# AVAYA

# Configuration — VLANs, Spanning Tree, and Link Aggregation
# Avaya Ethernet Routing Switch 5000 Series

Comments? infodev@avaya.com

company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

**Avaya Toll Fraud intervention**

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

**Trademarks**

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation 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 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. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

**Downloading Documentation**

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

**Contact Avaya Support**

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

# Contents

# Chapter 1: New in this Release

The following sections detail what's new in *Avaya Ethernet Routing Switch 5000 Configuration — VLANs, Spanning Tree and Link Aggregation,* NN47200-502 Release 6.2.

- Features on page 13
- Other changes on page 15

# Features

See the following sections for information about feature changes:

- Split Multi-link Trunk consistency with the Ethernet Routing Switch 8800/8600 on page 13
- Virtual Local Area Networks Scaling on page 13
- Link Aggregation Control Protocol over SMLT on page 14
- SMLT with Routing protocol support on page 14
- Autodetection and Autoconfiguration Uplink Enhancements on page 14

## Split Multi-link Trunk consistency with the Ethernet Routing Switch 8800/8600

In Release 6.2, Split Multi-link Trunk (SMLT) configuration is enhanced to more closely reflect the Ethernet Routing Switch 8800/8600 configuration. For more information, see SMLT consistency with the Ethernet Routing Switch 8800/8600 on page 114.

## Virtual Local Area Networks Scaling

Release 6.2 supports 1 024 (1K) concurrent Virtual Local Area Networks (VLAN). This feature allows you to extend the number of VLANs supported by a device up to 4k. The scaling limits for each platform can be determined based on the business need and available system resources. All the VLAN configured applications can work properly with the maximum configured of VLANs. The standard scaling limit is 256, 512, 1024, or 4094 VLANs. In Ethernet Routing Switch 5000 Series Release 6.2, the target scaling number is up to 4,096 concurrent VLAN IDs with the scaling capacity limited to 1,024 simultaneous VLANs. It supports up to a maximum of 1,024 VLANs.

**Important:**

No other capabilities extension for L2/L3 are enhanced as a result of VLAN scaling.

For more information, see Virtual Local Area Networks on page 19.

# Link Aggregation Control Protocol over SMLT

Link Aggregation Control Protocol (LACP) over SMLT improves handling in fail-over situations, for example, when a stack breaks, and improves trunking resilience. For more information, see.

- Link Aggregation Control Protocol over SMLT on page 114
- Link Aggregation Control Protocol over SMLT using the ACLI on page 187
- LACP over SMLT configuration example on page 295

# SMLT with Routing protocol support

This release improves route distribution across an SMLT by supporting Open Shortest Path First (OSPF) to distribute routes across the SMLT/SLT network. For more information, see SMLT with Routing protocol support on page 114.

# Autodetection and Autoconfiguration Uplink Enhancements

Autodetection and Autoconfiguration ( ADAC) Enhancements provide increased flexibility in deployments that use ADAC as follows:

- expanded support for up to 8 ADAC uplinks and 8 call-server links - individual ports or any combination of MLT, DMLT or LAG - per switch or stack
- the ability to change the non-ADAC VLANs on a port without disabling ADAC

For more information, see:

- ADAC and stacking on page 136
- Dynamic VLAN auto-configuration on page 135
- Configuring global ADAC settings on page 203
- Configuring ADAC settings on page 289

# Other changes

See the following sections for information about changes that are not feature-related:

# Enterprise Device Manager

Enterprise Device Manager (EDM) replaces both the Java-based Device Manager and Web-based management user interfaces. EDM is an embedded element management and configuration application for Ethernet Routing Switch 5000 Series switches. EDM provides a Web-based graphical user interface through a standard web browser for the convenience of full configuration and management on the switch, and retains the look and feel of Device Manager. For more information, see:

- Configuring VLANs using Enterprise Device Manager on page 215
- Configuring Spanning Tree using Enterprise Device Manager on page 231
- Configuring MLT using Enterprise Device Manager on page 263
- Configuring LACP and VLACP using Enterprise Device Manager on page 275
- Configuring SLPP using Enterprise Device Manager on page 283
- Configuring ADAC using Enterprise Device Manager on page 289
- Configuring ADAC using Enterprise Device Manager on page 289

## Multiple Port Configuration

Among the many functions available in EDM, you can configure port-specific features for a single port, a group of ports, or all ports. Multiple Port Configuration appears as a pane in the work area wherever this function is available. By default the pane appears and you can close and open it with a click of the task bar. For more information about EDM, see *Ethernet Routing Switch 5000 Series Fundamentals*, NN47200-104.

# Chapter 2:  Introduction

This document provides information you need to configure VLANs, Spanning Tree and Link Aggregation for the Ethernet Routing Switch 5000 Series.

## ACLI command modes

ACLI provides the following command modes:

- User EXEC
- Privileged EXEC
- Global Configuration
- Interface Configuration
- Router Configuration

Mode access is determined by access permission levels and password protection.

If no password is set, you can enter ACLI in User EXEC mode and use the **enable** command to move to the next level (Privileged EXEC mode). However, if you have read-only access, you cannot progress beyond User EXEC mode, the default mode. If you have read-write access you can progress from the default mode through all of the available modes.

With sufficient permission, you can use the rules in the following table to move between the command modes.

| Command mode and sample prompt | Entrance commands | Exit commands |
|---|---|---|
| User EXEC<br><br>`5650TD>` | No entrance command, default mode | `exit`<br>or<br>`logout` |
| Privileged EXEC<br><br>`5650TD#` | `enable` | `exit`<br>or<br>`logout` |
| Global Configuration<br><br>`5650TD(config)#` | `configure` | To return to Privileged EXEC mode, enter:<br>`end`<br>or<br>`exit` |

| Command mode and sample prompt | Entrance commands | Exit commands |
|---|---|---|
| | | To exit ACLI completely, enter:<br>`logout` |
| Interface Configuration<br><br>`5650TD(config-if)#` | From Global Configuration mode: To configure a port, enter:<br>`interface fastethernet <port number>`<br>To configure a VLAN, enter:<br>`interface vlan <vlan number>` | To return to Global Configuration mode, enter:<br>`exit`<br>To return to Privileged EXEC mode, enter:<br>`end`<br>To exit ACLI completely, enter:<br>`logout` |
| Router Configuration<br><br>`5650TD (config-router)#` | From Global Configuration mode, to configure OSPF, enter:<br>`router ospf`<br>To configure RIP, enter:<br>`router rip`<br>To configure VRRP, enter:<br>`router vrrp` | To return to Global Configuration mode, enter:<br>`exit`<br>To return to Privileged EXEC mode, enter:<br>`end`<br>To exit ACLI completely, enter:<br>`logout` |

See *Avaya Ethernet Routing Switch 5000 Series Fundamentals* , NN47200-104

# Chapter 3:  VLAN Fundamentals

## Virtual Local Area Networks

The Avaya Ethernet Routing Switch 5000 Series supports up to 1024 Virtual Local Area Networks (VLAN).

**Important:**

In Avaya Ethernet Routing Switch 5000 Series Release 6.2, the target scaling number is up to 4,096 concurrent VLAN IDs with the scaling capacity limited to 1,024 simultaneous VLANs. It supports up to a maximum of 1,024 VLANs.

Ports are grouped into broadcast domains by assigning them to the same VLAN. Frames received in one VLAN can only be forwarded within that VLAN, and multicast frames and unknown unicast frames are flooded only to ports in the same VLAN.

Setting up virtual LANs (VLAN) is a way to segment networks to increase network capacity and performance without changing the physical network topology (Figure 1: Port-based VLAN on page 19). With network segmentation, each switch port connects to a segment that is a single broadcast domain. When you configure a switch port to be a member of a VLAN, you add it to a group of ports (workgroup) that belong to one broadcast domain.
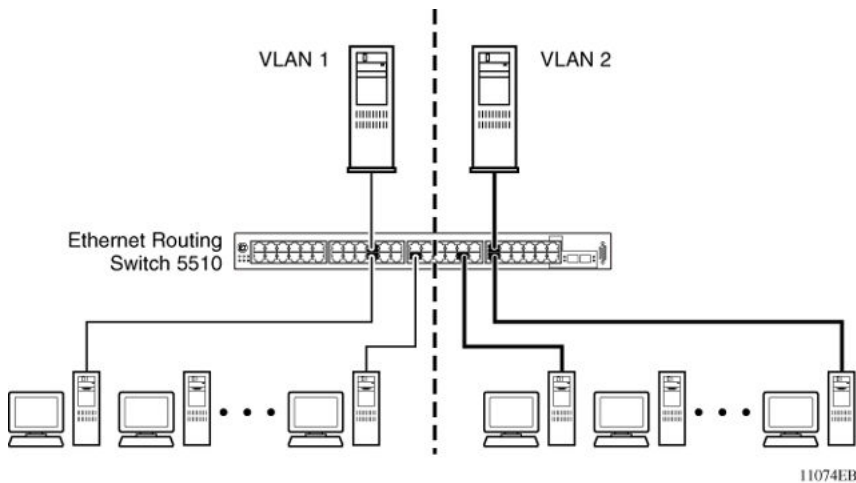


**Figure 1: Port-based VLAN**

The Avaya Ethernet Routing Switch 5000 Series allows ports to be assigned to VLANs using the Command Line Interface, or Device Manager. Different ports (and there devices) can be assigned to different broadcast domains. This feature provides network flexibility because

VLANs can be reassigned to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.

# IEEE 802.1Q Tagging

The Avaya Ethernet Routing Switch 5000 Series operates in accordance with the IEEE 802.1Q tagging rules. Important terms used with the 32-bit 802.1Q tagging feature are:

- VLAN identifier (VID) -- the 12-bit portion of the VLAN tag in the frame header that identifies an explicit VLAN. When other types of VLANs are enabled, this default value can be overridden by the values enabled in the management interfaces.

- Port VLAN identifier (PVID) -- a classification mechanism that associates a port with a specific VLAN. For example, a port with a PVID of 3 (PVID =3) assigns all untagged frames received on this port to VLAN 3.

- Tagged frame -- a frame that contains the 32-bit 802.1q field (VLAN tag). This field identifies the frame as belonging to a specific VLAN.

- Untagged frame -- a frame that does not carry any VLAN tagging information in the frame header.

- VLAN port members -- a group of ports that are all members of a particular VLAN. A port can be a member of one or more VLANs.

- Untagged member -- a port that has been configured as an untagged member of a specific VLAN. When an untagged frame exits the switch through an untagged member port, the frame header remains unchanged. When a tagged frame exits the switch through an untagged member port, the tag is stripped and the tagged frame is changed to an untagged frame.

- Tagged member -- a port that has been configured as a tagged member of a specific VLAN. When an untagged frame exits the switch through a tagged member port, the frame header is modified to include the 32-bit tag associated with the ingress port PVID. When a tagged frame exits the switch through a tagged member port, the frame header remains unchanged (original VID remains).

- User priority -- a three-bit field in the header of a tagged frame. The field is interpreted as a binary number, therefore has a value of 0 - 7. This field allows the tagged frame to carry the user-priority across bridged LANs where the individual LAN segments may be unable to signal priority information.

- Port priority -- the priority level assigned to untagged frames received on a port. This value becomes the user priority for the frame. Tagged packets get their user priority from the value contained in the 32-bit 802.1Q frame header.

- Unregistered packet -- a tagged frame that contains a VID where the receiving port is not a member of that VLAN.

- Filtering database identifier (FID) -- the specific filtering/forwarding database within the Avaya Ethernet Routing Switch 5000 Series switch that is assigned to each VLAN. Each

VLAN has its own filtering database, which is called independent VLAN learning (IVL). IVLs can have duplicate MAC addresses in different VLANs.

The default configuration settings for the Avaya Ethernet Routing Switch 5000 Series have all ports set as untagged members of VLAN 1 with all ports configured as PVID = 1. Every VLAN is assigned a unique VLAN identifier (VID) that distinguishes it from all other VLANs. In the default configuration example shown in Figure 2: Default VLAN Settings on page 21, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID =1). Untagged packets enter and leave the switch unchanged.
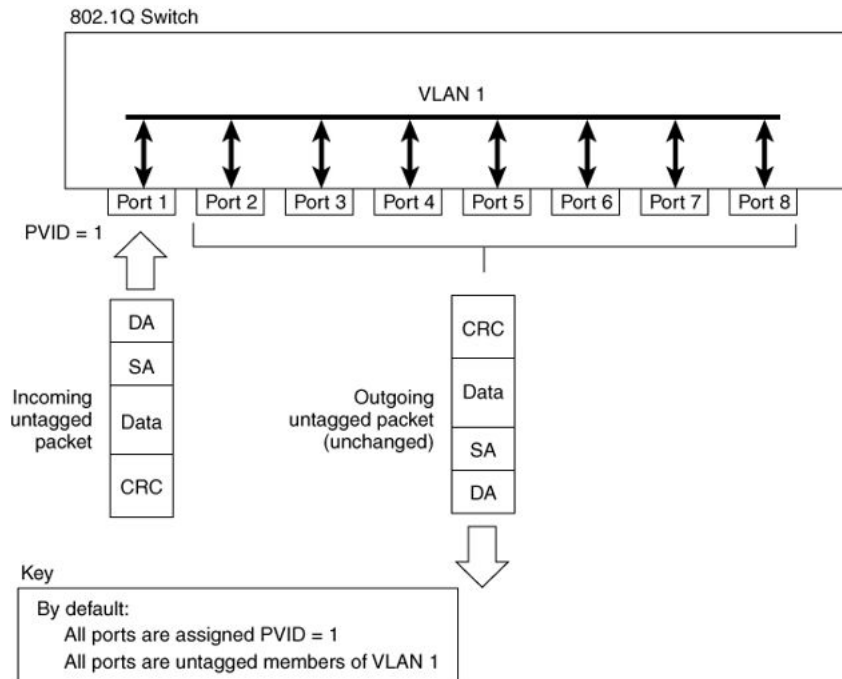


**Figure 2: Default VLAN Settings**

Switch ports can be configured to transmit frames tagged on some VLANs, and untagged on other VLANs.

When VLANs are configured, the egress tagging of each switch port can be configured as *Untag All*, *Untag PVID Only*, *Tag All* or *Tag PVID Only*.

In Figure 3: Port-based VLAN assignment on page 22, untagged incoming packets are assigned directly to VLAN 2 (PVID = 2). Port 5 is configured as a *tagged* member of VLAN 2, and port 7 is configured as an *untagged* member of VLAN 2.
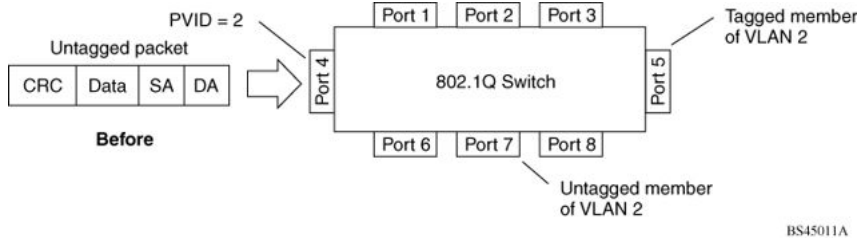
**Figure 3: Port-based VLAN assignment**

As shown in Figure 4: 802.1Q tagging (after port-based VLAN assignment) on page 22, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.
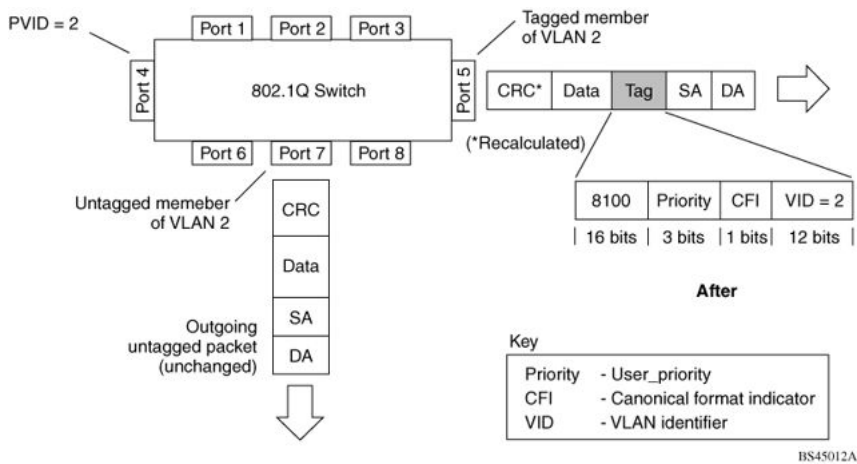


**Figure 4: 802.1Q tagging (after port-based VLAN assignment)**

In Figure 5: Protocol-based VLAN assignment on page 22, untagged incoming packets are assigned to VLAN 3 (protocol-based VLAN = 3, PVID = 2). Port 5 is configured as a tagged member of VLAN 3, and port 7 is configured as an untagged member of VLAN 3.
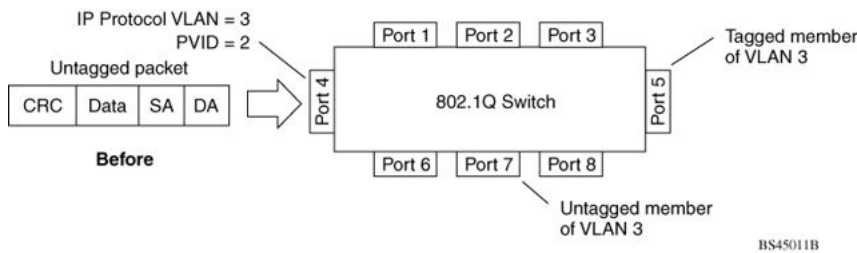


**Figure 5: Protocol-based VLAN assignment**

As shown in Figure 6: 802.1Q tagging (after protocol-based VLAN assignment) on page 23, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of VLAN 3. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of VLAN 3.
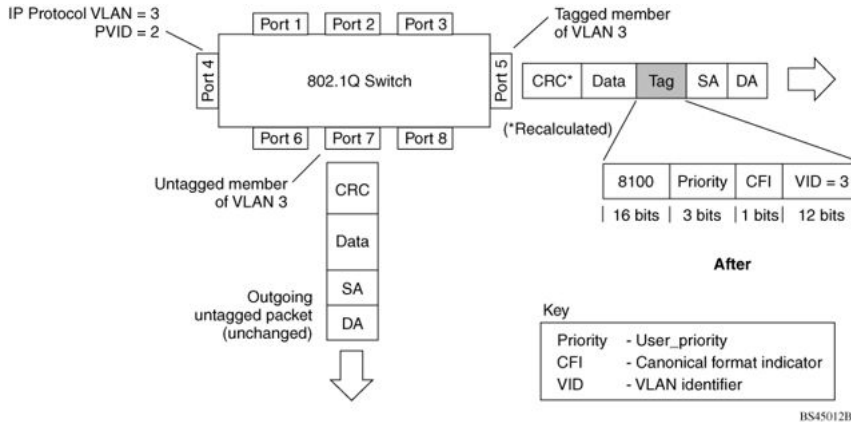
**Figure 6: 802.1Q tagging (after protocol-based VLAN assignment)**

In Figure 7: 802.1Q tag assignment on page 23, tagged incoming packets are assigned directly to VLAN 2 because of the tag assignment in the packet. Port 5 is configured as a tagged member of VLAN 2, and port 7 is configured as an untagged member of VLAN 2.
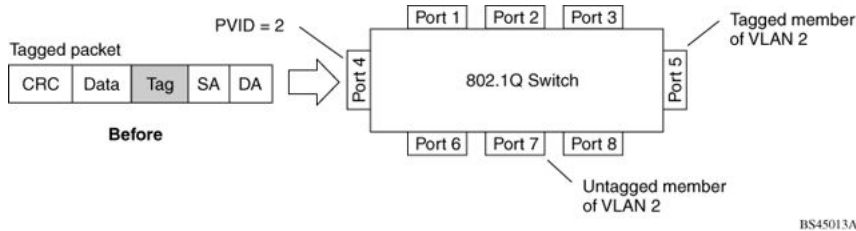


**Figure 7: 802.1Q tag assignment**

As shown in Figure 8: 802.1Q tagging (after 32-bit 802.1Q tag assignment) on page 24, the tagged packet remains unchanged as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. However, the tagged packet is stripped (untagged) as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.
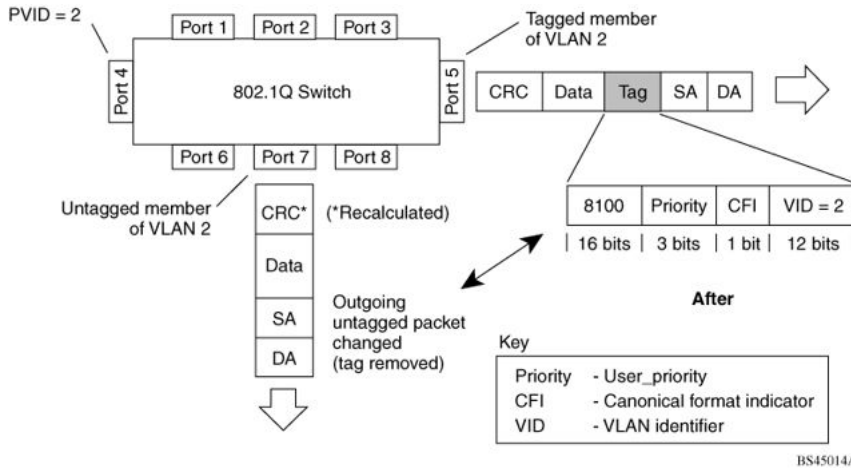
**Figure 8: 802.1Q tagging (after 32-bit 802.1Q tag assignment)**

In Figure 9: 802.1Q tag assignment on page 24, untagged incoming packets are assigned directly to VLAN 2. Port 5 is configured as a tagged member of VLAN 2, and port 7 is configured as an untagged member of VLAN 2.
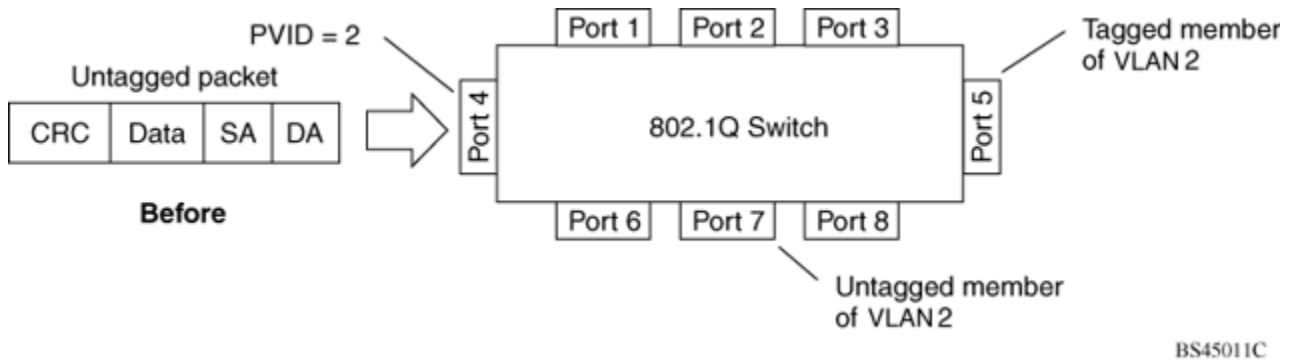


