8000-3:5# config mlt 1 ist enable
```

8000-4:

```
8000-4:5# config vlan 2 ip create 10.2.2.2/30
8000-4:5# config mlt 1 ist create ip 10.2.2.1 vlan-id 2
8000-4:5# config mlt 1 ist enable
```

ERS 8000 SMLT Cluster: Step 3 – Enable VLACP

8000-1, 8000-2: Same configuration on both switches

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

8000-3 & 8000-4: Same configuration on both switches

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

3.4.1.4 SMLT-2 for RSMLT Core

ERS 8000 SMLT Cluster: Create SMLT-2

8000-1, 8000-2, 8000-3 & 8000-4: Same configuration on all switches

```
8000-1:5# config mlt 2 create
8000-1:5# config mlt 2 name RSMLT_Core
8000-1:5# config mlt 2 perform-tagging enable
8000-1:5# config mlt 2 add port 1/6,2/8
8000-1:5# config vlan 3 add-mlt 2
8000-1:5# config vlan 30 add-mlt 2
8000-1:5# config mlt 2 smlt create smlt-id 2
```

3.4.1.5 Add VLAN 3 and 30 to IST

ERS 8000 SMLT Cluster: Add VLANs 3 and 30 to the IST

8000-1, 8000-2, 8000-3 & 8000-4: Same configuration on all switches

```
8000-1:5# config vlan 3 add-mlt 1
8000-1:5# config vlan 30 add-mlt 1
```

3.4.1.6 Add IP address to VLAN 3 and VLAN 30

ERS 8000 SMLT Cluster: Add IP address to VLAN 3 and 30

8000-1:

```
8000-1:5# config vlan 3 ip create 10.1.3.1/29
8000-1:5# config vlan 30 ip create 10.1.3.9/29
```

8000-2:

```
8000-2:5# config vlan 3 ip create 10.1.3.2/29
8000-1:5# config vlan 30 ip create 10.1.3.10/29
```

8000-3:

```
8000-3:5# config vlan 3 ip create 10.1.3.3/29
8000-3:5# config vlan 30 ip create 10.1.3.11/29
```

8000-4:

```
8000-4:5# config vlan 3 ip create 10.1.3.4/29
8000-4:5# config vlan 30 ip create 10.1.3.12/29
```

3.4.1.7 Circuitless IP (CLIP)

By default, the ERS 8800/8600 automatically adds an OSPF router-id. For trouble-shooting proposes or if you are using BGP-4, you may wish to set the OSPF router-id; please note that by default, the BGP router-id is derived from the OSPF router-id.

For this configuration example, assuming no exiting circuitless-ip address have already been configured, we will configure the following

- use CLIP ID 1 with the following IP addresses
  - 8000-1 : 10.1.1.1/32
  - 8000-2 : 10.1.1.2/32
  - 8000-3 : 10.2.1.1/32
  - 8000-4 : 10.2.1.2/32
- Enable OSPF on CLIP 1

Although you can use any mask with a Circuitless-IP address, it is recommended to use a 32-bit IP subnet mask.

Please note that by default, the CLIP address uses OSPF area 0. If the CLIP is used in a different OSPF area, please use the command '*config ip circuitless-ip-int <1..32> area <ipaddr>*' to change the OSPF area.

ERS 8000 SMLT Cluster: Create CLIP 1 and enable OSPF

8000-1:

```
8000-1:5# config ip circuitless-ip-int 1 create 10.1.1.1/32
8000-1:5# config ip circuitless-ip-int 1 ospf enable
```

8000-2:

```
8000-2:5# config ip circuitless-ip-int 1 create 10.1.1.2/32
8000-2:5# config ip circuitless-ip-int 1 ospf enable
```

8000-3:

```
8000-3:5# config ip circuitless-ip-int 1 create 10.2.1.1/32
8000-3:5# config ip circuitless-ip-int 1 ospf enable
```

8000-4:

```
8000-4:5# config ip circuitless-ip-int 1 create 10.2.1.2/32
8000-4:5# config ip circuitless-ip-int 1 ospf enable
```

3.4.1.8 Change the OSPF Router-ID

ERS 8000 SMLT Cluster: Change the OSPF router-id with the CLIP address

8000-1:

```
8000-1:5# config ip ospf router-id 10.1.1.1
```

8000-2:

```
8000-2:5# config ip ospf router-id 10.1.1.2
```

8000-3:

```
8000-3:5# config ip ospf router-id 10.2.1.1
```

8000-4:

```
8000-4:5# config ip ospf router-id 10.2.1.2
```

3.4.1.9 Enable OSPF

VLAN 3 and 30 will be configured with OSPF on the SMLT Switch cluster. For this example, we will make 8000-1 the OSPF DR for VLAN 3 and make 8000-2 the DR for VLAN 30.

ERS 8000 SMLT Cluster: Enable OSPF for VLAN 3 and 30, make via VLAN3 switch 8000-1 the DR, make via VLAN 30 switch 8000-2 the DR, and enable OSPF globally

8000-1:

```
8000-1:5# config vlan 3 ip ospf priority 100
8000-1:5# config vlan 3 ip ospf enable
8000-1:5# config vlan 30 ip ospf priority 0
8000-1:5# config vlan 30 ip ospf enable
8000-1:5# config ip ospf enable
```

8000-2:

```
8000-2:5# config vlan 3 ip ospf priority 0
8000-2:5# config vlan 3 ip ospf enable
8000-2:5# config vlan 30 ip ospf priority 100
8000-2:5# config vlan 30 ip ospf enable
8000-2:5# config ip ospf enable
```

8000-3 & 8000-4: Same configuration on both switches

```
8000-3:5# config vlan 3 ip ospf priority 0
8000-3:5# config vlan 3 ip ospf enable
8000-3:5# config vlan 30 ip ospf priority 0
8000-3:5# config vlan 30 ip ospf enable
```

3.4.1.10 Enable RSMLT

VLAN 3 with RSMLT using default timers

ERS 8000 SMLT Cluster: Enable RSMLT

8000-1, 8000-2, 8000-3 & 8000-4: Same configuration on all switches

```
8000-1:5# config vlan 3 ip rsmlt enable
8000-1:5# config vlan 30 ip rsmlt enable
```

3.4.1.11 CP Limit – SMLT port members

CP Limit will be enabled on all the SMLT core port members. For this example, we will select the moderate recommendations for CP-Limit.

ERS 8000 SMLT Cluster: CP Limit

8000-1, 8000-2, 8000-3 & 8000-4: Same configuration on all switches

```
8000-1:5# config ethernet 1/6,2/8 cp-limit enable multicast-limit 9000 broadcast-limit 9000
```

3.4.1.12 SLPP

SLPP will be enabled globally and on the SMLT access ports and core port members. In this example, we only show the configuration for the core ports. On the SMLT primary switch, we will set the SLPP packet-rx-threshold to 5 while on the SMLT secondary switch, we will set the SLPP packet-rx-threshold to 50 for the core ports.

SLPP should only be enabled on the SMLT access or core ports and not on the IST port members.

ERS 8000 SMLT Cluster: Enable SLPP for VLAN 3

8000-1:

```
8000-1:5# config slpp add 3,30
8000-1:5# config slpp operation enable
8000-1:5# config ethernet 1/6 slpp packet-rx enable
8000-1:5# config ethernet 1/6 slpp packet-rx-threshold 5
```

8000-2: Same configuration as VSP-1 except for the SLPP packet receive threshold

```
VSP-2:1(config-if)#slpp packet-rx-threshold 50
```

8000-3:

```
8000-3:5# config slpp add 3,30
8000-3:5# config slpp operation enable
8000-3:5# config ethernet 1/6 slpp packet-rx enable
8000-3:5# config ethernet 1/6 slpp packet-rx-threshold 5
```

8000-4: Same configuration as 8000-3 except for the SLPP packet receive threshold

```
8000-4:5# ethernet 1/6 slpp packet-rx-threshold 50
```

3.4.1.13 VLACP

We will enable VLACP in the core using VLACP short timers and with the recommended reserved MAC.

ERS 8000 SMLT Cluster: Enable VLACP

8000-1, 8000-2, 8000-3 & 8000-4: Same configuration on all switches