**Figure 9: 802.1Q tag assignment**

As shown in Figure 10: 802.1Q tagging (after 30-bit 802.1Q tag assignment) on page 25, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.
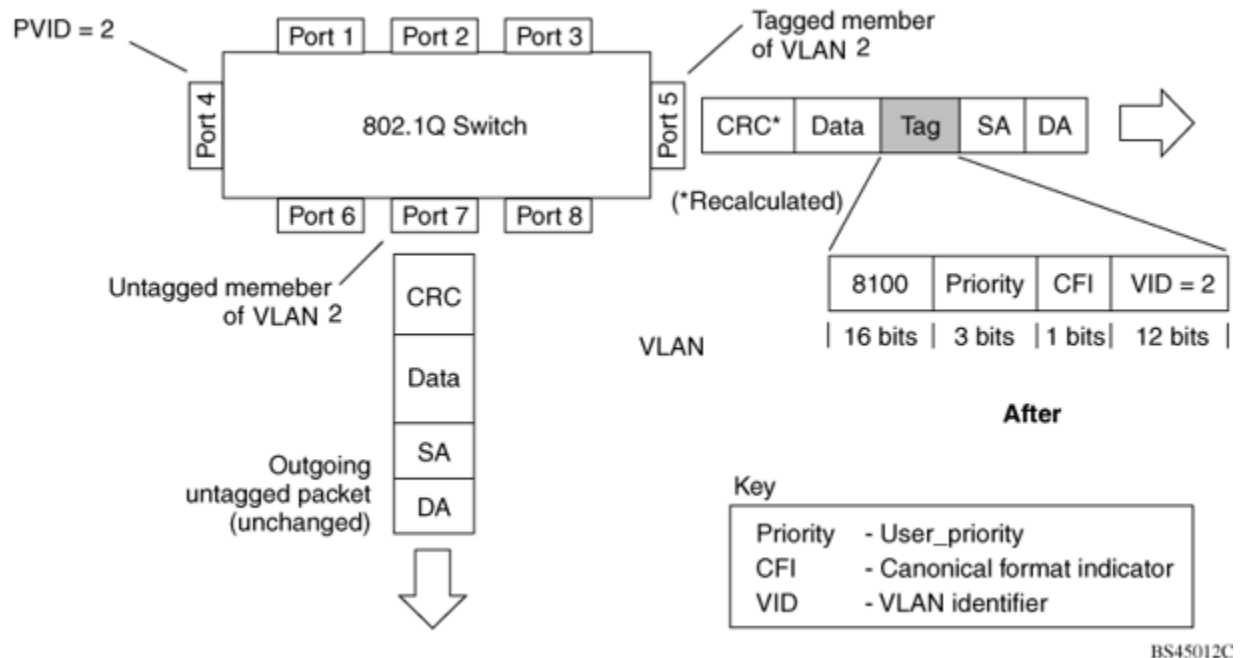
**Figure 10: 802.1Q tagging (after 30-bit 802.1Q tag assignment)**

# VLANs Spanning Multiple Switches

VLANs can be used to segment a network within a switch. When multiple switches are connected, you can connect users of one VLAN with users of that same VLAN in another switch. However, the configuration guidelines depend on whether both switches support 32-bit 802.1Q tagging.

With 32-bit 802.1Q tagging enabled on a port for a VLAN, all frames leaving the port for that VLAN are marked as belonging to that specific VLAN. Specific switch ports can be assigned as members of one or more VLANs that span multiple switches, without interfering with the Spanning Tree Protocol.

## VLANs spanning multiple 802.1Q tagged switches

Figure 11: VLANs spanning multiple 802.1Q tagged switches on page 26 shows VLANs spanning two Avaya Ethernet Routing Switch 5000 Series switches. The 32-bit 802.1Q tagging is enabled on S1, port 14 and on S2, port 13 for VLAN 1 and VLAN 2. Both ports are tagged members of VLAN 1 and VLAN 2.
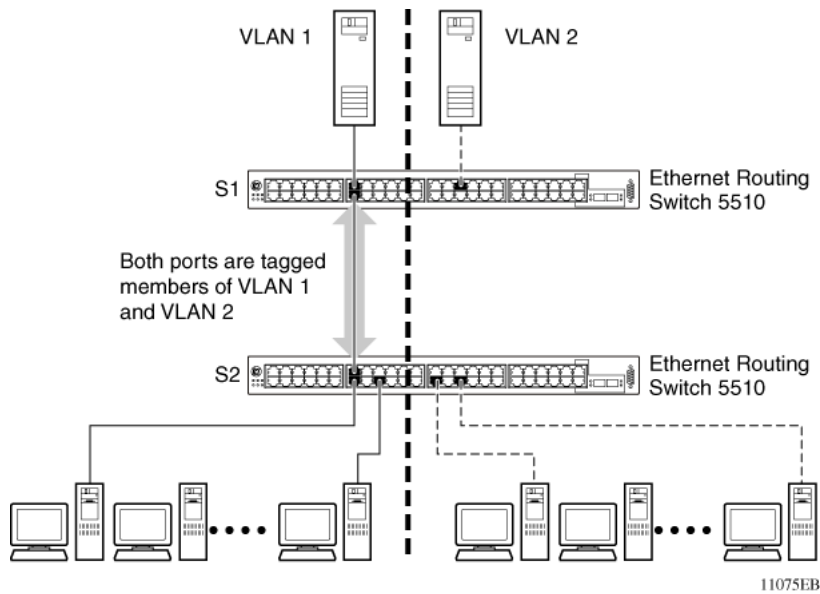
**Figure 11: VLANs spanning multiple 802.1Q tagged switches**

Because only one link exists between the two switches, the Spanning Tree Protocol (STP) treats this configuration as any other switch-to-switch connection. For this configuration to work properly, both switches must support the 32-bit 802.1Q tagging protocol.

## VLANS spanning multiple untagged switches

Figure 12: VLANs spanning multiple untagged switches on page 27 shows VLANs spanning multiple untagged switches. In this configuration, Switch S2 does not support 32-bit 802.1Q tagging and you must use a single switch port on each switch for each VLAN.

For this configuration to work properly, you must set spanning tree participation to Disabled (the STP is not supported across multiple LANs).
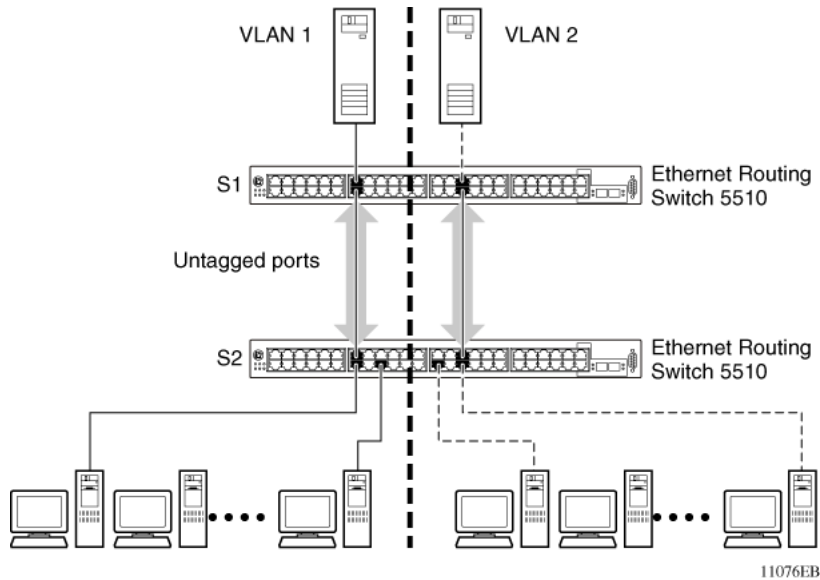
**Figure 12: VLANs spanning multiple untagged switches**

When the STP is enabled on these switches, only one link between the pair of switches forwards traffic. Because each port belongs to only one VLAN at a time, connectivity on the other VLAN is lost. Exercise care when configuring the switches to ensure that the VLAN configuration does not conflict with spanning tree configuration.

To connect multiple VLANs across switches with redundant links, you must disable the STP on all participating switch ports. Figure 13: Possible problems with VLANs and Spanning Tree Protocol on page 27 shows possible consequences of enabling the STP when using VLANs between untagged (non-802.1Q tagged) switches.
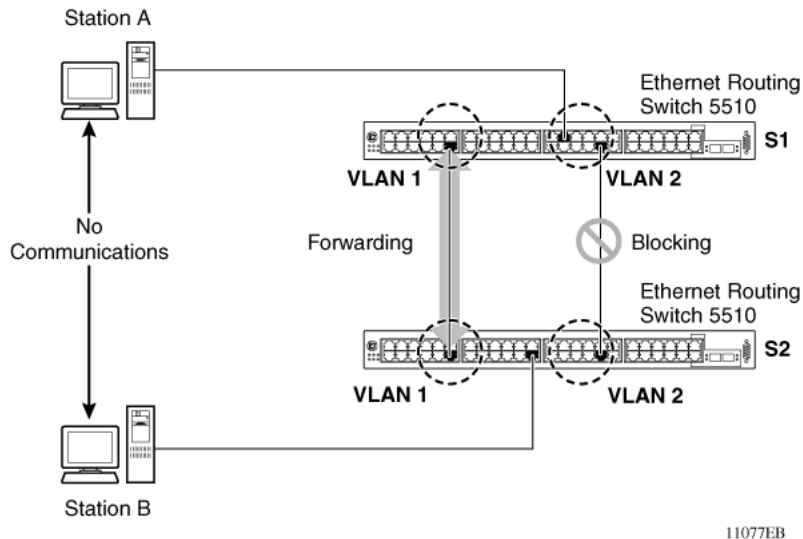


**Figure 13: Possible problems with VLANs and Spanning Tree Protocol**

As shown in Figure 13: Possible problems with VLANs and Spanning Tree Protocol on page 27, with STP enabled, only one connection between Switch S1 and Switch S2 is

forwarding at any time. Communications failure occurs between VLAN 2 of S1 and VLAN 2 of S2, blocking communications between Stations A and B.

The STP selects the link connecting VLAN 1 on Switches S1 and S2 as the forwarding link based on port speed, duplex-mode, and port priority. Because the other link connecting VLAN 2 is in Blocking mode, stations on VLAN 2 in Switch S1 cannot communicate with stations in VLAN 2 on Switch S2. With multiple links only one link will be forwarding.

## VLAN Summary

This section summarizes the VLAN examples discussed in the previous sections.

As shown in Figure 14: VLAN configuration spanning multiple switches on page 29, Switch S1 (Avaya Ethernet Routing Switch 5510) is configured with multiple VLANs:

   • Ports 17, 20, 25, and 26 are in VLAN 1.

   • Ports 16, 18, 19, 21, and 24 are in VLAN 2.

   • Port 22 is in VLAN 3.

Because S4 does not support 32-bit 802.1Q tagging, a single switch port on each switch must be used for each VLAN (see Figure 12: VLANs spanning multiple untagged switches on page 27).

The connection to S2 requires only one link between the switches because S1 and S2 are both Avaya Ethernet Routing Switch 5000 Series switches that support 32-bit 802.1Q tagging (see VLANs spanning multiple 802.1Q tagged switches on page 25).
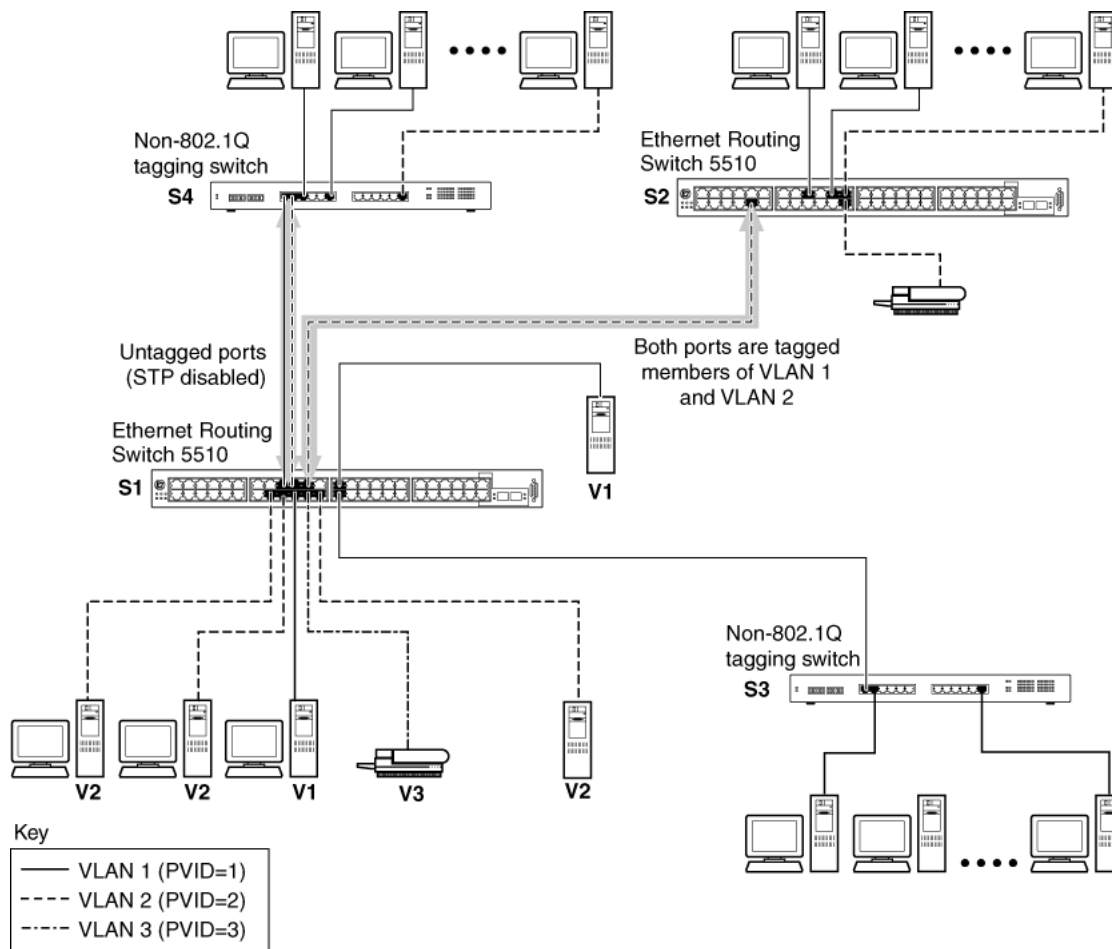
**Figure 14: VLAN configuration spanning multiple switches**

# VLAN Configuration Rules

VLANs operate according to specific configuration rules. When creating VLANs, consider the following rules that determine how the configured VLAN reacts in any network topology:

- If a port is a trunk group member, all trunk members are added or deleted from the VLAN.

- All ports involved in trunking must have the same VLAN configuration.

- VLANs are not dependent on Rate Limiting settings.

- If a port is an Internet Gateway Management Protocol (IGMP) member on any VLAN, and is removed from a VLAN, the port's IGMP membership is also removed.

- If you add a port to a different VLAN, and it is already configured as a static router port, you configure the port as an IGMP member on that specific VLAN.

# VLAN Configuration Control

VLAN Configuration Control (VCC) allows a switch administrator to control how VLANs are modified. VLAN Configuration Control is a superset of the existing AutoPVID functionality and incorporates this functionality for backwards compatibility. VLAN Configuration Control is globally applied to all VLANs on the switch.

VLAN Configuration Control offers four options for controlling VLAN modification:

1. **Strict** -- This option restricts the addition of an untagged port to a VLAN if it is already a member of another VLAN. To add an untagged port to a new VLAN, the switch administrator must remove the port from all other VLANs of which it is a member before adding it to the new VLAN. The PVID of the port is changed to the new VID to which it was added.

   > **Note:**
   >
   > Strict is the factory default setting.

2. **Automatic** -- This option automatically adds an untagged port to a new VLAN and automatically removes it from any previous VLAN membership. The PVID of the port is automatically changed to the VID of the VLAN it joins. Since the port is first added to the new VLAN and then removed from any previous membership, the Spanning Tree Group participation of the port will not be disabled as long as the VLANs involved are in the same Spanning Tree Group.

3. **AutoPVID** -- This option functions in the same manner as previous AutoPVID functionality. When an untagged port is added to a new VLAN, the port is added to the new VLAN and the PVID assigned to the new VID without removing it from any previous VLAN memberships. Using this option an untagged port can have membership in multiple VLANs.

4. **Flexible** -- This option functions in a similar manner to disabling AutoPVID functionality. When this option is used, an untagged port can belong to an unlimited number of VLANs. Any new additions of an untagged port to a new VLAN does not change the PVID of that port.

VLAN Configuration Control is only applied to ports with the tagging modes of **Untag All** and **Tag PVID Only**. Ports with the tagging modes of **Tag All** and **Untag PVID Only** are not governed by VLAN Configuration Control. Ports with the tagging modes of **Tag All** and **Untag PVID Only** can belong to multiple VLANs regardless of VLAN Configuration Control settings and must have their PVID manually changed.

# Multinetting

The Avaya Ethernet Routing Switch 5000 Series supports the definition and configuration of secondary interfaces on each VLAN. For more information about IP Multinetting, refer to *Avaya Ethernet Routing Switch 5000 Series Configuration - IP Routing Protocols*, NN47200-503.

# Chapter 4: Spanning Tree Protocol Fundamentals

## Spanning Tree Protocol groups

The Avaya Ethernet Routing Switch 5000 Series supports the Spanning Tree Protocol (STP) as defined in IEEE 802.1D. The Spanning Tree Protocol detects and eliminates logical loops in a bridged or switched network. When multiple paths exist, the spanning tree algorithm configures the network so that a bridge or switch uses only the most efficient path. If that path fails, the protocol automatically reconfigures the network to make another path become active, thus sustaining network operations.

The Avaya Ethernet Routing Switch 5000 Series supports multiple spanning tree groups (STG). The Avaya Ethernet Routing Switch 5000 Series supports a maximum of 8 STGs, either all in one stand-alone switch or across a stack. Multiple STGs provide multiple data paths, which can be used for load-balancing and redundancy. Load balancing is enabled between two switches using multiple STGs by configuring each path with a different VLAN and then assigning each VLAN to a separate STG. Each STG is independent. Each STG sends its own Bridge Protocol Data Units (BPDU), and each STG must be independently configured.

The STG, or bridge group, forms a loop-free topology that includes one or more virtual LANs (VLAN). The Avaya Ethernet Routing Switch 5000 Series supports multiple instances (8) of STGs running simultaneously.

The Avaya Ethernet Routing Switch 5000 Series supports a maximum of 256 VLANs. With a maximum of 8 STGs, on average, each STG can have 32 VLANs.

In the default configuration of the Avaya Ethernet Routing Switch 5000 Series, a single STG with the ID of 1 includes all ports on the switch. This STG is the default STG. Although ports can be added to or deleted from the default STG, the default STG (STG1) itself cannot be deleted from the system. Also you cannot delete the default VLAN (VLAN1) from STG1.

The tagging for the BPDUs from STG1, or the default STG, is user-configurable (as are tagging settings for all STGs). However, by default STG1 sends out only untagged BPDUs to operate with all devices that support only one instance of STP. (The default tagging of STG2 through STG8 is tagged.) The tagging setting for each STG is user-configurable.

> **Note:**
> If the STG is tagging a BPDU, the BPDU packet is tagged only on a tagged port. Also, ensure that the Filter Unregistered Frames option for the tagged port is disabled for this to function properly.

All other STGs, except the Default STG, must be created by the user. To become active, each STG must be enabled by the user after creation. Each STG is assigned an ID number from 2 to 8 (the Default STG is assigned the ID number 1). Ports or VLANs are assigned to an active STG. However, a port that is not a member of a VLAN is not allowed to join an STG.

When an STG is created, all ports belonging to any assigned VLAN are automatically added to the STG.

When an STG is no longer needed, disable and delete it. The procedure is to disable the STG, delete all VLAN and port memberships, and then delete the STG.

A unique multicast address can be configured for STGs 1 to 4.

> **Note:**
>
> If a unique multicast address for an STG is configured, each device in that STG must also be configured with the same spanning tree multicast address.

> **Note:**
>
> If Virtual LACP is enabled, the number of unique multicast addresses that can be configured for STGs is reduced to 3 (1 to 3).

## STG Configuration Guidelines

This section provides important information about configuring STGs:

- An STG must be created by following these steps:

    - Create the STG

    - Add the existing VLAN and port memberships

    - Enable the STG

- When a VLAN is created, that VLAN automatically belongs to STG 1, the default STG. If the VLAN is to be in another STG, it must be moved by assigning it to another STG.

- A newly created VLAN must be moved to an existing STG by following these steps:

    - Create the VLAN

    - Add the VLAN to an existing STG

- VLAN1 cannot be moved or deleted from STG1.

- You can create and add VLAN X directly to STG Y with `vlan create X type port Y` from ACLI if STG Y exists.

- VLANs must be contained within a single STG; a VLAN cannot span multiple STGs. By confining VLANs within a single STG, you avoid problems with spanning tree blocking ports and causing a loss of connectivity within the VLAN. When a VLAN spans multiple switches, the VLAN must be within the same spanning tree group (have the same STG ID) across all the switches.

- A port that is not a member of any VLAN cannot be added to any STG. The port must be added to a VLAN, and that VLAN added to the desired STG.

- Tagged ports can belong to more than one STG, but untagged ports can belong to only one STG.

- When a tagged port belongs to more than one STG, the egress BPDUs are tagged to distinguish the BPDUs of one STG from those of another STG.

- Because some STP-compliant devices do not support tagging, you can configure whether to send tagged or untagged BPDUs, even from tagged ports. The VLAN ID for the tagged BPDUs is 4000+STG ID.

- The default VLAN ID for tagged BPDUs is as follows:

    - 4001--STG1

    - 4002--STG2

    - 4003--STG3

    - 4004--STG4

    - 4005--STG5

    - 4006--STG6

    - 4007--STG7

    - 4008--STG8

- A VLAN ID can be selected for tagged BPDUs for each STG. Valid VLAN IDs are 1 to 4094.

- Tagged BPDUs cannot use the same VID as an active VLAN.

- An untagged port cannot span multiple STGs.

- When a port is removed from a VLAN that belongs to an STG, that port is also removed from the STG. However, if that port belongs to another VLAN in the same STG, the port remains in the STG.

- As an example, assume that port 1 belongs to VLAN1, and that VLAN1 belongs to STG1. When you remove port 1 from VLAN1, port 1 is also removed from STG1.