```
8000-1:5# config ethernet 1/6,2/8 vlacp fast-periodic-time 500
8000-1:5# config ethernet 1/6,2/8 vlacp timeout short
8000-1:5# config ethernet 1/6,2/8 vlacp timeout-scale 5
8000-1:5# config ethernet 1/6,2/8 vlacp macaddress 01:80:c2:00:00:0f
8000-1:5# config ethernet 1/6,2/8 vlacp enable
```

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

3.4.1.14 Discard Untagged Frames

It is recommended to enable discard untagged frames on all IST and SMLT ports.

ERS 8000 SMLT Cluster: Step 3 – Enable VLACP

8000-1, 8000-2: Same configuration on both switches

```
8000-1:5# config ethernet 2/1,3/1,1/6,2/8 untagged-frames-discard enable
```

8000-3 & 8000-4: Same configuration on both switches

```
8000-1:5# config ethernet 1/1,2/1,1/6,2/8 untagged-frames-discard enable
```

3.4.2 Verify Layer 3 RSMLT Operations

3.4.2.1 OSPF Operations

Verify that all the switches in the RSMLT core are peered:

show ip ospf neighbors

Results:

8000-1:

```
================================================================================
                          Ospf Neighbors
================================================================================
INTERFACE       NBRROUTERID     NBRIPADDR       PRIO_STATE    RTXQLEN PERMANENCE
--------------------------------------------------------------------------------
10.1.3.9        10.2.1.2        10.1.3.12       0    TwoWay   0       Dynamic
10.1.3.9        10.2.1.1        10.1.3.11       0    TwoWay   0       Dynamic
10.1.3.9        10.1.1.2        10.1.3.10       100  Full     0       Dynamic
10.1.3.1        10.2.1.1        10.1.3.3        0    Full     0       Dynamic
10.1.3.1        10.2.1.2        10.1.3.4        0    Full     0       Dynamic
10.1.3.1        10.1.1.2        10.1.3.2        0    Full     0       Dynamic
```

8000-2:

```
================================================================================
                          Ospf Neighbors
================================================================================
INTERFACE       NBRROUTERID     NBRIPADDR       PRIO_STATE    RTXQLEN PERMANENCE
--------------------------------------------------------------------------------
10.1.3.10       10.2.1.2        10.1.3.12       0    Full     0       Dynamic
10.1.3.10       10.2.1.1        10.1.3.11       0    Full     0       Dynamic
10.1.3.10       10.1.1.1        10.1.3.9        0    Full     0       Dynamic
10.1.3.2        10.2.1.1        10.1.3.3        0    TwoWay   0       Dynamic
10.1.3.2        10.2.1.2        10.1.3.4        0    TwoWay   0       Dynamic
10.1.3.2        10.1.1.1        10.1.3.1        100  Full     0       Dynamic
```

8000-3:

```
================================================================================
                          Ospf Neighbors
================================================================================
INTERFACE       NBRROUTERID     NBRIPADDR       PRIO_STATE    RTXQLEN PERMANENCE
--------------------------------------------------------------------------------
```

```
10.1.3.11       10.2.1.2        10.1.3.12       0    TwoWay   0       Dynamic
10.1.3.11       10.1.1.2        10.1.3.10       100  Full     0       Dynamic
10.1.3.11       10.1.1.1        10.1.3.9        0    TwoWay   0       Dynamic
10.1.3.3        10.1.1.1        10.1.3.1        100  Full     0       Dynamic
10.1.3.3        10.2.1.2        10.1.3.4        0    TwoWay   0       Dynamic
10.1.3.3        10.1.1.2        10.1.3.2        0    TwoWay   0       Dynamic
```

8000-4:

```
================================================================================
                        Ospf Neighbors
================================================================================
INTERFACE       NBRROUTERID     NBRIPADDR       PRIO_STATE    RTXQLEN PERMANENCE
--------------------------------------------------------------------------------
10.1.3.12       10.1.1.2        10.1.3.10       100  Full     0       Dynamic
10.1.3.12       10.2.1.1        10.1.3.11       0    TwoWay   0       Dynamic
10.1.3.12       10.1.1.1        10.1.3.9        0    TwoWay   0       Dynamic
10.1.3.4        10.2.1.1        10.1.3.3        0    TwoWay   0       Dynamic
10.1.3.4        10.1.1.1        10.1.3.1        100  Full     0       Dynamic
10.1.3.4        10.1.1.2        10.1.3.2        0    TwoWay   0       Dynamic
```

On each ERS 8800/8600 in the switch cluster verify the following information:

Option	Verify
INTERFACE	The local IP address should be displayed as follows: • 8000-1: ***10.1.3.1*** & ***10.1.3.9*** • 8000-2: ***10.1.3.2*** & ***10.1.3.10*** • 8000-3: ***10.1.3.3*** & ***10.1.3.11*** • 8000-4: ***10.1.3.4*** & ***10.1.3.12***
NBRIPADDR PRIO_STATE	Verify that switches 8000-2, 8000-3, 8000-4 peering state is displayed as ***Full*** pointing to 8000-1 VLAN 3's NBRIPADDR of 10.1.3.1 as it is the OSPF DR for VLAN 3. Verify that switches 8000-1, 8000-3, 8000-4 peering state is displayed as ***Full*** pointing to 8000-2 VLAN 30's NBRIPADDR of 10.1.3.10 as it is the OSPF DR for VLAN 30.

3.4.2.2 RSMLT Operations

Verify that the RSMLT instance is configured correctly and is functioning by issuing the following command:

show ip rsmlt info

Results:

8000-1:

```
================================================================================
                          Ip Rsmlt Local Info
================================================================================

VID    IP              MAC               ADMIN    OPER   HDTMR   HUTMR
--------------------------------------------------------------------------------
3      10.1.3.1        00:01:81:28:86:13 Enable   Up     60      180
30     10.1.3.9        00:01:81:28:86:14 Enable   Up     60      180

VID    SMLT ID                  SLT ID
--------------------------------------------------------------------------------
3        2
30       2
================================================================================
                          Ip Rsmlt Peer Info
================================================================================

VID    IP              MAC               ADMIN    OPER   HDTMR   HUTMR
--------------------------------------------------------------------------------
3      10.1.3.2        00:e0:7b:bc:22:01 Enable   Up     60      180
30     10.1.3.10       00:e0:7b:bc:22:14 Enable   Up     60      180

VID    HDT REMAIN   HUT REMAIN   SMLT ID                  SLT ID
--------------------------------------------------------------------------------
3      60           180          2
30     60           180          2
```

On each ERS 8800/8600 in the switch cluster verify the following information:

Option	Verify
VID	The VID should be displayed as ***3*** and ***30*** for SMLT 2.
IP	Verify the correct IP address for each switch: • 8000-1: ***10.1.3.1*** & ***10.1.3.9*** • 8000-2: ***10.1.3.2*** & ***10.1.3.10*** • 8000-3: ***10.1.3.3*** & ***10.1.3.11*** • 8000-4: ***10.1.3.4*** & ***10.1.3.12***
ADMIN	Verify that the RSMLT Admin is ***Enabled*** on both clusters. If not, there is a configuration error.
OPER	Verify that the RSMLT operation is ***Up*** on both clusters.
HUTMR HDRMR	Verify that the RSMLT holdup and holddown timer is set to ***60*** and ***180*** respectively on both clusters. If not, there is a configuration error.
SMLT ID	Verify the SMLT ID is showing ***2***.

Ip Rsmlt Peer Info	Verify the RSMLT Peer is showing:
	• 8000-1:
	  ○ VLAN 3: SMLT ***2***, IP ***10.1.3.2***
	  ○ VLAN 30: SMLT ***2***, IP ***10.1.3.10***
	• 8000-2:
	  ○ VLAN 30, SMLT ***2***, IP ***10.1.3.1***
	  ○ VLAN 30, SMLT ***2***, IP ***10.1.3.9***
	• 8000-3:
	  ○ VLAN 3, SMLT ***2***, IP ***10.1.3.4***
	  ○ VLAN 30: SMLT ***2***, IP ***10.1.3.12***
	• 8000-4:
	  ○ VLAN 3, SMLT ***2***, IP ***10.1.3.3***
	  ○ VLAN 30: SMLT ***2***, IP ***10.1.3.11***

3.4.2.3 CLIP Address

Verify that all the switches in the RSMLT core are peered:

show ip circuitless-ip-int info

Results:

8000-1:

```
================================================================================
                        Circuitless Ip Interface
================================================================================
INTERFACE    IP_ADDRESS      NET_MASK        OSPF_STATUS  PIM_STATUS    AREA_ID
ID
--------------------------------------------------------------------------------
1            10.1.1.1        255.255.255.255 enable       enable        0.0.0.0
```

On each ERS 8800/8600 in the switch cluster verify the following information:

Option	Verify
INTERFACE	The CLIP IP address should be displayed as follows: • 8000-1: ***10.1.1.1*** • 8000-2: ***10.1.1.2*** • 8000-3: ***10.2.1.1*** • 8000-4: ***10.2.1.2***

4. Configuring Ping Snoop to Verify Traffic Flow

Ping snoop is a feature that can be used to verify correct traffic flow behavior in an SMLT network. This is especially useful when determining traffic patterns during a link failure exercise.

This feature displays the path that IP traffic takes over an MLT or SMLT path. Ping snoop works by enabling a filter that copies ICMP messages to the CPU. The CPU then monitors the ICMP stream. The console displays the port that is used for each IP traffic flow, from source to destination station. There is no mechanism to prevent line rate ICMP traffic from going to the CPU as a result of enabling ping snoop.

You create a ping snoop filter by specifying a source and destination IP address. Then, you specify the ports on which you want to enable ping snoop. Only one ping snoop filter is supported on a port. If an ICMP request is received on any of the added ports, the source and destination IP address and the port on which the packet was received will be displayed on the management console.

Please note the Ping snoop is only supported on the ERS 8800/8600 and ERS 8300.

Note that the new hashing for IP traffic between a given source and destination IP address will be different for TCP/UDP packets and ICMP packets. Therefore the use of ping, in conjunction with the ERS 8800/8600 ping-snoop feature, is no longer always reliable to determine the hashed path taken by IP TCP/UDP traffic, if that hashing is performed by an R-module ingress port. If the hashing is performed by a legacy module, then ping-snoop functions just as before with other code releases.

4.1 Configuration Example – ERS 8600/8800 MLT Hashing

4.1.1 Ping Snoop and Legacy Modules

For legacy modules, ping snoop uses one of the available 8 global filters (0-7) for the classic modules, thus one global filter must be available before ping snoop can be used. Ping snoop can only be configured using CLI. If you use telnet to access the CLI, then you must enable log message to the screen if you wish to view the ping snoop message real time.

4.1.1.1 Configuration Example - Legacy Module Ping Snoop

The following example demonstrates how to enable ping snoop filter to capture ICMP packets from source or destination IP network 30.30.30.0/24 via ports 1/47 and 2/1. For legacy modules, legacy filters must be used.

ERS 8000: Step 1 – Create Ping Snoop Filter

```
8000-1:5# config diag ping-snoop create src-ip 30.30.30.0/24 dst-ip 30.30.30.0/24
```

ERS 8000: Step 2 – Add port members to filter

```
8000-1:5# config diag ping-snoop add-ports 1/47,2/1
```

ERS 8000: Step 3 – Enable Ping Snoop

```
8000-1:5# config diag ping-snoop enable true
```

4.1.1.2 Verify Operations – Ping Snoop Legacy Modules

You need to look at the log messages to see the results from Ping Snoop

Verify operations:

```
config log screen on
```

or

```
show log file tail
```

Results:

```
8000-1:5# CPP Task=tMainTask CPU6 [01/24/06 12:49:12] CPU INFO ICMP Reply received on
port 1/47 withSrc=30.30.30.10 Dst=30.30.30.3
8000-1:5# CPP Task=tMainTask CPU6 [01/24/06 12:49:12] CPU INFO ICMP Reply received on
port 1/47 withSrc=30.30.30.10 Dst=30.30.30.3
8000-1:5# CPP Task=tMainTask CPU6 [01/24/06 12:49:13] CPU INFO ICMP Reply
received on port 1/47 withSrc=30.30.30.10 Dst=30.30.30.3
```

By adding all the MLT/SMLT ports to this filter on a per switch basis, the user can determine the exact path traffic is taking.

4.1.1.3 Configuration Example – R-module Ping Snoop

The following example demonstrates to monitor both ICMP message type echo-reply and echo-request on port 4/9 with a source IP address range of 10.1.25.0/24 to a destination IP range of 10.0.0.0/8.

To view the pre-assigned ACL's:

```
8000-1:5#show filter acl
================================================================================
                                Vlan ACL Table
================================================================================
Acl  Type    AclName             State    Act  # of Global             Default Vlan
Id                                        Id   ACEs Action             Action  Id
--------------------------------------------------------------------------------

Displayed 0 of 0 Entries


================================================================================
                                Port ACL Table
================================================================================
Acl  Type    AclName             State    Act  # of Global             Default Port
Id                                        Id   ACEs Action             Action
--------------------------------------------------------------------------------
4082 Ingress IP Media filters ACL disabled 4082 16   none               permit
4096 Ingress IP Ping-Snoop ACL    disabled 4096 0    none               permit
```

ERS 8000: Step 1 – ACL 4096 and add port 4/9

```
8000-1:5# config filter acl 4096 port add 4/9
8000-1:5# config filter acl 4096 enable
```

ACLI

```
8000-1:5(config)#filter acl port 4096 4/9
8000-1:5(config)#filter acl 4096 enable
```

ERS 8000: Step 2 – Add ACE's to ACL 4096

```
ERS8610-1:5# config filter acl 4096 ace 1 create name echo_reply
ERS8610-1:5# config filter acl 4096 ace 1 ip src-ip eq 10.1.25.0/24
ERS8610-1:5# config filter acl 4096 ace 1 ip dst-ip eq 10.0.0.0/8
ERS8610-1:5# config filter acl 4096 ace 1 protocol icmp-msg-type eq echoreply
ERS8610-1:5# config filter acl 4096 ace 1 enable
ERS8610-1:5# config filter acl 4096 ace 2 create name echo_request
ERS8610-1:5# config filter acl 4096 ace 2 ip src-ip eq 10.1.25.0/24
ERS8610-1:5# config filter acl 4096 ace 2 ip dst-ip eq 10.0.0.0/8
ERS8610-1:5# config filter acl 4096 ace 2 protocol icmp-msg-type eq echo-request
ERS8610-1:5# config filter acl 4096 ace 2 enable
```

ACLI

```
8000-1:5(config)#filter acl ace 4096 1 name echo_reply
8000-1:5(config)#filter acl ace ip 4096 1 src-ip eq 10.1.25.0/24
8000-1:5(config)#filter acl ace ip 4096 1 dst-ip eq 10.0.0.0/8
8000-1:5(config)#filter acl ace protocol 4096 1 icmp-msg-type eq echoreply
8000-1:5(config)#filter acl ace 4096 1 enable
8000-1:5(config)#filter acl ace 4096 2 name echo_request
8000-1:5(config)#filter acl ace ip 4096 2 src-ip eq 10.1.25.0/24
8000-1:5(config)#filter acl ace ip 4096 2 dst-ip eq 10.0.0.0/8
8000-1:5(config)#filter acl ace protocol 4096 2 icmp-msg-type eq echo-request
8000-1:5(config)#filter acl ace 4096 2 enable
```

4.1.1.4 Enable log screen

```
ERS8610-B:5# config log screen on
```

4.1.1.5 Verify Operations – Ping Snoop R-modules

You need to look at the log messages to see the results from Ping Snoop.

Verify operations:

config log screen on

or

show log file tail

Results:

```
ERS8610-B:5# CPP Task=tMainTask CPU5 [07/17/06 16:09:40] CPU INFO ICMP Request
received on port 4/9 with Src=10.1.25.100 Dst=10.1.3.3