    However, if port 1 belongs to both VLAN1 and VLAN2 and both VLANs belong to STG1, removing port 1 from VLAN1 does not remove port 1 from STG1 because VLAN2 is still a member of STG1.

    An STG cannot be deleted until you disable it.

- A unique multicast address can be configured for STGs 1 to 4 only.

## Spanning Tree Fast Learning

Spanning Tree Fast Learning is an enhanced port mode supported by the Avaya Ethernet Routing Switch 5000 Series. If Spanning Tree Fast Learning is enabled on a port with no other

bridges, the port is brought up more quickly after a switch initialization or a spanning tree change. The port goes through the normal blocking and learning states before the forwarding state, but the hold times for these states is the bridge hello timer (2 seconds by default) instead of the bridge forward delay timer (15 seconds by default).

The port set with Fast Learning can forward data immediately, as soon as the switch learns that the port is enabled.

Fast Learning is intended for access ports in which only one device is connected to the switch (as in workstations with no other spanning tree devices). For these ports, it is not desirable to wait the usual 30 to 35 seconds for spanning tree initialization and bridge learning.

> **Note:**
>
> Use Spanning Tree Fast Learning with caution. This procedure is contrary to that specified in the IEEE 802.1D standard for Spanning Tree Protocol (STP) in which a port enters the blocking state after the initialization of the bridging device, or after a return from the disabled state when the port is enabled through configuration.

## STG port membership mode

IEEE 802.1D STGs support two different STP port membership modes: normal and auto. In the normal mode, when a port is assigned to VLAN X and VLAN X is in STP group Y, the port does not automatically become a member of STP group Y. In the auto mode, when a port is assigned to VLAN X and VLAN X is in STP group Y, the port automatically becomes a member of STP group Y.

To set the STG port membership mode using the ACLI, see Configuring STG port membership mode on page 157 and using DM, see Configuring STG Global properties on page 235.

## 802.1t path cost calculation

You can set the switch to calculate the STG path cost using either the IEEE 802.1d standard or the IEEE 802.1t standard. The 802.1t standard is a maintenance extension to the 802.1d standard.

To set the path cost calculation mode for the switch, see Configuring path cost calculation mode on page 157.

# Rapid Spanning Tree Protocol

The standard Spanning Tree implementation in 5000 Series switches is based on IEEE 802.1d, which is slow to respond to a topology change in the network (for example, a dysfunctional link in a network).

The Rapid Spanning Tree Protocol (RSTP or IEEE 802.1w) reduces recovery time after a network breakdown. It also maintains a backward compatibility with the IEEE 802.1d, which was the Spanning Tree implementation prior to RSTP. In certain configurations, the recovery time of RSTP can be reduced to less than 1 second. The backward compatibility is maintained by configuring a port to be in STP-compatible mode. A port operating in the STP-compatible mode transmits and receives only STP BPDUs and drops any RSTP BPDUs.

RSTP also reduces the amount of flooding in the network by enhancing the way the Topology Change Notification (TCN) packet is generated.

# Multiple Spanning Tree Protocol

You can use the Multiple Spanning Tree Protocol (MSTP or IEEE 802.1s) to configure multiple instances of RSTP on the same switch. Each RSTP instance can include one or more VLANs. The operation of the MSTP is similar to the current Avaya proprietary MSTP.

RSTP and MSTP enable the 5000 Series switch to achieve the following:

- Reduction of converging time from 30 seconds to less than 1 or 2 seconds when a topology change occurs in the network (that is, the port going up or down).

- Elimination of unnecessary flushing of the MAC database and flooding of traffic to the network with a new Topology Change mechanism.

- Backward compatibility with other switches that are running legacy 802.1d STP or Avaya MSTP (STP group 1 only).

- Under MSTP mode, simultaneous support of eight instances of RSTP. Instance 0 or CIST is the default group, which includes default VLAN 1. Instances 1 to 7 are called MSTIs 1-7.

- Ability to run Avaya MSTP, RSTP, or MSTP.

# Interoperability with legacy STP

RSTP provides a new parameter ForceVersion for backward compatibility with legacy STP. You can configure a port in either STP-compatible or RSTP mode.

- An STP compatible port transmits and receives only STP BPDUs. Any RSTP BPDU that the port receives in this mode is discarded.

- An RSTP compatible port transmits and receives only RSTP BPDUs. If an RSTP port receives an STP BPDU, it becomes an STP port. User intervention is required to bring this port back to RSTP mode. This process is called Port Protocol Migration.

# Differences in STP and RSTP port roles

RSTP is an enhanced version of STP. These two protocols have almost the same set of parameters.

Table 1: Differences in port roles for STP and RSTP on page 38 lists the differences in port roles for STP and RSTP. STP supports 2 port roles, while RSTP supports four port roles.

**Table 1: Differences in port roles for STP and RSTP**

| Port Role | STP | RSTP | Description |
|-----------|-----|------|-------------|
| Root | Yes | Yes | This port is receiving a better BPDU than its own and has the best path to reach the Root. Root port is in Forwarding state. |
| Designated | Yes | Yes | This port has the best BPDU on the segment. The Designated port is in Forwarding state. |
| Alternate | No | Yes | This port is receiving a better BPDU than its own and a Root port exists within the same switch. The Alternate port is in Discarding state. |
| Backup | No | Yes | This port is receiving a better BPDU than its own from another port within the same switch. The Backup port is in Discarding state. |

# Edge port

Edge port is a new parameter supported by RSTP. When a port is connected to a non-switch device such as a PC or a workstation, it must be configured as an Edge port for fast convergence. An active Edge port goes directly to Forwarding state without any delay. An Edge port becomes a non-Edge port if it receives a BPDU.

## Path cost values

RSTP and MSTP recommend new path cost values that support a wide range of link speeds. Table 2: Recommended path cost values on page 39 lists the recommended path cost values.

**Table 2: Recommended path cost values**

| Link speed | Recommended value |
|---|---|
| Less than or equal to 100 Kbit/s<br>1 Mbit/s<br>10 Mbit/s<br>100 Mbit/s | 200 000 000<br>20 000 000<br>2 000 000<br>200 000 |
| 1 Gbit/s<br>10 Gbit/s<br>100 Gbit/s | 20 000<br>2 000<br>200 |
| 1 Tbit/s<br>10 Tbit/s | 20<br>2 |

# Rapid convergent

In RSTP and MSTP, the environment root port or the designated port can ask its peer for permission to go to the Forwarding State. If the peer agrees, then the root port moves to the Forwarding State without any delay. This procedure is called the Negotiation Process.

RSTP and MSTP also allow information received on a port to be sent immediately if the port becomes dysfunctional, instead of waiting for the Maximum Age time.

The following example illustrates how an RSTP port state moves rapidly to Forwarding state without the risk of creating a loop in the network.

Switch A: ports 1 and 2 are in full duplex. Port 2 is an Edge port.

Switch B: ports 1, 2, and 3 are in full duplex. Port 2 is an Edge port.

Switch C: ports 1 and 2 are in full duplex. Port 2 is an Edge port.

Switch A is the Root.

## Negotiation Process

After powering up, all ports assume the role as Designated ports. All ports are in the Discarding state, except for Edge ports. Edge ports go directly to the Forwarding state without delay.

Switch A port 1 and switch B port 1 exchange BPDUs, and switch A knows that it is the Root and that switch A port 1 is the Designated port. Switch B learns that switch A has better priority.

Switch B port 1 becomes the Root port. Both switch A port 1 and switch B port 1 are still in the Discarding state.

Switch A starts the negotiation process by sending a BPDU with a proposal bit set.

Switch B receives the proposal BPDU and sets its non-Edge ports to the Discarding state. This operation is the sync process.

Switch B sends a BPDU with the agreement bit set to switch A.

Switch A sets port 1 to Forwarding, and switch B sets port 1 to Forwarding. PC 1 and PC 2 can talk to each other.

- The negotiation process now moves down to switch B port 3 and its partner port.

- PC 3 cannot talk to either PC 1 or PC 2 until the negotiation process between switch B and switch C is complete.
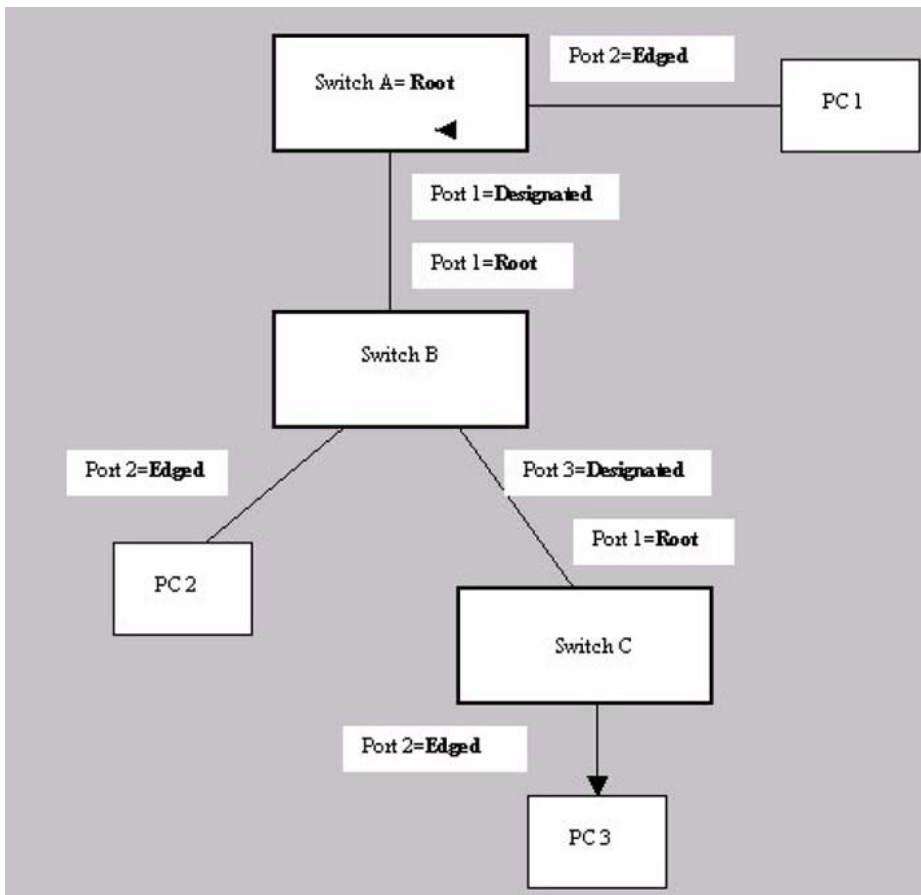


**Figure 15: Negotiation process**

The RSTP convergent time depends on how quickly the switch can exchange BPDUs during the negotiation process, and the number of switches in the network. For a 5000 Series switch, the convergent time depends on the hardware platform and the number of active applications running on the switch.

# Spanning Tree BPDU Filtering

The Ethernet Routing Switch 5000 Series supports the BPDU-Filtering feature for STPG, RSTP, and MSTP.

The Spanning Tree Protocol detects and eliminates logical loops in a bridged or switched network. Any bridge that participates in the spanning tree exchanges information with other bridges using configuration messages known as Bridge Protocol Data Units (BPDU). Based on the BPDU information exchange, the bridge with the lowest bridge ID becomes the root. This process is called the root selection process.

Typically, when a new bridge joins the spanning tree or an existing bridge leaves the spanning tree, the root selection process is repeated and a new root is selected.

The BPDU-Filtering feature allows the network administrator to achieve the following:

- Block an unwanted root selection process when an edge device, such as a laptop running Linux and enabled with STP, is added to the network. This prevents unknown devices from influencing an existing spanning tree topology.
- Block the flooding of BPDUs from an unknown device.

**Note:**

The STP BPDU-Filtering feature is not supported on Multi-Link Trunk (MLT) ports.

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 BPDU-Filtering 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 timer is disabled or the switch is reset before the timer expires, the port remains in the disabled state. Similarly, if a user disables BPDU-Filtering while the timer is running, the timer is stopped and that port stays in the disabled state. In this case, you must then manually enable the port to bring it back to the normal mode.

You can enable and disable the BPDU-Filtering feature on a per-port basis. The BPDU-Filtering timer is user-configurable for each port and has a valid range of between 10 and 65535 seconds. The port timer is disabled if it is configured as 0.

For details on configuring BPDU Filtering, refer to: Configuring STP BPDU Filtering using the ACLI on page 155.

# Configuring Spanning Tree using the Console Interface

The following sections provide instructions for configuring Spanning Tree in the three modes.

- Spanning Tree configuration in STPG mode on page 42
- Spanning Tree configuration in RSTP mode on page 50
- Spanning Tree configuration in MSTP mode on page 56

## Spanning Tree configuration in STPG mode

From the Spanning Tree Configuration Menu screen in the STPG mode (IEEE 802.1d), you can view Spanning Tree parameters and configure individual switch ports to participate in the Spanning Tree Algorithm.

To open the Spanning Tree Configuration Menu screen:

→    Choose **Spanning Tree Configuration** (or press **p**) from the main menu.

Table 3: Spanning Tree Configuration Menu options in STPG mode. on page 42 describes the **Spanning Tree Configuration Menu** options.

**Table 3: Spanning Tree Configuration Menu options in STPG mode.**

| Option | Description |
|---|---|
| **Spanning Tree Group Configuration** | Displays the Spanning Tree Group Configuration screen. (See Spanning Tree Group Configuration screen in STPG mode on page 43.) |
| **Spanning Tree Port Configuration** | Displays the Spanning Tree Port Configuration screen. (See Spanning Tree Port Configuration screen in STPG mode on page 45.) |
| **Display Spanning Tree Switch Settings** | Displays the Spanning Tree Switch Settings screen. (See Spanning Tree Switch Settings screen in STPG mode on page 47.) |
| **Display Spanning Tree VLAN Membership** | Displays the Spanning Tree VLAN Membership screen. |

## Spanning Tree Group Configuration screen in STPG mode

To open the Spanning Tree Group Configuration screen

Choose **Spanning Tree Group Configuration** (or press g) from the Spanning Tree Configuration Menu screen.

**Table 4: Spanning Tree Group Configuration parameters in STPG mode**

| Parameter | Description | |
|---|---|---|
| STP Mode | Shows the current STP operational mode for switch/stack. The modes available are:<br><br>• STPG (Avaya MSTP)<br><br>• RSTP (IEEE 802.1w)<br><br>• MSTP (IEEE 802.1s) | |
| Create STP Group | Creates a spanning tree group. | |
| | Default value | 1 |
| | Range | 1 to 8 |
| Delete STP Group | Deletes a spanning tree group. | |
| | Default value | Blank |
| | Range | Configured STP groups from 1 to 8 |
| Bridge Priority (in Hex) | Configures the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values. | |
| | Default value | 0x8000 |
| | Range | 0x0000 to 0xF000 |
| Bridge Hello Time | Configures the Hello Interval (the amount of time between transmissions of BPDUs) for the STP Group. This parameter takes effect only when this bridge becomes the root bridge.<br><br>**Note:**<br><br>Although you can set the Hello Interval for a bridge using bridge management software, after the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge Hello Interval parameter value. If any bridge | |

| Parameter | Description | |
|---|---|---|
| | becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network. | |
| | Default value | 2 seconds |
| | Range | 1 to 10 seconds |
| Bridge Max. Age Time | Configures the maximum age (in seconds) that a Hello message can attain before being discarded. This parameter takes effect only when the bridge becomes the root bridge. **Note:** If this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. | |
| | Default value | 20 seconds |
| | Range | 6 to 40 seconds |
| Bridge Forward Delay Time | Configures the Forward Delay parameter value for this bridge. This parameter takes effect only when this bridge becomes the root bridge. The Forward Delay parameter value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. **Note:** All bridges participating in the spanning tree network use the root bridge Forward Delay parameter value. | |
| | Default value | 15 seconds |
| | Range | 4 to 30 seconds |
| Add VLAN Membership | Adds a VLAN to the specified spanning tree group. | |
| | Default value | 1 |
| | Range | 1 to 4094. |
| Delete VLAN Membership | Deletes a VLAN from the specified spanning tree group. | |
| | Default value | Blank |
| | Range | Configured VLANs from 1 to 4094 |
| Tagged BPDU on tagged port | Specifies whether to send tagged or untagged BPDUs from a tagged port. | |

| Parameter | Description | |
|---|---|---|
| | Default value | STP Group 1: No; Other STP Groups: Yes |
| | Range | No or Yes |
| VID used for tagged BPDU | Specifies the VLAN ID (VID) for tagged BPDU for the specified spanning tree group. | |
| | Default value | 4001 to 4008 for STGs 1 through 8, respectively |
| | Range | 1 to 4094 |
| STP Multicast Address | Specifies the STP Multicast Address. | |
| | Default value | 01-80-C2-00-00-00 |
| STP Group State | Sets the STP Group to active or inactive. **Note**: You cannot set the default STG (STG 1) to Inactive. | |
| | Default value | Active for STG 1; Inactive for STGs 2 to 8 |
| | Range | Active or Inactive |

## Spanning Tree Port Configuration screen in STPG mode

With the Spanning Tree Port Configuration screen, you can configure individual switch ports or all switch ports to participate in the Spanning Tree.

**Note:**

If spanning tree participation of any trunk member is changed (enabled or disabled), the spanning tree participation of all members of that trunk is changed similarly.

Table 5: Spanning Tree Port Configuration parameters in STPG mode on page 45 describes the Spanning Tree Port Configuration screen fields.

**Table 5: Spanning Tree Port Configuration parameters in STPG mode**

| Field | Description | |
|---|---|---|
| **STP Group** | Specifies the number of the spanning tree group (STG) to view. To view another STG, type that STG ID number and press Enter, or press the spacebar on your keyboard to toggle the STP Group numbers. | |
| | Default value | 1 |
| | Range | Configured STP Groups from 1 to 8 |

| Field | Description | |
|---|---|---|
| **STP Mode** | Indicates the STP mode in which the switch or stack is operating. | |
| **Unit** | This field only appears if the switch is participating in a stack configuration. The field specifies the number of the unit to view. To view another unit, type its unit number and press Enter, or press the spacebar on your keyboard to toggle the unit numbers. | |
| **Port** | Indicates the switch port numbers that correspond to the field values in that row (for example, the field values in row 2 apply to switch port 2). | |
| | **Note:** | |
| | The values in the Switch row affect all switch ports and, when the switch is part of a stack, the values in the Stack row affect all ports in the entire stack. | |
| **Trunk** | The read-only data displayed in this column indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen. | |
| **Participation** | Configures any (or all) of ports on the switch for Spanning tree participation. When an individual port is a trunk member, changing this setting for one trunk member changes the setting for all members of that trunk. Consider how this can change your network topology before you change this setting. The Fast Learning parameter is the same as Normal Learning, except that the state transition timer is shortened to 2 seconds. | |
| | Default value | Normal Learning |
| | Range | Normal Learning, Fast Learning, Disabled |
| **Priority** | This read-only field is a bridge spanning tree parameter that prioritizes the lowest port path cost to the root. When one or more ports have the same path cost, STP selects the path with the highest priority (lowest numerical value). | |
| | Default value | 128 |
| | Range | 0 to 255 |
| **Path Cost** | This read-only field is a bridge spanning tree parameter that determines the lowest path cost to the root. | |
| | Default value | in 802.1d mode:<br><br>• Path cost = 1000 / LAN speed in Mbyte/s<br><br>• 1 for 1 Gigabit port |

| Field | Description | |
|---|---|---|
| | | in 802.1t mode: <br><br> • Path cost = 2*10^10 / LAN speed in Kbyte/s <br><br> • 20 000 for 1 Gigabit port (default on ERS5000) <br><br> . <br> The higher the LAN speed, the lower the path cost. |
| | Range | in 802.1d mode: 1 to 65535 in 802.1t mode: 1 to 200 000 000 |
| **State** | This read-only field indicates the current port state within the spanning tree network. Each port can transition to various states, as determined by the Participation field setting. For example, when the Participation field is set to Disabled, the port does not participate in the spanning tree and transitions to the Forwarding state (the default). When the Participation field is set to Enabled, the port transitions from the Disabled state through the Blocking, Listening, and Learning states before entering the Forwarding state. | |
| | Default value | Topology dependent |
| | Range | Disabled, Blocking, Listening, Learning, Forwarding |

## Spanning Tree Switch Settings screen in STPG mode

With the Spanning Tree Switch Settings screen, you can view spanning tree parameter values for the Ethernet Routing Switch 5000 Series.

To open the Spanning Tree Switch Settings screen:

Choose **Display Spanning Tree Switch Settings** (or press d) from the Spanning Tree Configuration Menu screen.

**Table 6: Spanning Tree Switch Settings parameters in STPG mode**

| Parameter | Description | |
|---|---|---|
| **STP Group** | Specifies the number of the spanning tree group (STG) to view. To view another STG, type that STG ID number and press Enter, or press the spacebar on your keyboard to toggle the STP Group numbers. | |
| | Default value | 1 |

| Parameter | Description | |
|---|---|---|
| | Range | Configured STP Groups from 1 to 8 |
| **STP Mode** | Shows the current STP operational mode for switch/stack:<br><br>• Avaya MSTP (STPG)<br><br>• IEEE 802.1w (RSTP)<br><br>• IEEE 802.1s (MSTP) | |
| **Bridge Priority** | Indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values compared first, followed by the hardware addresses. | |
| | Default value | 0x8000 |
| | Range | HEX: 0x0000 - 0xF000 |
| **Designated Root** | Indicates the bridge ID of the root bridge, as determined by spanning tree. | |
| **Root Port** | Indicates the switch port number that offers the lowest path cost to the root bridge. | |
| **Root Path Cost** | Indicates the path cost from this switch port to the root bridge. | |
| | Default value | 0 |
| | Range | Unit 1-8<br>Port 1-50 (in stack mode)<br>Port 1-50 (in standalone mode) |
| **Hello Time** | Defines the amount of time between transmissions of BPDUs. | |
| | Range | 1 to 10 seconds |
| **Maximum Age Time** | Indicates the Maximum Age Time parameter value that the root bridge is currently using. This value specifies the maximum age that a Hello message can attain before being discarded.<br><br>**Note:**<br><br>The root bridge Maximum Age Time parameter value becomes the actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. | |
| | Default value | 20 seconds |

| Parameter | Description | |
|---|---|---|
| | Range | 6 to 40 seconds |
| **Forward Delay** | Indicates the Forward Delay parameter value that the root bridge is currently using. This value specifies the amount of time that the bridge ports remain in each of the Listening and Learning states before entering the Forwarding state.<br><br>**Note:**<br>The root bridge Forward Delay parameter value becomes the actual Forward Delay parameter value for all bridges participating in the spanning tree network. | |
| | Default value | 15 seconds |
| | Range | 4 to 30 seconds |
| **Bridge Hello Time** | Defines the time interval (in seconds) for sending the BPDUs from the bridge. | |
| | Range | 1 to 10 seconds |
| **Bridge Maximum Age Time** | Specifies the maximum age (in seconds) that a Hello message can attain before being discarded. This parameter, specified by management for this bridge, takes effect only when the bridge becomes the root bridge.<br><br>**Note:**<br>If this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. | |
| | Default value | 20 seconds |
| | Range | 6 to 40 seconds |
| **Bridge Forward Delay** | Indicates the Forward Delay parameter value specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge.<br>The Forward Delay parameter value specifies the amount of time that the bridge ports remain in each of the Listening and Learning states before entering the Forwarding state.<br><br>**Note:**<br>All bridges participating in the spanning tree network use the root bridge Forward Delay parameter value. | |
| | Default value | 15 seconds |
| | Range | 4 to 30 seconds |

## Spanning Tree VLAN Membership screen in STPG mode

With the Spanning Tree VLAN Membership screen, you can view which VLANs belong to the selected STP Group. (STP Group 1 is the default STP group.)

To open the Spanning Tree VLAN Membership screen:

Choose **Spanning Tree VLAN Membership** (or press v) from the Spanning Tree Configuration Menu screen.

**Table 7: Spanning Tree VLAN Membership parameters**

| Parameter | Description | |
|---|---|---|
| **STP Group** | Specifies the number of the Spanning Tree Group instances to view. To view another instance, press the spacebar on your keyboard to toggle the STP instances. | |
| | Default value | 1 |
| | Range | 1 - 8. Only created STPs are displayed. |
| **VLAN Membership** | Displays the total number of VLANs in the specified STP Group, as well as the VLAN IDs of the VLAN members. | |

# Spanning Tree configuration in RSTP mode

With the Spanning Tree Configuration Menu screen, you can view spanning tree parameters and configure individual switch ports to participate in the Spanning Tree Algorithm (STA).

To open the Spanning Tree Configuration Menu screen:

Choose **Spanning Tree Configuration** (or press p) from the main menu.

**Table 8: Spanning Tree Configuration main menu options**

| Menu option | Description |
|---|---|
| **Spanning Tree Group Configuration** | Displays the Spanning Tree Group Configuration screen. (See Spanning Tree Group Configuration screen in RSTP mode on page 51.) |
| **Spanning Tree Port Configuration** | Displays the Spanning Tree Port Configuration screen. (See Spanning Tree Port Configuration screen in RSTP mode on page 52.) |

| Menu option | Description |
|---|---|
| **Display Spanning Tree Switch Settings** | Displays the Spanning Tree Switch Settings screen. (See Spanning Tree Switch Settings screen in RSTP mode on page 54.) |

## Spanning Tree Group Configuration screen in RSTP mode

With the Spanning Tree Group Configuration screen, you can create and configure spanning tree groups (STGs).

To open the Spanning Tree Group Configuration screen:

Choose **Spanning Tree Group Configuration** (or press g) from the Spanning Tree Configuration Menu screen.

**Table 9: Spanning Tree Group Configuration parameters in RSTP mode**

| Parameter | Description | |
|---|---|---|
| **STP Mode** | Shows the current STP operational mode for switch/stack: <br> • Avaya MSTP (STPG) <br> • IEEE 802.1w (RSTP) <br> • IEEE 802.1s (MSTP) | |
| **Bridge Priority (in Hex)** | For the STP Group, configures the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values. | |
| | Default value | 0x8000 |
| | Range | 0x0000 to 0xF000 |
| **Bridge Hello Time** | For the STP Group, configures the Hello Interval (the amount of time between transmissions of BPDUs). This parameter takes effect only when this bridge becomes the root bridge. Although you can set the Hello Interval for a bridge using bridge management software, after the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network. | |
| | Default value | 2 seconds |
| | Range | 1 to 10 seconds |

| Parameter | Description | |
|---|---|---|
| **Bridge Max. Age Time** | For the STP Group, configures the maximum age (in seconds) that a Hello message can attain before being discarded. This parameter takes effect only when the bridge becomes the root bridge. If this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. | |
| | Default value | 20 seconds |
| | Range | 6 to 40 seconds |
| **Bridge Forward Delay Time** | For the STP Group, configures the Forward Delay parameter value for this bridge. This parameter takes effect only when this bridge becomes the root bridge. The Forward Delay parameter value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. Note that all bridges participating in the spanning tree network use the root bridge Forward Delay parameter value. | |
| | Default value | 15 seconds |
| | Range | 4 to 30 seconds |
| **Bridge Tx Hold Count** | Indicates the number of BPDUs that are sent in each Hello Time interval. This number limits the maximum transmission rate. | |
| **Default Path Cost Type** | Indicates the default representation of path costs. 32 bits (default in MSTP/RSTP mode, supported in STPG mode) 16 bits (default in STPG mode, supported in MSTP/RSTP mode). | |
| | Default value | 32 bits in MSTP/RSTP mode 16 bits in legacy STPG mode |

## Spanning Tree Port Configuration screen in RSTP mode

With the Spanning Tree Port Configuration screen, you can configure individual switch ports or all switch ports for participation in the spanning tree.

**Note:**

If spanning tree participation of any trunk member is changed (enabled or disabled), the spanning tree participation of all members of that trunk is changed similarly.

Choose **Spanning Tree Port Configuration** (or press c) from the **Spanning Tree Configuration Menu** to open the Spanning Tree Port Configuration screen.

**Table 10: Spanning Tree Port Configuration parameters in RSTP mode**

| Field | Description | |
|---|---|---|
| Unit | This field appears only if the switch is participating in a stack configuration. The field specifies the number of the unit to view. To view another unit, type its unit number and press Enter, or press the spacebar on your keyboard to toggle the unit numbers. | |
| Port | Indicates the switch port numbers that correspond to the field values in that row (for example, the field values in row 2 apply to switch port 2). The values in the Switch row affect all switch ports, and when the switch is part of a stack, the values in the Stack row affect all ports in the entire stack. | |
| Trunk | The read-only data displayed in this column indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen. | |
| Learning | Indicates the port states of Spanning Tree. | |
| | Range | Enabled, Disabled |
| Edge | Indicates if a port is an Edge port. When a port is connected to a non-switch device such as a PC or a workstation, configure it as an Edge port. An active Edge port goes directly to Forwarding state without any delay. | |
| Priority | This read-only field is a bridge spanning tree parameter that prioritizes the lowest port path cost to the root. When one or more ports have the same path cost, STP selects the path with the highest priority (lowest numerical value). | |
| | Default value | 128 |
| | Range | 0 to 255 |
| Path Cost | This read-only field is a bridge spanning tree parameter that determines the lowest path cost to the root. | |
| | Default value | 20000 for 1 Gigabit port Path cost = 2*10^10/LAN speed (in Kbits/s) The higher the LAN speed, the lower the path cost. |
| | Range | 1 to 200 000 000 |

| Field | Description |
|-------|-------------|
| **Role** | A role represents a functionality characteristic or capability of a resource to which policies are applied. The role of a port can be Root, Designated, Alternate, or Backup. |
| **State** | Indicates the current state of the Port as defined by the Rapid Spanning Tree Protocol. The state of a Port can be Forwarding in one instance and Discarding (Blocking) in another. |

## Spanning Tree Switch Settings screen in RSTP mode

With the Spanning Tree Switch Settings screen, you can view spanning tree parameter values for the Ethernet Routing Switch 5000 Series.

To open the Spanning Tree Switch Settings screen:

Choose **Display Spanning Tree Switch Settings** (or press d) from the Spanning Tree Configuration Menu screen.

**Table 11: Spanning Tree Switch Settings parameters in RSTP mode**

| Field | Description | |
|-------|-------------|---|
| **STP Mode** | Indicates the mode of the STP operation for the switch. The possible values for the STP mode are:<br><br>• STPG (Avaya MSTP)<br><br>• RSTP (IEEE 802.1w)<br><br>• MSTP (IEEE 802.1s) | |
| **Bridge Priority** | Indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values compared first, followed by the hardware addresses. | |
| | Default value | 0x8000 |
| | Range | HEX: 0x0000 - 0xF000 |
| **Designated Root** | This field specifies the unique Bridge Identifier of the bridge. It is recorded as the CIST Root in the configuration BPDUs that are transmitted. | |
| **Root Port** | Indicates the switch port number that offers the lowest path cost to the root bridge. The local switch is the root bridge when this value is 0 (path cost). | |
| | Default value | 0 |

| Field | Description | |
|---|---|---|
| | Range | Unit: 1-8, Port 1-50 (in stack mode)<br>Port: 1-98 (in standalone mode) |
| **Root Path Cost** | Indicates the path cost from this switch port to the root bridge. | |
| | Default value | 0 |
| | Range | Not applicable |
| **Hello Time** | Defines the amount of time between transmissions of BPDUs. | |
| | Range | 1 to 10 seconds |
| **Maximum Age Time** | Indicates the Maximum Age Time parameter value that the root bridge is currently using. This value specifies the maximum age that a Hello message can attain before being discarded. The root bridge Maximum Age Time parameter value becomes the actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. | |
| | Default value | 20 seconds |
| | Range | 6 to 40 seconds |
| **Forward Delay** | Indicates the Forward Delay parameter value that the root bridge is currently using. This value specifies the amount of time that the bridge ports remain in each of the Discarding and Learning states before entering the Forwarding state.<br>The root bridge Forward Delay parameter value becomes the actual Forward Delay parameter value for all bridges participating in the spanning tree network. | |
| | Default value | 15 seconds |
| | Range | 4 to 30 seconds |
| **Bridge Hello Time** | For the STP Group, configures the Hello Interval. This parameter takes effect only when this bridge becomes the root bridge.<br>Although you can set the Hello Interval for a bridge using the bridge management software, after the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network. | |
| | Default value | 2 seconds |

| Field | Description | |
|---|---|---|
| | Range | 1 to 10 seconds |
| **Bridge Maximum Age Time** | Specifies the maximum age (in seconds) that a Hello message can attain before being discarded. This parameter, specified by management for this bridge, takes effect only when the bridge becomes the root bridge.<br>If this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. | |
| | Default value | 20 seconds |
| | Range | 6 to 40 seconds |
| **Bridge Forward Delay** | Indicates the Forward Delay parameter value specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge.<br>The Forward Delay parameter value specifies the amount of time that the bridge ports remain in each of the Discarding and Learning states before entering the Forwarding state.<br>All bridges participating in the spanning tree network use the root bridge Forward Delay parameter value. | |
| | Default value | 15 seconds |
| | Range | 4 to 30 seconds |
| **Tx Hold Count** | This is the value used by the Port Transmit state machine to limit the maximum transmission rate. The value can range from 1 to 10 | |
| **Default Path Cost Type** | Indicates the way that path cost is represented and used. | |

# Spanning Tree configuration in MSTP mode

With the Spanning Tree Configuration Menu screen, you can view spanning tree parameters and configure individual switch ports to participate in the spanning tree algorithm (STA).

To open the Spanning Tree Configuration Menu screen:

Choose **Spanning Tree Configuration** (or press p) from the main menu.

**Table 12: Spanning Tree Configuration Menu options in MSTP mode**

| Option | Description |
|---|---|
| **Spanning Tree Group Configuration** | Displays the Spanning Tree Group Configuration screen. |

| Option | Description |
|---|---|
| **Spanning Tree Port Configuration** | Displays the Spanning Tree Port Configuration screen. |
| **Display Spanning Tree Switch Settings** | Displays the Spanning Tree Switch Settings screen. |
| **Display Spanning Tree VLAN Membership** | Displays the Spanning Tree VLAN Membership screen. |

## Spanning Tree Group Configuration screen in MSTP mode

With the Spanning Tree Group Configuration screen, you can create and configure spanning tree groups (STGs).

To open the Spanning Tree Group Configuration screen:

Choose **Spanning Tree Group Configuration** (or press g) from the Spanning Tree Configuration Menu screen.

**Table 13: Spanning Tree Group Configuration parameters in MSTP mode**

| Parameter | Description | |
|---|---|---|
| **STP mode** | Indicates the STP mode in which the switch is operating. The available modes are:<br><br>• STPG (Avaya MSTP)<br><br>• RSTP (IEEE 802.1w)<br><br>• MSTP (IEEE 802.1s) | |
| **Create STP Group** | Creates a spanning Tree group. You can also use this parameter to select the STP Group information to display. | |
| | Default value | CIST |
| | Range | 1 to 7 (MSTIs) |
| **Delete STP Group** | Deletes a spanning tree group. You cannot delete the CIST STP Group, and you can delete only nonactive STP Groups (that is, MSTIs). | |
| | Default Value | Blank |
| | Range | 1 to 8; only created STP Groups are available |
| **Bridge Priority** | For the STP Group, configures the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values. | |

| Parameter | Description | |
|---|---|---|
| | Default value | 0x8000 |
| | Range | 0x0000 -0xF000 |
| **Bridge Max. Age Time** | For the STP Group, configures the maximum age (in seconds) that a Hello message can attain before being discarded. This parameter takes effect only when the bridge becomes the root bridge.<br>If this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. | |
| | Default value | 20 seconds |
| | Range | 6 to 40 seconds |
| **Bridge Forward Delay Time** | For the STP Group, configures the Forward Delay parameter value for this bridge. This parameter takes effect only when this bridge becomes the root bridge.<br>The Forward Delay parameter value specifies the amount of time that the bridge ports remain in each of the Discarding and Learning states before entering the Forwarding state.<br>All bridges participating in the spanning tree network use the root bridge Forward Delay parameter value. | |
| | Default value | 15 seconds |
| | Range | 4 to 30 seconds |
| **Bridge Tx Hold Count** | Indicates the number of BPDUs that are sent in each Hello Time interval. The value used by the Port Transmit state machine to limit the maximum transmission rate. | |
| | Default value | 3 |
| | Range | 1 to 10 |
| **Max. Hop Count** | The Maximum Hop Count value in 1/100 seconds. The specified value must be a multiple of 100. | |
| | Default value | 2000 |
| | Range | 600 to 4000, measured in 1/100 second |
| **Default Path Cost Type** | The version of the Spanning Tree default Path Costs that are used by this Bridge. A value of 16 Bits specifies the 16-bit default path costs from IEEE Standard 802.1D-1998. A value of 32 Bits specifies the 32-bit default path costs from IEEE Standard 802.1t. | |
| | Default value | 32 Bits |
| | Range | 16 Bits, 32 Bits |

| Parameter | Description | |
|---|---|---|
| **Add VLAN Membership** | Adds a VLAN to the specified spanning tree group.<br><br>**Note:**<br>This field is updated with active VLANs currently defined in the system. A newly created and active VLAN is assigned to STP Group 1 by default. | |
| | Default value | 1 |
| | Range | 1 to 4094 |
| **Delete VLAN Membership** | Deletes a VLAN from the specified STP group.<br><br>**Note:**<br>You cannot remove VLAN 1 from STP Group 1. | |
| | Default value | Blank |
| | Range | 1 to 4094; but only configured ones are available |
| **STP Group State** | Specifies whether the MSTI is active or inactive.<br><br>**Note:**<br>You cannot set the default STG (CIST) to inactive. To enable an STP Group, at least one active VLAN must be assigned to that STP Group (MSTI). | |
| | Default value | Active for CIST; Inactive for MSTIs 1 to 7. |
| | Range | Active or Inactive |

## Spanning Tree Port Configuration screen in MSTP mode

With the Spanning Tree Port Configuration screen, you can configure individual switch ports or all switch ports for participation in the spanning tree.

> **Note:**
> If spanning tree participation of any trunk member is changed (enabled or disabled), the spanning tree participation of all members of that trunk is changed similarly.

To open the Spanning Tree Port Configuration screen:

> Choose **Spanning Tree Port Configuration** (or press c) from the **Spanning Tree Configuration Menu** to open the Spanning Tree Port Configuration screen.

**Table 14: Spanning Tree Port Configuration screen fields in MSTP mode**

| Field | Description | |
|---|---|---|
| **STP Group** | Specifies the MSTP instance for which to display the port properties. Press the spacebar to toggle between the CIST and the configured MSTI instances. | |
| **Port** | Indicates the switch port numbers that correspond to the field values in that row (for example, the field values in row 2 apply to switch port 2). The values in the Switch row affect all switch ports, and when the switch is part of a stack, the values in the Stack row affect all ports in the entire stack. | |
| **Trunk** | The read-only data displayed in this column indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen. | |
| **Learning** | Configures any (or all) of the switch ports for Spanning tree participation.<br>When an individual port is a trunk member (see Trunk field), changing this setting for one of the trunk members changes the setting for all members of that trunk. Consider how this will change your network topology before you change this setting. | |
| | Default value | Enabled |
| **Edge** | A value of Yes indicates that this port is to be assumed as an edge-port and a value of No indicates that this port is to be assumed as a non-edge port. | |
| | Default value | No |
| | Range | No, Yes |
| **Priority** | This read-only field is a bridge spanning tree parameter that prioritizes the lowest port path cost to the root. When one or more ports have the same path cost, STP selects the path with the highest priority (lowest numerical value). | |
| | Default value | 128 |
| | Range | 0 to 255 |
| **Path Cost** | This read-only field is a bridge spanning tree parameter that determines the lowest path cost to the root. | |
| | Default value | Default value is 20000 for 1 Gigabit port Path Cost = 2*10^10/LAN speed (in Kbit/s) The higher the LAN speed, the lower the path cost. |
| | Range | 1 to 200 000 000 |
| **Role** | The current role of the port as defined by Multiple Spanning Tree Protocol. | |

| Field | Description | |
|---|---|---|
| | Default | Disabled |
| | Range | Disabled, Root, Designated, Alternate, Backup |
| **State** | This read-only field indicates the current port state within the spanning tree network. Each port can transition to various states, as determined by the Participation field setting. For example, when the Participation field is set to Disabled, the port does not participate in the spanning tree and transitions to the Forwarding state (the default). When the Participation field is set to Enabled, the port transitions from the Disabled state through the Blocking, Listening, and Learning states before entering the Forwarding state. | |
| | Default value | Topology dependent |
| | Range | Discarding, Learning, Forwarding |

## Spanning Tree Switch Settings screen in MSTP mode

With the Spanning Tree Switch Settings screen, you can view spanning tree parameter values for the Ethernet Routing Switch 5000 Series.

To open the Spanning Tree Switch Settings screen:

Choose **Display Spanning Tree Switch Settings** (or press d) from the Spanning Tree Configuration Menu screen.

**Table 15: Spanning Tree Switch Settings parameters in MSTP mode**

| Parameter | Description | |
|---|---|---|
| **STP Group** | Specifies the MSTP instance for which to display the properties. Press the spacebar to toggle between the CIST and the configured MSTI instances. | |
| **Bridge Priority** | Indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values compared first, followed by the hardware addresses. | |
| | Default value | 8000 |
| | Range | 0x0000 - 0xF000 |
| **CIST Root** | Common and Internal Spanning Tree (CIST) Root field shows the CIST External or Internal Root elected between devices. CIST Internal Root is used only on devices from the same | |

| Parameter | Description | |
|---|---|---|
| | region. CIST External (Common Spanning Tree) Root is elected between devices from different regions or between devices with different STP modes. This parameter displays these values depending on network configuration. | |
| **Regional Root** | Shows the CIST Regional Root bridge elected between devices from the same region (in other words, the root for the Region). | |
| **Root Port** | Indicates the switch port number that offers the lowest path cost to the root bridge. The local switch is the root bridge when this value is 0 (path cost). | |
| | Range | Unit: 1-8, Port 1-50 (in stack mode) Port: 1-50 (in standalone mode) |
| **Root Path Cost** | Indicates the path cost from this switch port to the root bridge. | |
| | Default value | 0 |
| | Range | Not applicable |
| **Regional Root Path Cost** | Indicates the Path Cost to CIST Regional Root seen from this device. | |
| **Maximum Age Time** | Indicates the Maximum Age Time parameter value that the root bridge is currently using. This value specifies the maximum age that a Hello message can attain before being discarded. The root bridge Maximum Age Time parameter value becomes the actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. | |
| | Default value | 20 seconds |
| | Range | 6 to 40 seconds |
| **Forward Delay** | Indicates the Forward Delay parameter value that the root bridge is currently using. This value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. The root bridge Forward Delay parameter value becomes the actual Forward Delay parameter value for all bridges participating in the spanning tree network. | |
| | Default value | 15 seconds |
| | Range | 4 to 30 seconds |
| **Bridge Hold Time** | This value determines the time interval during which no more than two configuration BPDUs can be transmitted by this node. | |

| Parameter | Description | |
|---|---|---|
| | Default value | 1 second |
| **Bridge Maximum Age Time** | Specifies the maximum age (in seconds) that a Hello message can attain before being discarded. This parameter, specified by management for this bridge, takes effect only when the bridge becomes the root bridge. | |
| | If this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. | |
| | Default value | 20 seconds |
| | Range | 6 to 40 seconds |
| **Bridge Forward Delay** | Indicates the Forward Delay parameter value specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. | |
| | The Forward Delay parameter value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. | |
| | All bridges participating in the spanning tree network use the root bridge Forward Delay parameter value. | |
| | Default value | 15 seconds |
| | Range | 4 to 30 seconds |
| **Tx Hold Count** | Indicates the number of BPDUs that are sent in each Hello Time interval. This number limits the maximum transmission rate. | |
| | Default value | 3 |
| | Range | 1 to 10 |
| **Hop Count (Max)** | This value is decremented by each device (inside a region) starting from Regional Root switch. When it reaches 0 (zero), STP information is discarded, and a new root is elected. The Root port on this device becomes a Designated port. | |
| | Default value | 2000 (20 hops) |
| | Range | 600 to 4000 (6 to 40 hops). |
| **Default Path Cost Type** | Indicates the default representation of path costs. 32 bits (default in MSTP/RSTP mode, supported in STPG mode) 16 bits (default in STPG mode, supported in MSTP/RSTP mode). | |
| | Default value | 32 bits in MSTP/RSTP mode 16 bits in legacy STPG mode |
| **Region Name** | Name of the Region. CIST External Root interprets devices from the same region as a single switch. | |

| Parameter | Description | |
|---|---|---|
| | Default value | The MAC address of the device |
| | Range | 1 to 32 chars (string) |

# Spanning Tree VLAN Membership screen in MSTP mode

With the Spanning Tree VLAN Membership screen, you can view which VLANs belong to the selected STP Group. (The CIST is displayed by default.)

To open the Spanning Tree VLAN Membership screen:

Choose **Spanning Tree VLAN Membership** (or press $v$) from the Spanning Tree Configuration Menu screen.

**Table 16: Spanning Tree VLAN Membership parameters**

| Parameter | Description | |
|---|---|---|
| **STP Group** | Specifies the number of the Spanning Tree Group instances (CIST/MSTI) you want to view. To view another instance, press the spacebar on your keyboard to toggle the STP instances (MSTIs). | |
| | Default value | CIST |
| | Range | CIST, MSTI-1 to MSTI-7. Only created MSTIs are displayed. |
| **VLAN Membership** | Displays the total number of VLANs in the specified STP Group, as well as the VLAN IDs of the VLAN members. | |

# Chapter 5: Multi-Link Trunking Fundamentals

The following sections contain fundamental information regarding Multi-Link Trunking.