ERS8610-B:5# CPP Task=tMainTask CPU5 [07/17/06 16:09:41] CPU INFO ICMP Request
received on port 4/9 with Src=10.1.25.100 Dst=10.1.3.3

ERS8610-B:5# CPP Task=tMainTask CPU5 [07/17/06 16:09:42] CPU INFO ICMP Request
received on port 4/9 with Src=10.1.25.100 Dst=10.1.3.3

ERS8610-B:5# ping 10.1.25.100

CPP Task=tMainTask CPU5 [07/17/06 16:10:11] CPU INFO ICMP Reply received on port 4/9
with Src=10.1.25.100 Dst=10.1.25.3

ERS8610-B:5# 10.1.25.100 is alive
```

4.1.2 MLT Port Index calculation

The port index command can be used to calculate the port used for a specific MLT number. This can be configured by using the following command where the src-port and dst-port are optional:

- ERS8600:6# ***config sys set hash-calc getmltindex traffic-type <non-ip|ipv4|ipv6> dest-val <destination address> src-val <source address> mltID <1-256> src-port <0 – 65535> dst-port <0 – 65535>***

4.1.2.1 Configuration Example

The following example demonstrates to find the index from a source IP address of 10.1.25.1 to a destination IP address of 10.2.3.5 for MLT 2.

ERS 8000:

```
8000-2:6# config sys set hash-calc getmltindex traffic-type ipv4 dest-val
10.2.3.5 src-val 10.1.25.1 mltID 2
```

Results:

```
If the ingress port is on R-module card[2,4,7], the traffic will egress out of port:
4/8 for mltid: 2

If the ingress port is on non-Rmodule card[3], the traffic will egress out of port:
4/8 for mltid: 2
```

4.1.3 Stackable Switch MLT Port Index calculation

The port index command can be used to calculate the port used for a specific MLT number. This can be configured by using the following command where the src-port and dst-port are optional:

When MLT load-balancing is set to basic mode:

- 7024XLS#***show mlt hash-calc <1– 32> dest-mac <destination mac> src-mac <source mac> vlan <1-4096> ethertype <0x0600-0xffff> src-port <unit/port>***

When MLT load-balancing is set to advance mode:

- 7024XLS#***show mlt hash-calc <1– 32> dest-ip <destination address> src-ip <source address> tcp-udp-dport <0-65535> tcp-udp-sport <0-65535>***

4.1.3.1 Configuration Example

The following example demonstrates to find the index from a source IP address of 10.1.25.1 to a destination IP address of 10.2.3.5 for MLT 2.

VSP 7000, ERS 5000, or ERS 4000: Assuming MLT is configured in basic mode using MLT 3 where the source port is 1/4. MLT 3 is made up of ports 1/23 and 1/24.

```
7024XLS#show mlt hash-calc 3 dest-mac 0000.5e00.012c src-mac f0de.f13c.321b
vlan 1000 ethertype 0x800 src-port 1/4
```

Results:

```
Hash Calc:  23
```

4.2 VSP 9000 MLT Port Index calculation

The port index command can be used to calculate the port used for a specific MLT number. This can be configured by using the following command where the src-port and dst-port are optional:

- VSP-9012:1# ***hash-calc getmltindex traffic-type <non-ip|ipv4> dest-val <destination address> src-val <source address> mltID <1-512> src-port <0 – 65535> dst-port <0 – 65535>***

4.2.1.1 Configuration Example

The following example demonstrates to find the index from a source IP address of 10.1.25.1 to a destination IP address of 10.2.3.5 for MLT 2.

VSP 9000:

```
VSP-9012:1# hash-calc getmltindex traffic-type ipv4 dest-val 10.2.3.5 src-val
10.1.25.1 mltID 2
```

Results:

```
Traffic will egress port 4/8 for this flow for MltId 2.
```

5. Reference Documentation

Document Title	Publication Number	Description
Switch Clustering Best Practises	NN48500-584	
Super Large Campus Technical Solution Guide	NN48500-609	
Large Campus Technical Solution Guide	NN48500-575	
Medium Campus Technical Solution Guide	NN48500-574	
Small Campus Technical Solution Guide	NN48500-573	