## Multi-Link trunks

With Multi-Link trunks, you can group up to eight switch ports together to form a link to another switch or server, thus increasing aggregate throughput of the interconnection between the devices (up to 8 Gigabits in full-duplex mode). Up to 32 Multi-Link trunks can be configured. The trunk members can reside on a single unit or on multiple units within the same stack configuration as a distributed trunk. Multi-Link Trunking software detects misconfigured (or broken) trunk links and redirects traffic on the misconfigured or broken trunk link to other trunk members within that trunk.

The Command Line Interface (ACLI) or Device Manager (DM) can be used to create switch-to-switch and switch-to-server Multi-Link trunk links.

## Client-server configuration using Multi-Link trunks

Figure 16: Client/server configuration example on page 66 shows an example of how Multi-Link Trunking can be used in a client/server configuration. In this example, both servers connect directly to Switch S1. FS2 is connected through a trunk configuration. The switch-to-switch connections are through trunks.

Clients accessing data from the servers (FS1 and FS2) are provided with maximized bandwidth through trunks T1, T2, T3, T4, and T5. Trunk members (the ports making up each trunk) do not have to be consecutive switch ports; ports can be selected randomly, as shown by T5.

With spanning tree enabled, one of the trunks (T2 or T3) acts as a redundant (backup) trunk to Switch S2. With spanning tree disabled, trunks T2 and T3 must be configured into separate VLANs for this configuration to function properly.
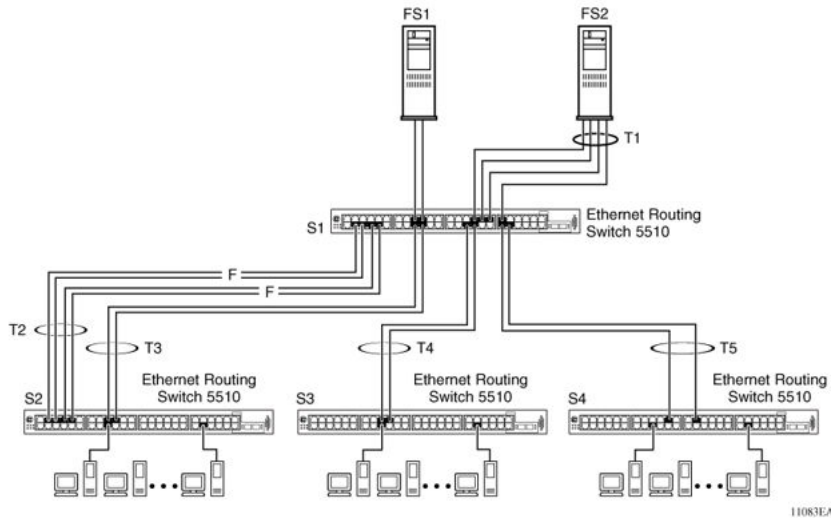
**Figure 16: Client/server configuration example**

# Before configuring trunks

When a trunk is created and enabled, the trunk members (switch ports) take on certain settings necessary for the correct operation of the Multi-Link Trunking feature.

Before configuring a Multi-Link trunk, consider these settings, along with specific configuration rules, as follows:

1. Read the configuration rules provided in the next section, Multi-Link Trunking Configuration Rules on page 67.

2. Determine which switch ports (up to eight) are to become trunk members (the specific ports making up the trunk). A minimum of two ports are required for each trunk.

   **Note:**

   Disabled ports can belong to MLTs. For traffic to flow to your configured MLT ports, be sure they are enabled.

3. Ensure that the trunk member ports have the same VLAN configuration.

4. To avoid configuration errors, all network cabling must be complete and stable before configuring any trunks.

   **Note:**

   If trunk ports are STP enabled, ensure that all potential trunk members are connected to their corresponding members; otherwise, STP cannot converge correctly, and traffic loss can result.

5. Consider how the existing spanning tree will react to the new trunk configuration.

> **Note:**
> If potential trunk ports are connected and STP is disabled on these ports, a loop is formed; to avoid this situation, enable the trunk before you disable STP.

6. Consider how existing VLANs will be affected by the addition of a trunk.

# Multi-Link Trunking Configuration Rules

The Multi-Link Trunking feature is deterministic; that is, it operates according to specific configuration rules. When creating trunks, consider the following rules that determine how the Multi-Link trunk reacts in any network topology:

- Disabled ports can belong to MLTs. For traffic to flow to your configured MLT ports, be sure they are enabled (set to Enabled through the Port Configuration screen or through network management).
- All trunk members must have the same VLAN configuration before the Trunk Status field on the Trunk Configuration screen can be set to Enabled using the ACLI.

> **Note:**
> Only the first six trunks can be configured on this screen. You must use ACLI or EDM to configure trunks with an ID greater than 6.

- When an active port is configured in a trunk, the port becomes a trunk member when the Trunk Status field is set to Enabled. The spanning tree parameters for the port then change to reflect the new trunk settings.
- If the spanning tree participation of any trunk member is changed to Enabled or Disabled, the spanning tree participation of all members of that trunk changes similarly.
- If the VLAN settings of any trunk member is changed, the VLAN settings of all members of that trunk change similarly.
- A trunk member cannot be configured as a monitor port.
- Entire trunks cannot be monitored by a monitor port; however, trunk members can be monitored.
- All trunk members must have identical Internet Gateway Management Protocol (IGMP) configurations.
- If you change the IGMP snooping configuration for any trunk member, the IGMP snooping settings for all trunk members change.
- Avaya recommends that you do not enable MAC Address Security on trunk ports.

- MLT ports can be set to participate in different STGs. They must have the same spanning tree learning in every group but not necessarily have the same learning between different groups to consistently update their state in the port driver.
- Like normal ports, MLT ports can be set to participate with different spanning tree learning for different spanning tree groups. Trunk ports that are in multiple spanning tree groups must be tagged, and all MLT members must belong to the same spanning tree group.

## MLT load-balancing

With the Ethernet Routing Switch 5000 Series you can choose between MAC-based (basic) or IP-based (advanced) load balancing. You can configure this option using the ACLI.

The 5000 Series switch uses the following formula to perform MLT load-balancing:

{(A XOR B) MOD x}

If A and B are the same, the XOR is false, and if they are different, it is true.

The variables used in the formula represent different parameters for each load-balancing mode:

- MAC-based (basic): In the basic mode, A and B represent the three least significant bits in the source and destination MAC addresses, respectively, and x represents the number of active links in the MLT.
- IP-based (advanced): In the advanced mode, A and B represent the three least significant bits in the source and destination IP addresses, respectively, and x represents the number of active links in the MLT.

For example, consider MAC-based load balancing with an Ethernet frame that has the following source and destination MAC addresses:

- Source MAC: 0x0000A4F8B321
- Destination MAC: 0x0000A2123456

Assume that the MLT is comprised of four ports. In this example, the last byte of the source MAC address is 0x21, the binary representation of which is 00100001. The three least significant bits are 001. Likewise, the binary representation of the last byte in the destination MAC address, 0x56, is 01010110, of which 110 are the bits of least significance. The formula is {(A XOR B) MOD x}, where A and B are the three least significant bits in the source and destination MAC addresses, and x is the number of active links in the MLT. Thus:

{(001 XOR 110) MOD 4} = 7 MOD 4 = 3

Therefore, because the ports in the MLT are numbered 0 through 3, this Ethernet frame will traverse the fourth port of the MLT.

## Removal of MLT restrictions

If any trunk member is set to Disabled (not active) through the Port Configuration screen or through network management, the trunk member is no longer removed from the trunk. The

trunk member remains a disabled member of the trunk, and so no longer has to be reconfigured to rejoin the trunk. A trunk member can also now be disabled if only two trunk members exist on the trunk.

The lowest numbered port in the trunk can now be disabled as well. However, Avaya does not recommend disabling the lowest numbered port if Spanning Tree is enabled on the trunk.

# Adding and deleting links from existing Multi-Link trunks

Ports cannot be added or removed from an Avaya Ethernet Routing Switch 5000 Series switch MLT, unless MLT is first disabled. When MLT is disabled, the ports assigned to the MLT are not disabled. The ports form separate links and create a network loop.

# How a Multi-Link trunk reacts to losing distributed trunk members

A Multi-Link trunk (Figure 17: Loss of distributed trunk member on page 70) can cover separate units in a stack configuration. If a unit in the stack becomes inactive due to loss of power or unit failure, the unaffected trunk members remain operational.
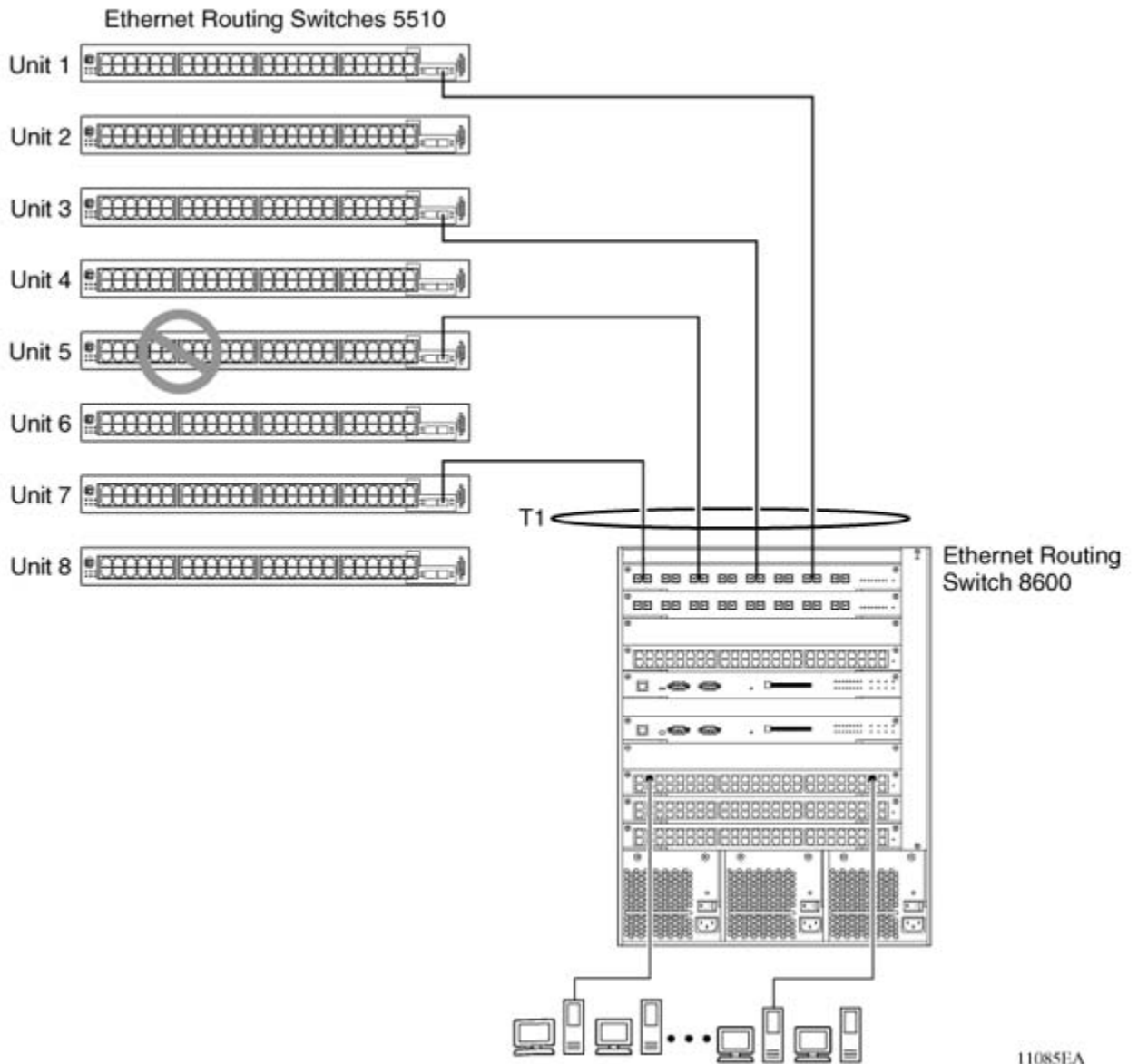
**Figure 17: Loss of distributed trunk member**

However, until the cause of the failure is corrected or the trunk Status field is changed to Disabled, any of the following parameters for the affected trunk cannot be modified:

- VLAN configuration
- Spanning Tree configuration
- Port configuration
- IGMP configuration

In addition, Avaya recommends that you do not modify Rate Limiting until the cause of failure is corrected or the trunk is disabled.

# Spanning Tree Considerations for Multi-Link trunks

The spanning tree Path Cost parameter is recalculated based on the aggregate bandwidth of the trunk. For example, Figure 18: Path Cost Arbitration on page 71 shows a two-port trunk (T1) with two port members operating at an aggregate bandwidth of 2 GB, with a comparable Path Cost of 1. Trunk 2 has two ports at 100 Mbit/s with a Path Cost of 5.

When the Path Cost calculations for both trunks are equal, the software chooses the trunk containing the lowest numbered port as the forwarding path.

> **Note:**
>
> The default spanning tree Path Cost for all gigabit ports is always equal to 1.

Be careful when configuring trunks so as to not add one gigabit link physically in front of another trunk; the trunk will be blocked because they both have a Path Cost of 1.
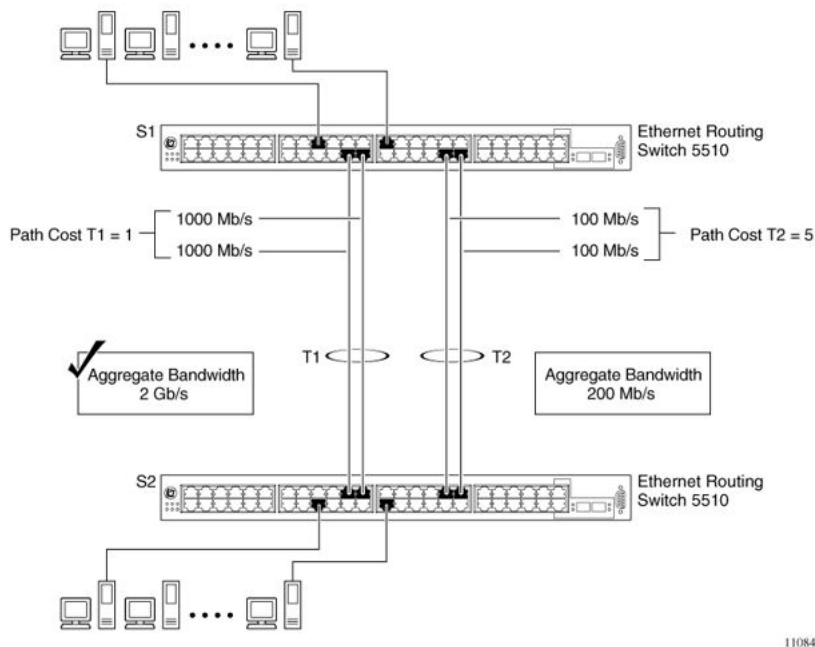


**Figure 18: Path Cost Arbitration**

The switch can also detect trunk member ports that are physically misconfigured. For example, in Figure 19: Correctly Configured Trunk on page 72, trunk member ports 2, 4, and 6 of Switch S1 are configured correctly to trunk member ports 7, 9, and 11 of Switch S2. The Spanning Tree Port Configuration screen for each switch shows the port state field for each port in the Forwarding state.

S1 Port Configuration screen



S2 Port Configuration screen
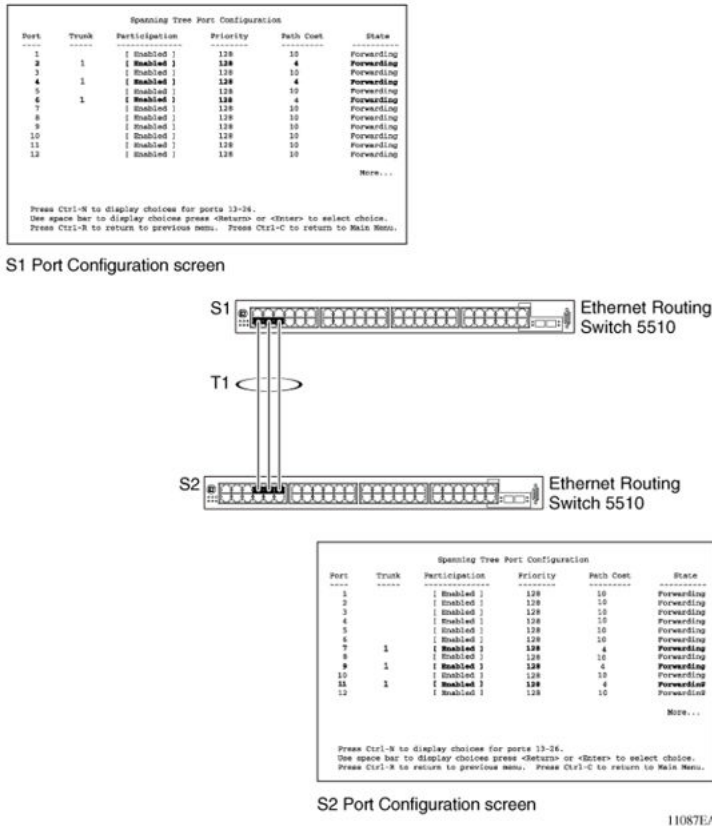
**Figure 19: Correctly Configured Trunk**

**Note:**

Cost varies with port speed. For example, the cost for a 1 Gbit/s port is 1, while the cost for a 100 Mbit/s port is 3.

If trunk member port 11 of root Switch S2 is physically disconnected and then reconnected to port 13, the Spanning Tree Port Configuration screen for Switch S1 changes to show port 6 in the Blocking state (Figure 20: Detecting a Misconfigured Port on page 73)

S1 Port Configuration screen



S2 Port Configuration screen

11088EA

**Figure 20: Detecting a Misconfigured Port**

**Note:**

If the port speed is 100 Mbit/s, then the STP cost for trunk members on S2 is 5.

# Port membership in Multi-Link Trunking

When a Multi-Link trunk is created, the individual trunk members (the specific ports that make up the trunk) logically connect and react as a single entity. For example, if you change spanning tree parameters for any trunk member, the spanning tree parameters for all trunk members change.

To change port membership in Multi-Link Trunking:

1. Disable the trunk.

2. Make the change.

3. Re-enable the trunk.

All configured trunks are indicated in the Spanning Tree Configuration screen. The Trunk field lists the active trunks, adjacent to the port numbers that correspond to the specific trunk member for that trunk.

When you change a Spanning Tree parameter for one trunk member, the modification affects all trunk members.

The trunk is also viewed by management stations as a single spanning tree port. The spanning tree port is represented by the trunk member with the lowest port number. For example, if ports 13, 14, 15, and 16 are trunk members of trunk T1, the management station views trunk T1 as spanning tree port 13.

# SMLT

This section describes the Split Multi-Link Trunking (SMLT) feature and includes the following topics:

## Overview

Split Multi-Link Trunking (SMLT) is an extension of MLT that allows edge switches using MLT to dual-home to two SMLT aggregation switches. SMLT is transparent to the edge switches supporting MLT. In addition to link failure protection and flexible bandwidth scaling, SMLT improves the level of Layer 2/Layer 3 resiliency by providing nodal protection.

Because SMLT inherently avoids loops, SMLT networks do not require the use of IEEE 802.1D Spanning Tree protocols to enable loop free triangle topologies.

SMLT avoids loops by allowing two aggregation switches to appear as a single device to edge switches, which are dual-homed to the aggregation switches. The aggregation switches are interconnected using an Inter-Switch Trunk (IST), which allows them to exchange addressing and state information (permitting rapid fault detection and forwarding path modification).

Although SMLT is primarily designed for Layer 2, it also provides benefits for Layer 3 networks as well.

**Important:**

For SMLT to function properly, you must manually disable STP on all SMLT, IST, and SLT ports in all spanning tree groups or instances to which the ports belong. You must also disable STP on all edge switch MLT ports that are connected to the SMLT or SLT.

SMLT is supported on standalone units or in a stack. You can configure a maximum of 31 SMLT trunks on one device.

SMLT is supported on standalone or stacked units in triangle, square, or full mesh configuration (see Figure 21: SMLT in triangle configuration on page 77 and Figure 23: SMLT in square configuration on page 82) and on stacks in triangle configuration.

You cannot configure SMLT data when SMLT is running. To modify an SLT or SMLT, you must disable SMLT on that port or trunk. As well, in this release, IGMP over SMLT is not supported.

**Note:**

The Ethernet Routing Switch 5000 Series offers support for LACP (IEEE 802.3ad) over SMLT in a triangle topology only. Layer 2 Edge switches must support Multi-Link Trunking to allow communications with SMLT aggregation switches.

**Note:**

To enable SMLT on the Ethernet Routing Switch 5000 Series, you must first enable Global IP Routing.

**Note:**

With release 5.0 software and above, PIM-SM is not supported over an IST link.

## Advantages of SMLT

SMLT improves the reliability of Layer 2 networks that operate between user access switches and the network center aggregation switch by providing:

- Load sharing among all links
- Fast failover in case of link failures
- Elimination of single point of failure
- Fast recovery in case of nodal failure
- A transparent and interoperable solution
- Removal of STP convergence issues

## SMLT compared to Spanning Tree Protocol

Networks that are designed with non-SMLT access switches dual-homed to two aggregation switches have the following design constraints:

- Spanning Tree must be used to detect loops

- No load sharing exists over redundant links

- Slow network convergence exists in case of failure

SMLT helps eliminate all single points of failure and, unlike STP, creates multiple paths from all access switches to the core of the network. Furthermore, in case of failure, SMLT recovers as quickly as possible so that no unused capacity is created. Finally, SMLT provides a transparent and interoperable solution that requires no modification on the part of the majority of existing user access devices.

# How does SMLT work?

SMLT can be set up in triangle or square configuration. All configurations of SMLT rely on pairs of aggregation switches connected by IST links. These links are usually MLT or DMLT links.

## Triangle SMLT configuration

Triangle SMLT configuration requires one pair of aggregation switches as shown in . Triangle SMLT can be set up with standalone switches or in a stack configuration.
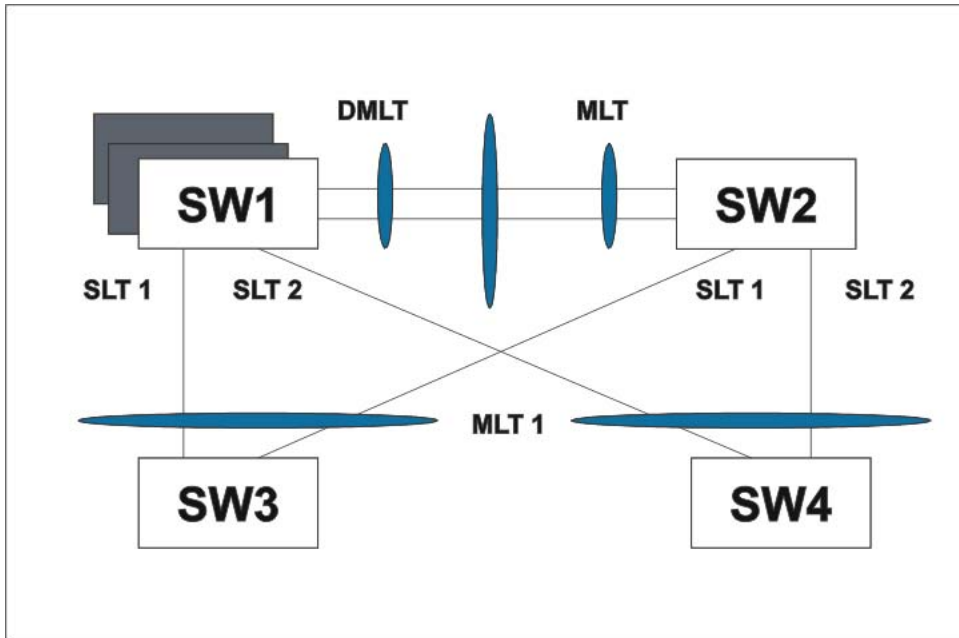
**Figure 21: SMLT in triangle configuration**

# Detailed configuration example for SMLT triangle configuration

The following illustration and command set provides an example of SMLT triangle configuration.
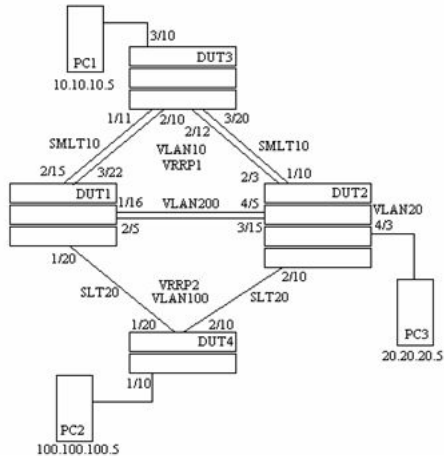
**Figure 22: SMLT triangle configuration**

**Table 17: SMLT triangle configuration**

| VLAN | Components |
|---|---|
| VLAN10 | DUT1 10.10.10.2 DUT2 10.10.10.3 VRRPIP1 10.10.10.1 PC1: 10.10.10.5 |
| VLAN100 | DUT1 100.100.100.3 DUT2 100.100.100.2 VRRPIP2 100.100.100.1 PC2: 100.100.100.5 |
| VLAN200 | DUT1: 200.200.200.1 DUT2: 200.200.200.2 |
| VLAN20 | DUT2: 20.20.20.1 PC3: 20.20.20.5 |

Configure DUT1

```
vlan create 10 type port
vlan create 100 type port
vlan create 200 type port
vlan port 1/20,2/5,1/16,3/22,2/15 tag enable
vlan mem add 100 1/20,1/16,2/5
vlan mem add 200 1/16,2/5
vlan mem add 10 2/15,3/22,1/16,2/5
vlan mem rem 1 1/20,2/5,1/16,3/22,2/15
```

```
ip routing
in vlan 200
ip add 200.200.200.1 255.255.255.0
exit
in vlan 10
ip add 10.10.10.2 255.255.255.0
exit
in vlan 100
```

```
ip add 100.100.100.3 255.255.255.0
exit
```

```
mlt 10 ena mem 2/15,3/22
mlt spanning-tree 10 stp all learning disable
```

```
mlt 30 ena mem 1/16,2/5
mlt spanning-tree 30 stp all learning disable
```

```
in mlt 30
ist peer-ip 200.200.200.2
ist vlan 200
ist ena
exit
```

```
in mlt 10
smlt 10
exit
```

```
in fast 1/20
smlt 20
exit
```

```
in vlan 100
ip vrrp address 1 100.100.100.1
ip vrrp 1 enable backup-master enable
ip ospf enable
exit
```

```
in vlan 10
ip vrrp address 2 10.10.10.1
ip vrrp 2 enable backup-master enabl
ip ospf enable
exit
```

```
in vlan  200
ip ospf enable
exit
```

```
router vrrp ena
router ospf ena
```

Configure DUT2.

```
vlan create 10 type port
vlan create 100 type port
vlan create 200 type port
vlan create 20 type port
vlan port 2/10,4/5,3/15,1/10,2/3 tag enable
vlan mem add 200 4/5,3/15
vlan mem add 10 2/3,1/10,4/5,3/15
vlan mem rem 1 2/10,4/5,3/15,1/10,2/3
vlan mem rem 1 4/3
```

```
vlan mem add 20 4/3
vlan port 4/3 pvid 20

ip routing
in vlan 200
ip add 200.200.200.2 255.255.255.0
exit
in vlan 10
ip add 10.10.10.3 255.255.255.0
exit
in vlan 100
ip add 100.100.100.2 255.255.255.0
exit

in vlan 20
ip add 20.20.20.1 255.255.255.0
exit

mlt 10 ena mem 2/3,1/10
mlt spanning-tree 10 stp all learning disable

mlt 30 ena mem 4/5,3/15
mlt spanning-tree 30 stp all learning disable

in mlt 30
ist peer-ip 200.200.200.1
ist vlan 200
ist ena
exit

in mlt 10
smlt 10
exit

in fast 2/20
smlt 20
exit

in vlan 100
\ip vrrp address 1 100.100.100.1
ip vrrp 1 enable backup-master enable
ip ospf enable
exit

in vlan 10
ip vrrp address 1 10.10.10.1
ip vrrp 2 enable backup-master enable
```

```
ip ospf enable
exit
```

```
in vlan 200
ip ospf enable
exit
```

```
in vlan 20
ip ospf enable
exit
```

```
router vrrp ena
router ospf ena
```

Configure DUT3.

```
vlan create 10 type port
vlan port 1/11,2/10,2/12,3/20 tag enable
vlan mem add 10 1/11,2/10,2/12,3/20
vlan mem rem 1 1/11,2/10,2/12,3/20,3/10
vlan mem add 10 3/10
vlan port 3/10 pvid 10
```

```
mlt 10 ena mem 1/11,2/10,2/12,3/20
mlt spanning-tree 10 stp all learning disable
```

Configure DUT4.

```
vlan create 10 type port
vlan port 1/20,2/10 tag enable
vlan mem add 100 1/20,2/10
vlan mem rem 1 1/20,2/10,1/10
vlan mem add 100 1/10
vlan port 1/10 pvid 100
```

```
mlt 20 ena mem 1/20,2/10
mlt spanning-tree 20 stp all learning disable
```

**Note:**

Valid license should be present on aggregation DUTs: DUT1 and DUT2.

## Square SMLT configuration

Square SMLT configuration requires two pairs of aggregation switches connected back to back (see Figure 23: SMLT in square configuration on page 82). Square configuration supports standalone switches.
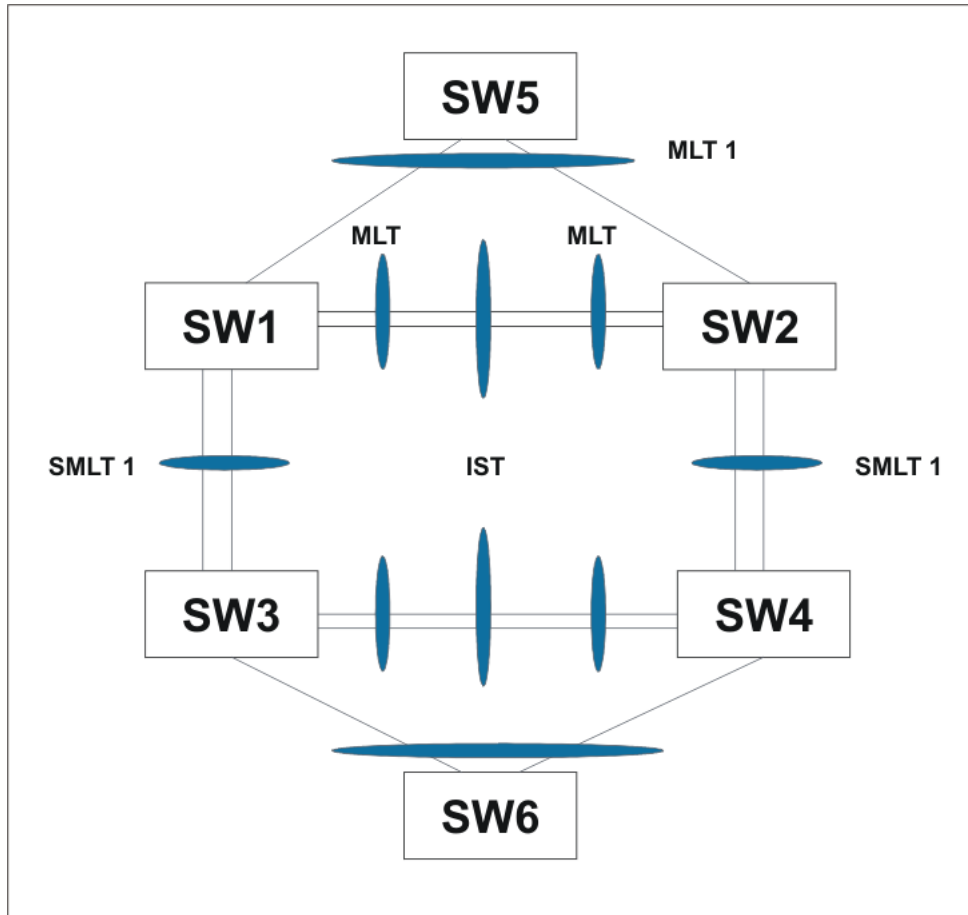
**Figure 23: SMLT in square configuration**

## Detailed configuration example for SMLT in square configuration

The following three diagrams describe the setup of SMLT in square configuration using VRRP for L3 routing. All devices are assumed to be 5000 Series devices.

Vlan 20 comprises Edge Device 1, SMLT 1 ports (MLT 1 ports) on 'A' and 'B' and the IST Ports (MLT 3 ports) on 'A' and 'B'.

Vlan 30 comprises Edge Device 2, SMLT 3 ports (MLT 1 ports) on 'C' and 'D' and IST Ports (MLT 3 ports ) on 'C' and 'D'.

Vlan 40 comprises SMLT 2 ports on 'A', 'B', 'C', 'D' (MLT 2 ports) and IST ports (MLT 3 ports) on 'A', 'B', 'C', 'D'.

IST Vlans (vlan 10 and all IST switches) have not been mentioned in figure 1 since they are internal to the system. These comprise only the IST ports in each IST switch.

IST ports on all switches need to be tagged ports. SMLT ports may be tagged or untagged.

Each of the IST switches will be running 2 VRRP instances.

- On switches 'A' and 'B', one VRRP instance will be running for Vlan 20 (VRID 20) and one for Vlan 40 (VRID 41).
- On switches 'C' and 'D', one VRRP instance will be running for Vlan 30 (VRID 30) and one for Vlan 40 (VRID 42).
- On switches 'A' and 'B', VRIP 40.0.0.42 (VRIP on 'C' and 'D') will be the next hop to reach the 30.0.0.0/24 network.
- On switches 'C' and 'D', VRIP 40.0.0.41 (VRIP on 'A' and 'B') will be the next hop to reach the 20.0.0.0/24 network.

Additionally, backup-master needs to be enabled on all switches for all VRs.

If MLTs or ports are part of multiple Vlans, ensure that their PVID is set appropriately.
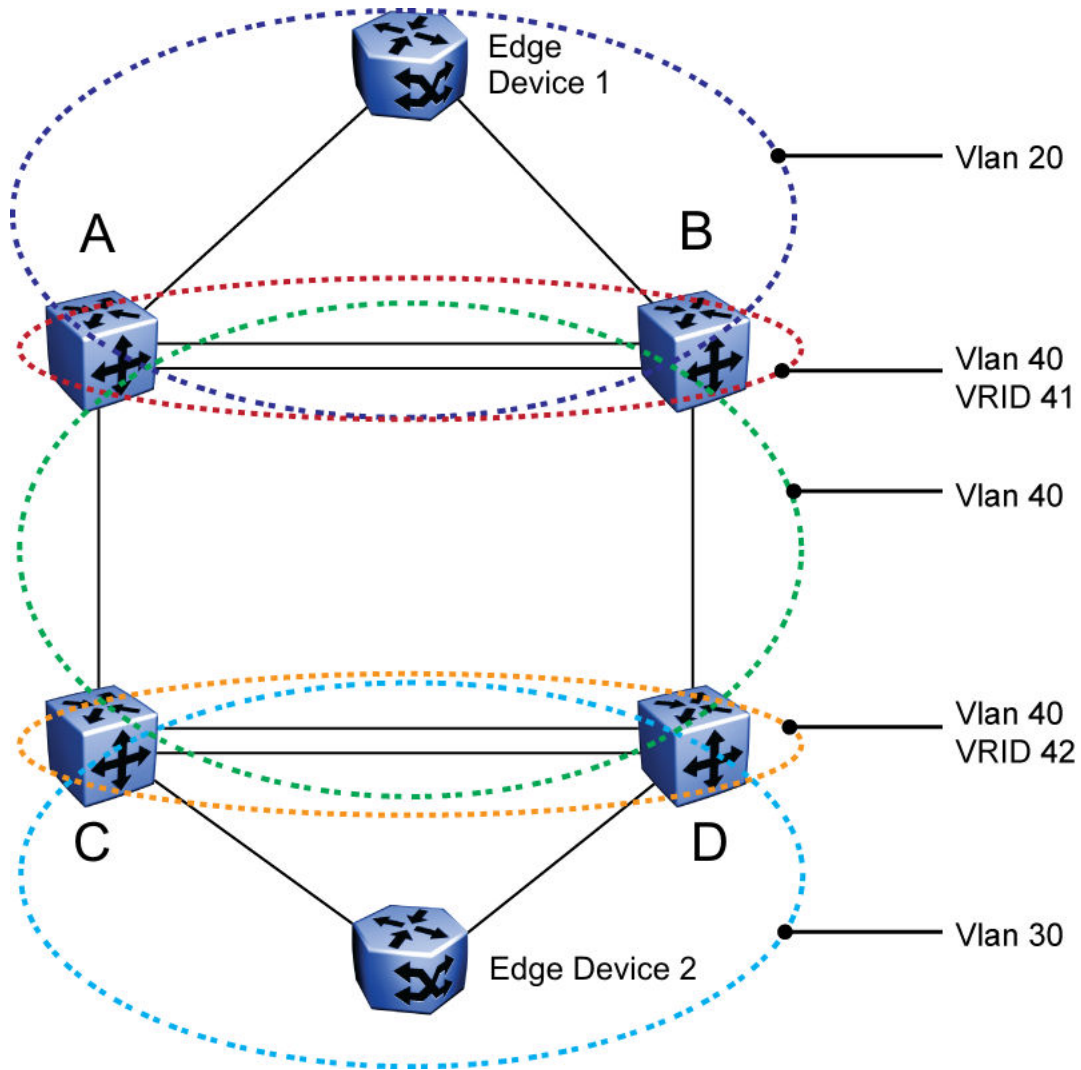
**Figure 24: Square VRRP SMLT setup. Vlans and VRRP (IST vlans not indicated)**
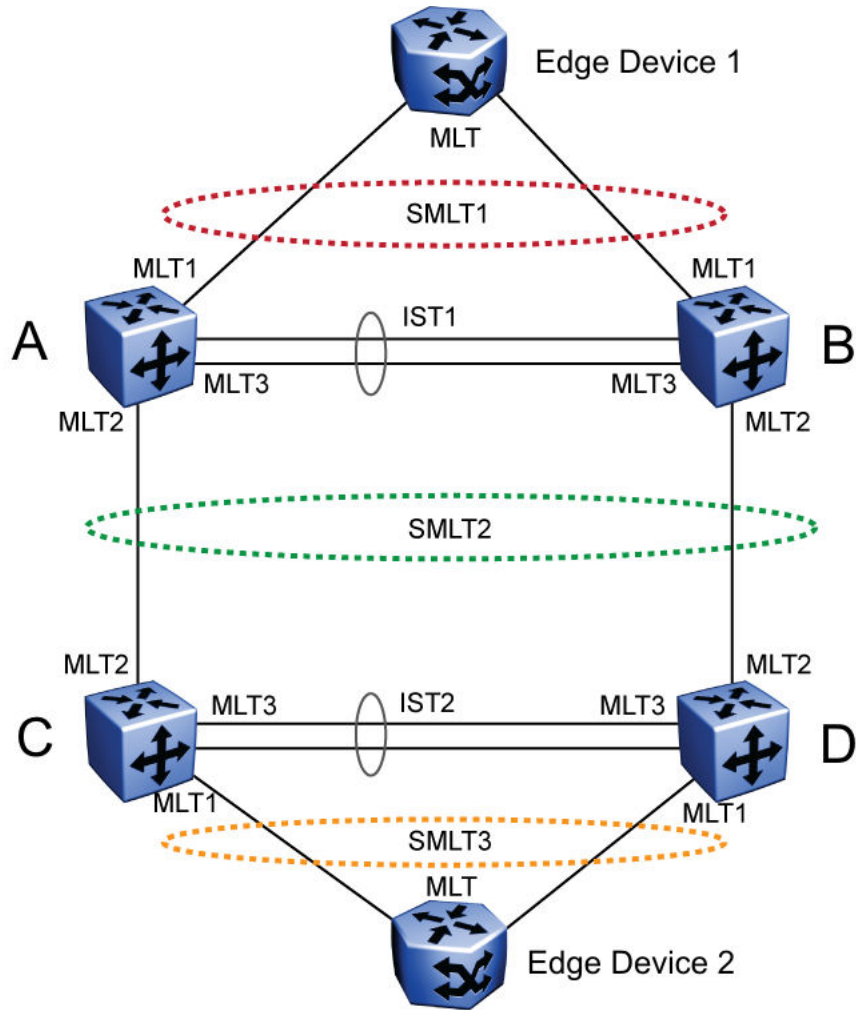
**Figure 25: Square VRRP SMLT setup. SMLTs and ISTs**
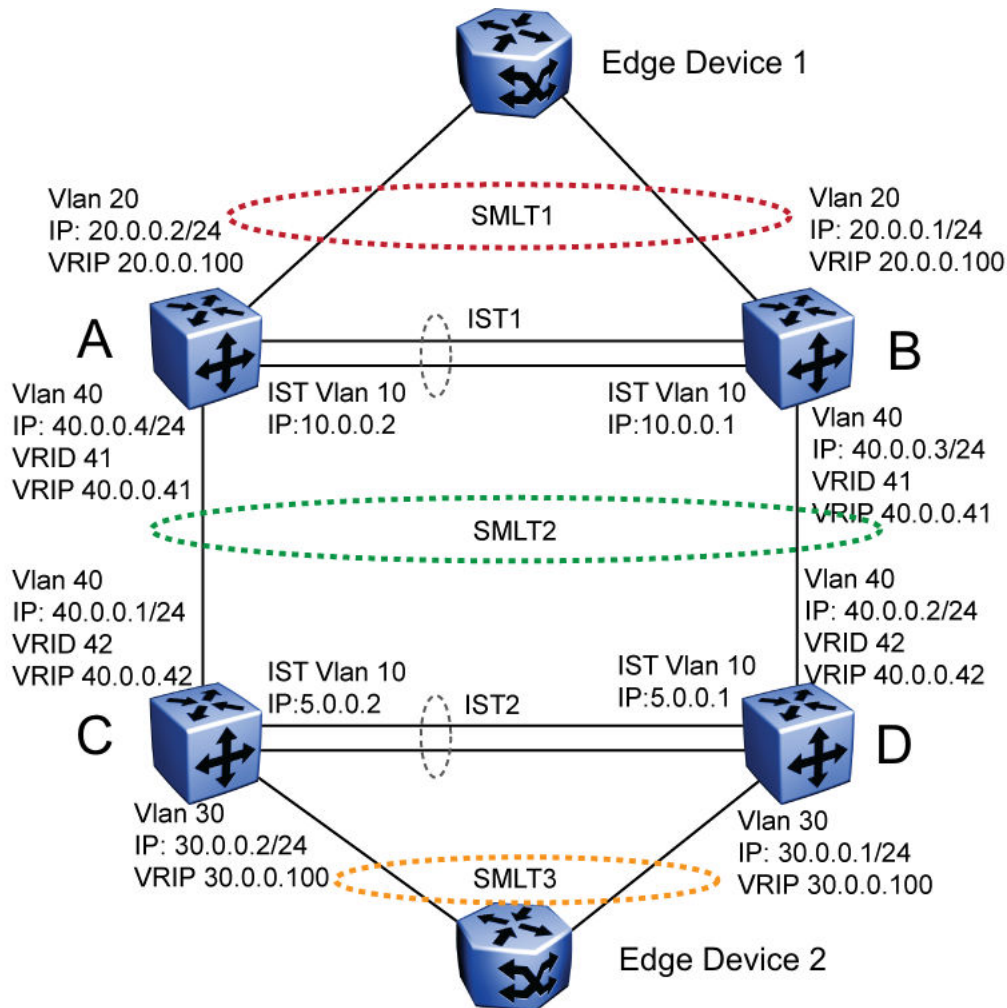
**Figure 26: Square VRRP SMLT setup. Interface and VRRP IP addresses**

The following paragraphs provide the configuration commands.

### Edge Device 1

```
enable
configure terminal
vlan members remove 1 all
vlan create 20 type port
vlan members add 20 all
mlt 1 enable members
5-8 learning disable
```

### Edge Device 2

```
enable
configure terminal
vlan members remove 1 all
vlan create 30 type port
```

```
vlan members add 30 all
 mlt 1 enable members 5-8 learning disable
```

**IST switch A**

```
enable
configure terminal
vlan configcontrol autopvid
ip routing
router vrrp enable
vlan
create 10 type port
vlan members add 10 3,4,5,6
interface vlan 10
ip address 10.0.0.2 255.255.255.0
exit
```

```
vlan create 20 type port
vlan members add 20 3,4,5,6,13,14
interface vlan 20
ip address 20.0.0.2 255.255.255.0
ip vrrp address 20 20.0.0.100
ip vrrp 20 enable backup-master enable
exit
```

```
 mlt 1 enable members 13,14 learning disable
interface mlt 1
smlt 1
exit
```

```
vlan create 40 type port
vlan members add
40 3,4,5,6,17,18
interface vlan 40
ip address 40.0.0.4 255.255.255.0
p vrrp address
41 40.0.0.41
iip vrrp 41 enable backup-master enable
exit
```

```
mlt 2 enable members 17,18 learning disable
interface mlt 2
smlt 2
exit
```

```
ip route 30.0.0.0 255.255.255.0 40.0.0.42 1
```

**IST switch B**

```
enable
configure terminal
vlan configcontrol autopvid ip routing
router vrrp
enable
vlan create 10 type port
```

```
vlan
members add 10 3,4,5,6
interface vlan 10
ip address 10.0.0.1 255.255.255.0
exit
```

```
vlan port 3,4,5,6 tagging enable pvid 10
mlt 3 enable members 3,4,5,6 learning disable
interface
mlt 3
ist enable peer-ip 10.0.0.2 vlan 10 exit
```

```
vlan create 20 type port
vlan members add
20 3,4,5,6,13,14
interface vlan 20
ip address 20.0.0.1 255.255.255.0
ip vrrp address 20 20.0.0.100
ip vrrp 20 enable backup-master enable
exit
```

```
mlt 1 enable members 13,14 learning disable
interface mlt 1
smlt 1
exit
```

```
vlan create 40 create type port
vlan members add 40 3,4,5,6,17,18
interface vlan 40
ip address 40.0.0.3 255.255.255.0
ip vrrp address 41 40.0.0.41
ip vrrp 41 enable backup-master enable
exit
```

```
mlt 2 enable members 17,18 learning disable
interface mlt 2
smlt 2
exit
```

```
ip route 30.0.0.0 255.255.255.0 40.0.0.42 1
```

### IST switch C

```
enable
configure terminal
vlan configcontrol autopvid
ip routing
```

```
router vrrp enable
vlan create 10 type port
vlan members add 10 3,4,5,6
interface vlan 10
```

```
ip address 5.0.0.1 255.255.255.0
exit
```

```
vlan port 3,4,5,6 tagging enable pvid 10
mlt 3 enable members 3,4,5,6 learning disable
interface mlt 3
ist enable peer-ip 5.0.0.2 vlan 10
exit
```

```
 vlan create 30 type port
vlan members add 30 3,4,5,6,13,14
interface vlan 30
ip address 30.0.0.1 255.255.255.0
ip vrrp address 30 30.0.0.100
ip vrrp 30 enable backup-master enable
exit
```

```
mlt 1 enable members 13,14 learning disable
interface mlt 1
smlt 1
exit
```

```
vlan create 40 create type port
vlan members add 40 3,4,5,6,17,18
interface vlan 40
ip address 40.0.0.2 255.255.255.0
ip vrrp address 42 40.0.0.42
ip vrrp 42 enable backup-master enable
mlt 2 enable members 17,18 learning disable
exit
```

```
interface mlt 2
smlt 2
exit
```

```
ip route 20.0.0.0 255.255.255.0 40.0.0.41 1
```

## IST switch D

```
enable
configure terminal
vlan configcontrol autopvid
ip routing
```

```
router vrrp enable
vlan create 10 type port
vlan members add 10 3,4,5,6
interface vlan 10
ip address 5.0.0.2 255.255.255.0
exit
```

```
vlan port 3,4,5,6 tagging enable pvid 10
mlt 3 enable members 3,4,5,6 learning disable
interface mlt 3
```

```
ist enable peer-ip 5.0.0.1 vlan 10
exit
```

```
vlan create 30 type port
vlan members add 30 3,4,5,6,13,14 interface
vlan 30 ip address 30.0.0.2 255.255.255.0
ip vrrp address 30 30.0.0.100
ip vrrp 30 enable backup-master enable
exit
```

```
mlt 1 enable members 13,14 learning disable
interface mlt 1
smlt 1
exit
```

```
vlan create 40 create type port
vlan members add 40 3,4,5,6,17,18
interface vlan 40
ip address 40.0.0.1 255.255.255.0
ip vrrp address 42 40.0.0.42
ip vrrp 42 enable backup-master enable
exit
```

```
mlt 2 enable members 17,18 learning disable
interface mlt 2
smlt 2
exit
```

```
ip route 20.0.0.0 255.255.255.0 40.0.0.41 1
```

## SMLT in full mesh configuration

The following section outlines the setup of SMLT in a full mesh configuration and provides the configuration commands.

### Edge Device 1

```
enable
configure terminal
vlan members remove 1 all
vlan create 20 type port
vlan members add 20 all
mlt 1 enable members 5-8 learning disable
```

### Edge Device 2

```
enable
configure terminal
vlan members remove 1 all
vlan create 30 type port
vlan members add 30 all
mlt 1 enable members 5-8 learning disable
```

## IST switch A

```
enable
configure terminal
vlan configcontrol autopvid

ip routing
router vrrp enable

vlan create 10 type port
vlan members add 10 3,4,5,6
interface vlan 10
ip address 10.0.0.2 255.255.255.0
exit
vlan port 3,4,5,6 tagging enable pvid 10
mlt 3 enable members 3,4,5,6 learning disable

interface mlt 3
ist enable peer-ip 10.0.0.1 vlan 10
exit

vlan create 20 type port
vlan members add 20 3,4,5,6,13,14
interface vlan 20
ip address 20.0.0.2 255.255.255.0
ip vrrp address 20 20.0.0.100
ip vrrp 20 enable backup-master enable
exit

mlt 1 enable members 13,14 learning disable
interface mlt 1
smlt 1
exit
vlan create 40 type port
vlan members add 40 3,4,5,6,17,18,19,20
interface vlan 40
ip address 40.0.0.4 255.255.255.0
ip vrrp address 41 40.0.0.41
ip vrrp 41 enable backup-master enable
exit

mlt 2 enable members 17,18,19,20 learning disable
interface mlt 2
smlt 2
exit

ip route 30.0.0.0 255.255.255.0 40.0.0.42 1
```

### IST switch B

```
enable
configure terminal
vlan configcontrol autopvid

ip routing
router vrrp enable

vlan create 10 type port
vlan members add 10 3,4,5,6
interface vlan 10
ip address 10.0.0.1 255.255.255.0
exit
vlan port 3,4,5,6 tagging enable pvid 10
mlt 3 enable members 3,4,5,6 learning disable
interface mlt 3
ist enable peer-ip 10.0.0.2 vlan 10
exit

vlan create 20 type port
vlan members add 20 3,4,5,6,13,14
interface vlan 20
ip address 20.0.0.1 255.255.255.0
ip vrrp address 20 20.0.0.100
ip vrrp 20 enable backup-master enable
exit

mlt 1 enable members 13,14 learning disable
interface mlt 1
smlt 1
exit

vlan create 40 create type port
vlan members add 40 3,4,5,6,17,18,19,20
interface vlan 40
ip address 40.0.0.3 255.255.255.0
ip vrrp address 41 40.0.0.41
ip vrrp 41 enable backup-master enable
exit

mlt 2 enable members 17,18,19,20 learning disable
interface mlt 2
smlt 2
exit

ip route 30.0.0.0 255.255.255.0 40.0.0.42 1
```

## IST switch C

```
enable
configure terminal
vlan configcontrol autopvid

ip routing
router vrrp enable

vlan create 10 type port
vlan members add 10 3,4,5,6
interface vlan 10
ip address 5.0.0.1 255.255.255.0
vlan port 3,4,5,6 tagging enable pvid 10
mlt 3 enable members 3,4,5,6 learning disable
interface mlt 3
ist enable peer-ip 5.0.0.2 vlan 10
exit

vlan create 30 type port
vlan members add 30 3,4,5,6,13,14
interface vlan 30
ip address 30.0.0.1 255.255.255.0
ip vrrp address 30 30.0.0.100
ip vrrp 30 enable backup-master enable
exit

mlt 1 enable members 13,14 learning disable
interface mlt 1
smlt 1
exit

vlan create 40 create type port
vlan members add 40 3,4,5,6,17,18,19,20
interface vlan 40
ip address 40.0.0.2 255.255.255.0
ip vrrp address 42 40.0.0.42
ip vrrp 42 enable backup-master enable
exit

mlt 2 enable members 17,18,19,20 learning disable
interface mlt 2
smlt 2
exit

ip route 20.0.0.0 255.255.255.0 40.0.0.41 1
```

### IST switch D

```
enable
configure terminal
vlan configcontrol autopvid
```

```
ip routing
router vrrp enable
```

```
vlan create 10 type port
vlan members add 10 3,4,5,6
interface vlan 10
ip address 5.0.0.2 255.255.255.0
exit
vlan port 3,4,5,6 tagging enable pvid 10
mlt 3 enable members 3,4,5,6 learning disable
interface mlt 3
ist enable peer-ip 5.0.0.1 vlan 10
exit
```

```
vlan create 30 type port
vlan members add 30 3,4,5,6,13,14
interface vlan 30
ip address 30.0.0.2 255.255.255.0
ip vrrp address 30 30.0.0.100
ip vrrp 30 enable backup-master enable
exit
```

```
mlt 1 enable members 13,14 learning disable
interface mlt 1
smlt 1]
exit
```

```
vlan create 40 create type port
vlan members add 40 3,4,5,6,17,18,19,20
interface vlan 40
ip address 40.0.0.1 255.255.255.0
ip vrrp address 42 40.0.0.42
ip vrrp 42 enable backup-master enable
exit
```

```
mlt 2 enable members 17,18,19,20 learning disable
interface mlt 2
smlt 2
exit
```

```
ip route 20.0.0.0 255.255.255.0 40.0.0.41 1
```

# SMLT in stack configuration

The SMLT aggregation switches can be a single switch or a stack. There is no restriction on the number of units in the SMLT stack, but for better recovery in case of failure, the stack should contain at least three units. If you use a stack of just two units, one unit leaving the stack leaves two isolated single units because all IST, SMLT, and SLT ports on these two units will be

disabled. For fastest recovery, SMLT should have at least one link connected to the base unit.

In a stack, the SMLT can be active only on the base unit or the temporary base unit, and it is solely responsible for the peer to peer switch communication. In stack mode, only the base unit or the temporary base unit can take ownership of the SMLT IST operations. The base unit keeps the master copy of the SMLT configuration and propagates the configuration during the data exchange cycle as it forms a stack. The base unit distributes the following information to the non-base unit:

- peer IP address
- IST MLT ID
- IST VLAN ID
- SMLT port information
- SLT port information

Each nonbase unit will get the SMLT configuration data from the base unit and will save it to its own NVRAM.

When a new unit joins the stack, the following checks must be successful:

- SMLT settings on the base unit can be configured on the new unit.
- The SMLT configuration programmed on the unit matches the SMLT configuration programmed on the base unit.
- The IST trunk is still enabled and active on the stack.

If one or more of these checks is not successful, the SMLT application will stop running, but SMLT will still be administratively enabled.

When a unit leaves the stack, SMLT will stop running on that unit and IST, SMLT and SLT will be disabled on all ports. The base unit will relay all of the resulting port down events to its SMLT peer.

When one unit in the stack becomes inactive, the stack responds as follows:

- If the base unit becomes inactive, the temporary base will take over.
- If a nonbase unit becomes inactive, the base unit will notify the rest of the stack with a list of all SMLT and SLT ports lost.
- If all of the IST ports were on the inactive unit, SMLT will stop running.

## 5000 Series switches as SMLT aggregation switches

The following figure illustrates an SMLT configuration with a pair of Ethernet Routing Switch 5000 Series devices (E and F) operating as aggregation switches. Also included are four separate user access switches (A, B, C, and D).
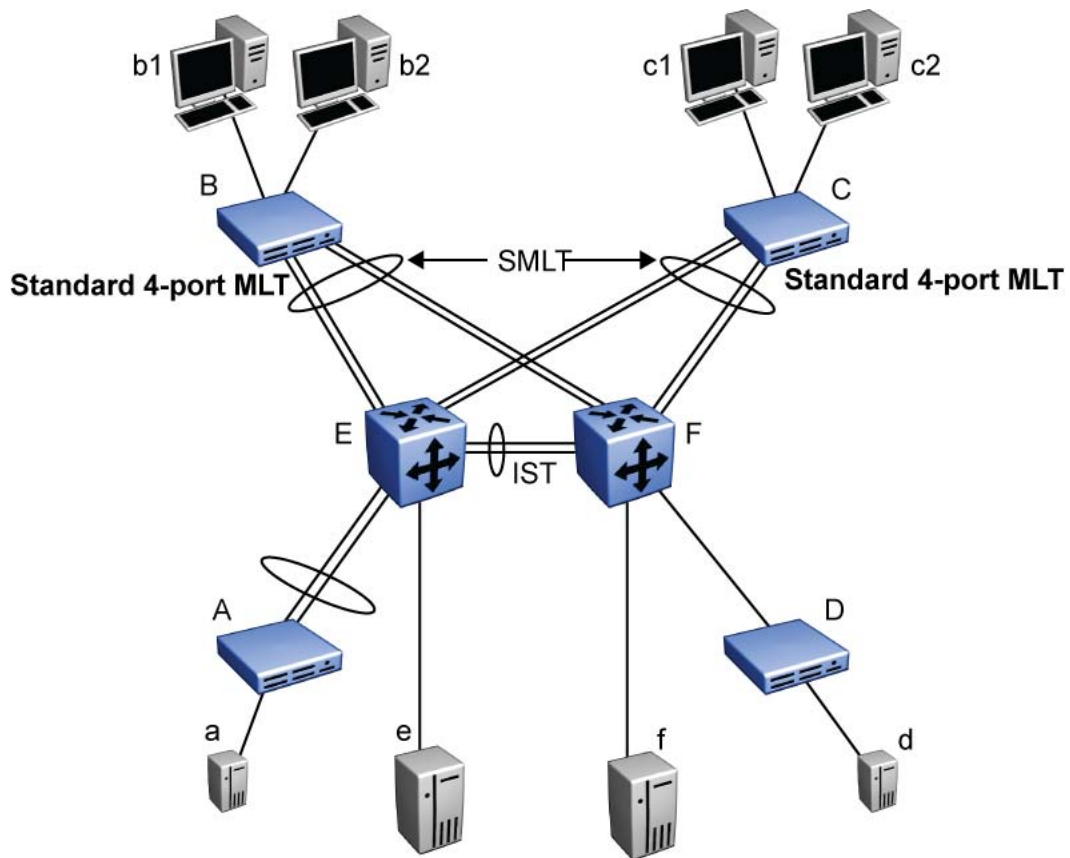
**Figure 27: 5000 Series switches as SMLT aggregation switches**

Refer to the following sections for a description of the components shown in this SMLT example:

- Inter-switch trunks (IST) on page 96
- Other SMLT aggregation switch connections on page 97

## Inter-switch trunks (IST)

The implementation of SMLT only requires two SMLT-capable aggregation switches. User access switches B and C do not support SMLT. They are connected to the aggregation switches E and F using standard Multi-Link trunks split between the two aggregation switches. To support this SMLT configuration, the aggregation switches must be connected through an Inter-switch trunk (IST).

**Important:**

For SMLT to function properly, you must manually disable STP on all SMLT, IST, and SLT ports in all spanning tree groups or instances to which the ports belong. You must also disable STP on all edge switch MLT ports that are connected to the SMLT or SLT.

Aggregation switches use the IST to:

• Confirm that they are alive and exchange MAC address forwarding tables.

• Send traffic between single switches attached to the aggregation switches.

• Serve as a backup if one SMLT link fails.

Because the IST is required for the proper operation of the SMLT, you must use multiple links aggregated in an IST MLT to ensure reliability and high availability.

When you set IST links between two 5000 Series devices, the switches must be running the identical software version.

Avaya also recommends that IST-linked switches run identical hardware. When the hardware is the same at both ends, you can more easily modify and maintain the IST configurations.

You can configure IST links on mixed 5000 Series hardware; however, in this case be sure that both devices have matching IST configurations.

5000 Series IST links cannot be partnered with Ethernet Routing Switch 8000 devices.

**Important:**

The Ethernet Routing Switch 5510 does not support IST MLTs configured with multiple STGs. To configure an IST with multiple STGs, you must use either the Ethernet Routing Switch 5520 or 5530.

In addition to the IST VLAN, IST ports must also belong to all SMLT VLANs (as well as any other non-SMLT VLANs that require the IST to carry traffic between the switches.) As a result, IST ports must be tagged ports because they span these multiple VLANs.

# Other SMLT aggregation switch connections

In this example, a, b1, b2, c1, c2, and d are clients and printers, while e and f can be servers or routers.

User-access switches B and C can use any method for determining which link of their Multi-Link trunk connections to use for forwarding a packet, as long as the same link is used for a given Source Address/Destination Address (SA/DA) pair. This is true, regardless of whether the DA is known by B or C. SMLT aggregation switches always send traffic directly to a user access switch and only use the IST for traffic that they cannot forward in another more direct way.

The examples that follow explain the process in more detail.

-
-
-
-

## Example 1- Traffic flow from a to b1 or b2

Assuming a and b1/b2 are communicating through Layer 2, traffic flows from A to switch E and is then forwarded over the direct link from switch E to B. Traffic coming from b1 or b2 to a is sent by B on one of its MLT ports.

B can send traffic from b1 to a on the link to switch E, and send traffic from b2 to a on the link to F. In the case of traffic from b1, switch E forwards the traffic directly to switch A, while traffic from b2, which arrives at F, is forwarded across the IST to E and then on to A.

## Example 2- Traffic flow from b1/b2 to c1/c2

Traffic from b1/b2 to c1/c2 is always sent by switch B down its MLT to the core. No matter which switch (E or F) the traffic arrives at, the switch directs traffic to C through the local link.

## Example 3- Traffic flow from a to d

Traffic from a to d and vice versa is forwarded across the IST because it is the shortest path. This path is treated purely as a standard link with no account taken of SMLT or the fact that the link is an IST.

## Example 4- Traffic flow from f to c1/c2

Traffic from f to c1/c2 is sent out directly from F. Return traffic from c1/c2 can flow directly to f if switch C forwards the traffic to F. Otherwise, the return traffic passes across the IST after switch C sends it down the link to E.

# SLT

With Single Link Trunking (SLT) you can configure a split Multi-Link trunk using a single port. The single port SLT behaves like an MLT-based SMLT and can coexist with SMLTs in the same system. With SLT, you can scale the number of split Multi-Link trunks on a switch to the maximum number of available ports.

**Important:**

For SMLT to function properly, you must manually disable STP on all SMLT, IST, and SLT ports in all spanning tree groups or instances to which the ports belong. You must also disable STP on all edge switch MLT ports that are connected to the SMLT or SLT.

SMLT and SLT links can exist in the following combinations on the SMLT aggregation switch pair:

- MLT-based SMLT + MLT-based SMLT

- MLT-based SMLT + SLT

- SLT + SLT

Rules for configuring SLTs:

- The dual-homed device connected to the aggregation switches must be capable of supporting MLT.

- Each SLT is assigned an SMLT ID from 1 to 512. (The actual number of SLTs is limited only by the number of available ports on the device, minus two that must be reserved for the IST connection. For example, with a 48-port unit, you can configure a maximum of 46 SLTs.)

- SLT ports can be designated as Access or Trunk (that is, IEEE 802.1Q tagged or not tagged) and changing the type does not affect their behavior.

- You cannot change an SLT into an MLT-based SMLT by adding more ports. You must first delete the SLT, and then reconfigure the port as SMLT/MLT.

- You cannot change an MLT-based SMLT into a SLT by deleting all ports but one. You must first remove the SMLT, delete the MLT, and then reconfigure the port as an SLT.

- A port cannot be configured as an MLT-based SMLT and as an SLT at the same time.

Figure 28: SLT example on page 100shows a configuration in which both aggregation switches have single port SLTs with the same IDs. This configuration allows as many SLTs, as available ports exist on the switch.
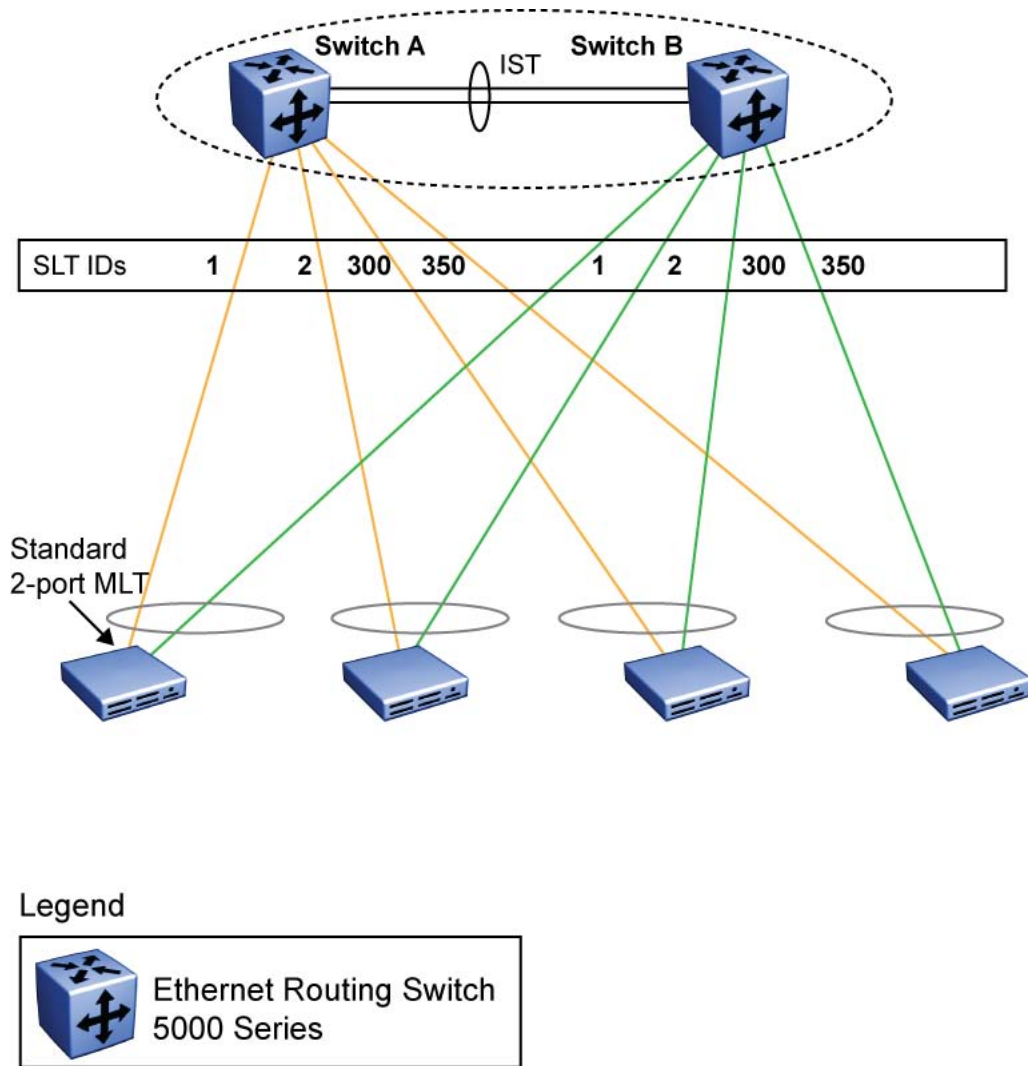
**Figure 28: SLT example**

# Using SMLT with SLT

You can configure a split trunk with an SLT on one side and an MLT-based SMLT on the other. Both must have the same SMLT ID. In addition to general use, Figure 29: Changing a split trunk from MLT-based SMLT to SLT on page 101 shows how this configuration can be used for upgrading an MLT-based SMLT to an SLT without taking down the split trunk.
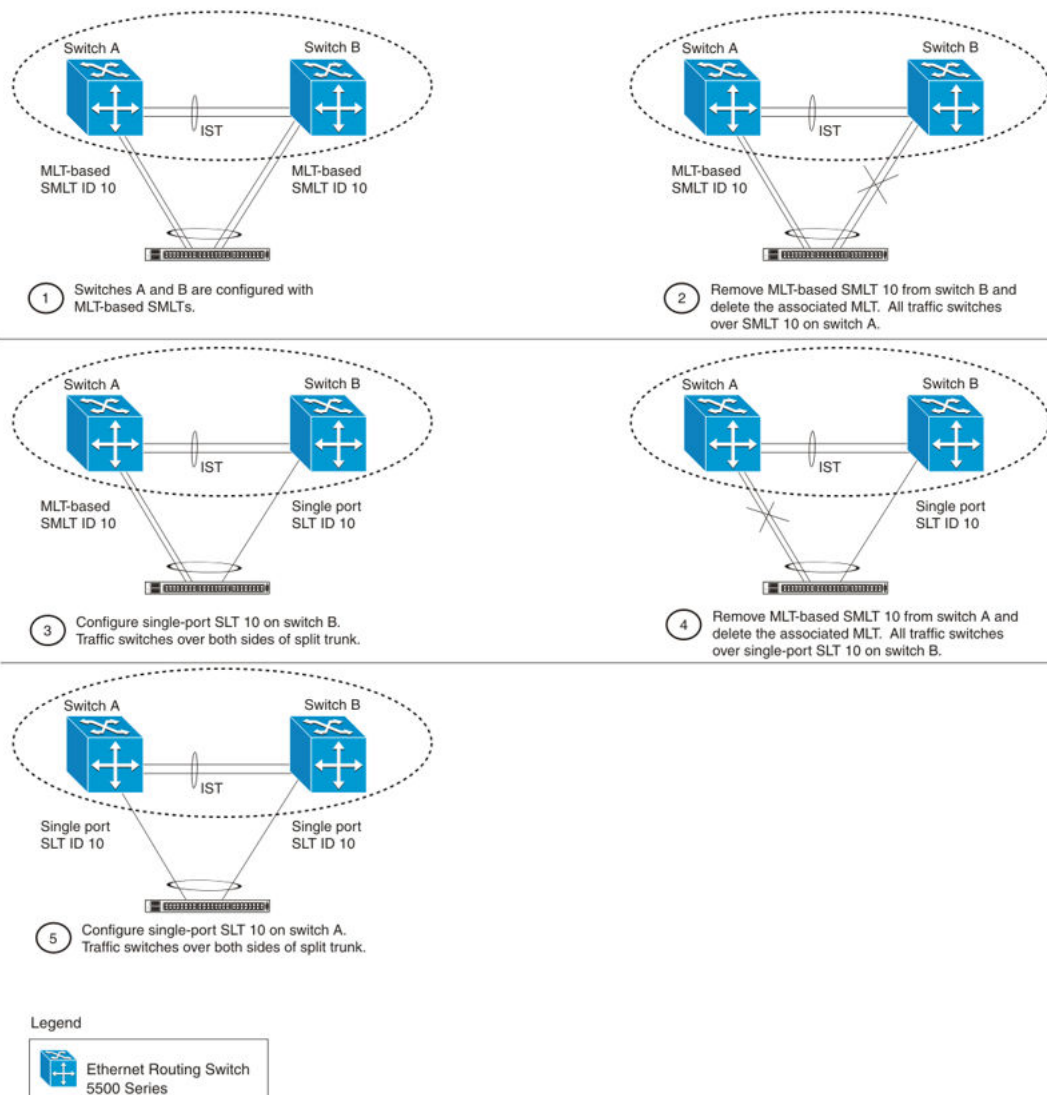
**Figure 29: Changing a split trunk from MLT-based SMLT to SLT**

**Important:**

When you perform the steps listed in Figure 29: Changing a split trunk from MLT-based SMLT to SLT on page 101 and you remove the MLT-based SMLTs (steps 2 and 4), physically disable the ports by removing the cables or by shutting the ports down using the ACLI. Otherwise, because STP is disabled on the ports, a loop can form as soon as the SMLT is removed.

# SMLT and SLT Configuration steps

To enable SMLTs, ISTs, and SLTs on the 5000 Series switches, you must complete the following steps in the order indicated.

**Important:**

For SMLT to function properly, you must manually disable STP on all SMLT, IST, and SLT ports in all spanning tree groups or instances to which the ports belong. You must also disable STP on all edge switch MLT ports that are connected to the SMLT or SLT.

1. Configure VLANs, including port membership, VLAN IP, and port tagging.

2. Configure STP groups:

    a. Create STP groups.

    b. Assign VLAN membership.

    c. Enable STP groups.

    d. Set STP port participation.

3. Enable Global IP Routing on the devices (always required).

4. If the switches are to be used for Layer 3 routing, enable VRRP on the units (required for Layer 3 only).

5. Configure MLTs on the devices:

    a. Create MLT groups by assigning trunk members.

    b. Disable STP participation on all trunk member ports.

    c. Enable the MLTs.

6. Configure SMLTs on the devices:

    a. Assign the Peer IP address and VLAN ID to the IST MLT.

    b. Enable the IST.

    c. Create the SMLTs.

    d. Create the SLTs (if applicable).

7. Make IST connections and ensure IST session is running.

8. Make SMLT/SLT connections and check SMLT/SLT status.

**Note:**

These are the recommended steps for a new installation. For existing networks, perform steps 1 through 6 as closely as possible. To minimize loops, you can perform step 5 before steps 1 through 4.

To disable SMLTs and SLTs, perform the same steps in reverse order.

## SMLT configuration example with VRRP and OSPF

Figure 30: SMLT configuration example with VRRP and OSPF on page 103 shows an example of aggregation switches configured with SMLT, VRRP, and OSPF. For more information on VRRP and OSPF, see *Avaya Ethernet Routing Switch 5000 Series Configuration — IP Routing Protocols* , NN47200-503.
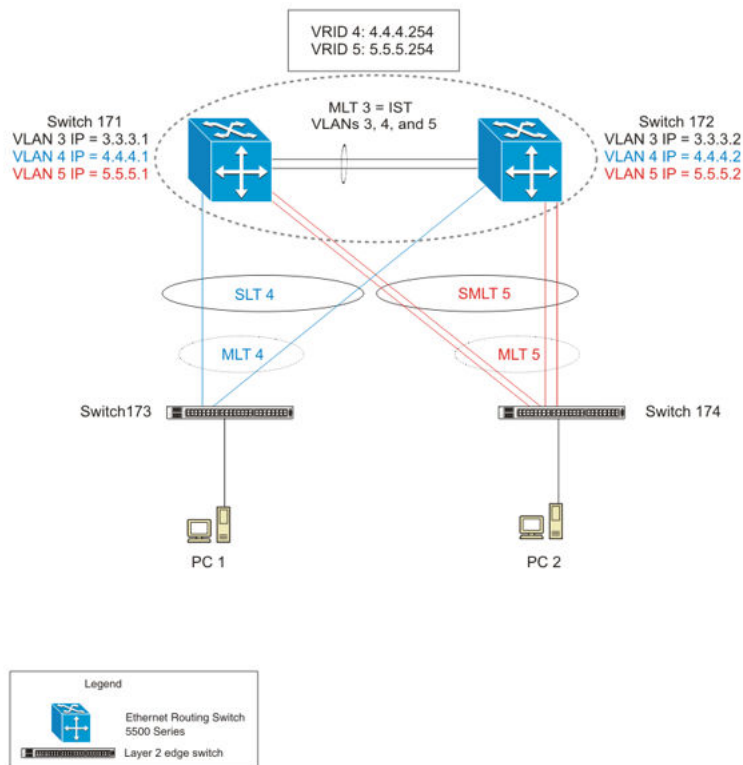
**Figure 30: SMLT configuration example with VRRP and OSPF**

To configure the example shown in Figure 30: SMLT configuration example with VRRP and OSPF on page 103, you must perform the following tasks:

### For aggregation switch 171

1. Create VLANs 3, 4, and 5.

2. Set ports 1-5 as tagging.

3. Assign ports 1 and 2 to VLAN 3.

4. Assign ports 1, 2 and 3 to VLAN 4.

5. Assign ports 1, 2, 4 and 5 to VLAN 5.

6. Set VLAN 3 IP to 3.3.3.1 .

7. Set VLAN 4 IP to 4.4.4.1 .

8. Set VLAN 5 IP to 5.5.5.1 .

9. Enable IP routing globally.

10. Create MLT 3 with ports 1 and 2.

11. Disable STP on ports 1 and 2.

12. Set IST = MLT 3, Peer IP=3.3.3.2, VLAN 3.

13. Disable STP on port 3 and configure it as SLT with SMLT ID 4.

14. Create MLT 5 with ports 4 to 5.

15. Disable STP on ports 4 to 5.

16. Set MLT 5 as SMLT 5.

17. Enable VRRP globally.

18. Enable VRRP on VLAN 4 with VRID 4 and VRIP 4.4.4.254.

19. Enable VRRP back up master.

20. Enable VRRP on VLAN 5 with VRID 5 and VRIP 5.5.5.254.

21. Enable VRRP back up master.

22. Enable OSPF globally.

23. Enable OSPF on VLANs 3,4 and 5.

**For aggregation switch 172**

1. Create VLANs 3, 4, and 5.

2. Set ports 1 to 5 as tagging.

3. Assign ports 1 and 2 to VLAN 3.

4. Assign ports 1, 2 and 3 to VLAN 4.

5. Assign ports 1, 2, 4 and 5 to VLAN 5.

6. Set VLAN 3 IP to 3.3.3.2.

7. Set VLAN 4 IP to 4.4.4.2.

8. Set VLAN 5 IP to 5.5.5.2.

9. Enable IP routing.

10. Create MLT 3 with ports 1 and 2.

11. Disable STP on ports 1 and 2.

12. Set IST = MLT 3, Peer IP=3.3.3.1, VLAN 3.

13. Disable STP on port 3 and configure it as SLT with SMLT ID 4.

14. Create MLT 5 with ports 4 to 5.

15. Disable STP on ports 4 to 5.

16. Set MLT 5 as SMLT 5.

17. Enable VRRP globally.

18. Enable VRRP on VLAN 4 with VRID 4 and VRIP 4.4.4.254.

19. Enable VRRP back up master.

20. Enable VRRP on VLAN 5 with VRID 5 and VRIP 5.5.5.254.

21. Enable VRRP back up master.

22. Enable OSPF globally.

23. Enable OSPF on VLAN 3, 4, and 5

### For edge switch 173

1. Create Vlan 4.

2. Assign ports 3 to 4 to Vlan 4.

3. Create MLT 4 with ports 3 to 4.

4. Disable STP on MLT 4.

### For edge switch 174

1. Create Vlan 5.

2. Assign ports 3 to 6 to Vlan 5.

3. Create MLT 5 with ports 3 to 6.

4. Disable STP on MLT 5.

## Detailed configuration commands

### Aggregation switch 171 configuration
### IST, SMLT and SLT configuration

```
5520-48T-PWR(config)#vlan create 3 type port
5520-48T-PWR(config)#vlan create 4 type port
5520-48T-PWR(config)#vlan create 5 type port
5520-48T-PWR(config)#vlan port 1-5 tagging enable
5520-48T-PWR(config)#vlan member add 3 1-2
5520-48T-PWR(config)#vlan member add 4 1-2
5520-48T-PWR(config)#vlan member add 5 1-2
5520-48T-PWR(config)#vlan member remove 1 1-5
5520-48T-PWR(config)#vlan member add 4 3
5520-48T-PWR(config)#vlan member add 5 4,5
5520-48T-PWR(config)#ip routing
```

```
5520-48T-PWR(config)#interface vlan 3
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 3.3.3.1 255.255.255.0
5520-48T-PWR(config-if)#exit
```

```
5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip routing
```

```
5520-48T-PWR(config-if)#ip address 4.4.4.1 255.255.255.0
5520-48T-PWR(config-if)#exit

5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 5.5.5.1 255.255.255.0
5520-48T-PWR(config-if)#exit

5520-48T-PWR(config)#mlt 3 member 1-2
5520-48T-PWR(config)#mlt spanning-tree 3 stp all learning disable
5520-48T-PWR(config)#mlt 3 enable
5520-48T-PWR(config)#interface mlt 3
5520-48T-PWR(config-if)#ist enable peer-ip 3.3.3.2 vlan 3
5520-48T-PWR(config-if)#exit

5520-48T-PWR(config)#interface fastEthernet 3
5520-48T-PWR(config-if)#spanning-tree learning disable
5520-48T-PWR(config-if)#smlt 4
5520-48T-PWR(config-if)#exit

5520-48T-PWR(config)#mlt 5 member 4-5
5520-48T-PWR(config)#mlt spanning-tree 5 stp all learning disable
5520-48T-PWR(config)#mlt 5 enable
5520-48T-PWR(config-if)#interface mlt 5
5520-48T-PWR(config-if)#smlt 5
5520-48T-PWR(config-if)#exit
```

### VRRP and OSPF

```
5520-48T-PWR(config)#router vrrp enable
5520-48T-PWR(config)#router ospf enable
5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip vrrp address 4 4.4.4.254
5520-48T-PWR(config-if)#ip vrrp 4 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit

5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip vrrp address 5 5.5.5.254
5520-48T-PWR(config-if)#ip vrrp 5 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable 5520-48T-PWR(config-if)#exit
```

### Aggregation switch 172 configuration

### IST, SMLT and SLT configuration

```
5520-48T-PWR(config)#vlan create 3 type port
5520-48T-PWR(config)#vlan create 4 type port
5520-48T-PWR(config)#vlan create 5 type port
5520-48T-PWR(config)#vlan port 1-5 tagging enable
5520-48T-PWR(config)#vlan member add 3 1-2
5520-48T-PWR(config)#vlan member add 4 1-2
5520-48T-PWR(config)#vlan member add 5 1-2
5520-48T-PWR(config)#vlan member remove 1 1-5
5520-48T-PWR(config)#vlan member add 4 3
```

```
5520-48T-PWR(config)#vlan member add 5 4,5
5520-48T-PWR(config)#ip routing
```

```
5520-48T-PWR(config)#interface vlan 3
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 3.3.3.2 255.255.255.0
5520-48T-PWR(config-if)#exit
```

```
5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 4.4.4.2 255.255.255.0
5520-48T-PWR(config-if)#exit
```

```
5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 5.5.5.2 255.255.255.0
5520-48T-PWR(config-if)#exit
```

```
5520-48T-PWR(config)#mlt 3 member 1-2
5520-48T-PWR(config)#mlt spanning-tree 3 stp all learning disable
5520-48T-PWR(config)#mlt 3 enable
5520-48T-PWR(config)#interface mlt 3
5520-48T-PWR(config-if)#ist enable peer-ip 3.3.3.1 vlan 3
5520-48T-PWR(config-if)#exit
```

```
5520-48T-PWR(config)#interface fastEthernet 3
5520-48T-PWR(config-if)#spanning-tree learning disable
5520-48T-PWR(config-if)#smlt 4
5520-48T-PWR(config-if)#exit
```

```
5520-48T-PWR(config)#mlt 5 member 4-5
5520-48T-PWR(config)#mlt spanning-tree 5 stp all learning disable
5520-48T-PWR(config)#mlt 5 enable
5520-48T-PWR(config-if)#interface mlt 5
5520-48T-PWR(config-if)#smlt 5
5520-48T-PWR(config-if)#exit
```

## VRRP and OSPF

```
5520-48T-PWR(config)#router vrrp enable
5520-48T-PWR(config)#router ospf enable
5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip vrrp address 4 4.4.4.254
5520-48T-PWR(config-if)#ip vrrp 4 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit
```

```
5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip vrrp address 5 5.5.5.254
5520-48T-PWR(config-if)#ip vrrp 5 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit
```

### Edge switch 173 configuration (5000 Series)

```
5510-48T(config)#vlan create 4 type port
 5510-48T(config)#vlan port 3-4 tagging enable
5510-48T(config)#vlan member add 4 3-4
5510-24T(config)#mlt 4 member 3-4
5510-24T(config)#mlt spanning-tree 4 stp all learning disable
5510-24T(config)#mlt 4 enable
```

### Edge switch 174 configuration (5000 Series)

```
5510-48T(config)#vlan create 5 type port
 5510-48T(config)#vlan port 3-6 tagging enable
5510-48T(config)#vlan member add 5 3-6
5510-24T(config)#mlt 5 member 3-6
5510-24T(config)#mlt spanning-tree 5 stp all learning disable
5510-24T(config)#mlt 5 enable
```

## SLT configuration example with VRRP and OSPF

on page 109shows an example of aggregation switches configured with SLT, VRRP and OSPF. For more information on VRRP and OSPF, see *Avaya Ethernet Routing Switch 5000 Series Configuration — IP Routing Protocols*, NN47200-503.
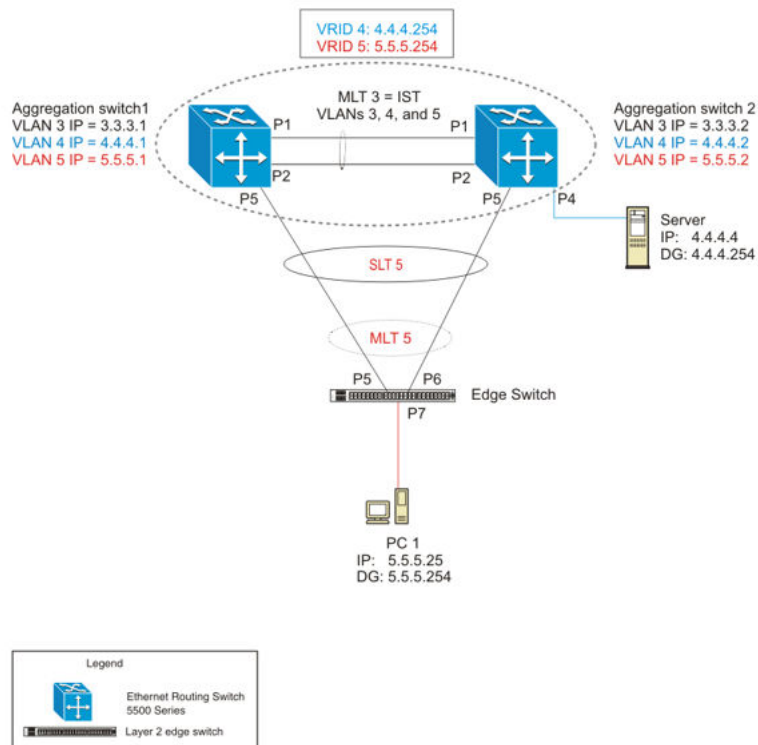
**Figure 31: SLT configuration example with VRRP and OSPF**

To configure the example shown in Figure 31: SLT configuration example with VRRP and OSPF on page 109, you must perform the following tasks.

### For aggregation switch 1:

1. Create VLANs 3, 4, and 5.
2. Set ports 1 to 5 as tagging.
3. Assign ports 1 and 2 to VLAN 3.
4. Assign ports 1, 2 and 4 to VLAN 4.
5. Assign ports 1, 2, and 5 to VLAN 5.
6. Set VLAN 3 IP to 3.3.3.1 .
7. Set VLAN 4 IP to 4.4.4.1 .
8. Set VLAN 5 IP to 5.5.5.1 .
9. Enable IP routing globally.
10. Create MLT 3 with ports 1-2.
11. Disable STP on ports 1-2.

12. Set IST = MLT 3, Peer IP=3.3.3.2, VLAN 3.

13. Disable STP on port 5.

14. Set port 5 as SLT 5.

15. Enable VRRP globally

16. Enable VRRP on VLAN 4 with VRID 4 and VRIP 4.4.4.254.

17. Enable VRRP back up master.

18. Enable VRRP on VLAN 5 with VRID 5 and VRIP 5.5.5.254 .

19. Enable VRRP back up master.

20. Enable OSPF globally.

21. Enable OSPF on VLANs 3,4 and 5.

**For aggregation switch 2:**

1. Create VLANs 3, 4, and 5.

2. Set ports 1 to 5 as tagging.

3. Assign ports 1 and 2 to VLAN 3.

4. Assign ports 1, 2 and 4 to Vlan 4.

5. Assign ports 1, 2 and 5 to Vlan 5.

6. Set Vlan 3 IP to 3.3.3.2.

7. Set Vlan 4 IP to 4.4.4.2.

8. Set Vlan 5 IP to 5.5.5.2.

9. Enable IP routing.

10. Create MLT 3 with ports 1 and 2.

11. Disable STP on ports 1 and 2.

12. Set IST = MLT 3, Peer IP=3.3.3.1, Vlan 3.

13. Disable STP on port 5.

14. Set port 5 as SLT 5.

15. Enable VRRP globally.

16. Enable VRRP on Vlan 4 with VRID 4 and VRIP 4.4.4.254.

17. Enable VRRP back up master.

18. Enable VRRP on Vlan 5 with VRID 5 and VRIP 5.5.5.254.

19. Enable VRRP back up master.

20. Enable OSPF globally.

21. Enable OSPF on Vlan 3, 4 and 5.

**For edge switch 1:**

1. Create Vlan 4.
2. Assign ports 5 to 7 to Vlan 4.
3. Create Vlan 5.
4. Assign ports 5 to 7 to Vlan 5.
5. Create MLT 5 with ports 5 to 6

# Detailed configuration commands

The following sections describe the detailed ACLI commands required to carry out the configuration described in Figure 31: SLT configuration example with VRRP and OSPF on page 109

## Aggregation switch 1 configuration

## IST, SMLT and SLT configuration

```
5520-48T-PWR(config)#vlan create 3 type port
5520-48T-PWR(config)#vlan create 4 type port
5520-48T-PWR(config)#vlan create 5 type port
5520-48T-PWR(config)#vlan port 1,2,4,5 tagging enable
5520-48T-PWR(config)#vlan member add 3 1-2
5520-48T-PWR(config)#vlan member add 4 1-2,4
5520-48T-PWR(config)#vlan member add 5 1,2,5
5520-48T-PWR(config)#vlan member remove 1 1-5
5520-48T-PWR(config)#ip routing

5520-48T-PWR(config)#interface vlan 3
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 3.3.3.1 255.255.255.0
5520-48T-PWR(config-if)#exit

5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 4.4.4.1 255.255.255.0
5520-48T-PWR(config-if)#exit

5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 5.5.5.1 255.255.255.0
5520-48T-PWR(config-if)#exit

5520-48T-PWR(config)#mlt 3 member 1-2
5520-48T-PWR(config)#mlt spanning-tree 3 stp all learning disable
5520-48T-PWR(config)#mlt 3 enable
5520-48T-PWR(config)#interface mlt 3
5520-48T-PWR(config-if)#ist enable peer-ip 3.3.3.2 vlan 3
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface fastEthernet 5
5520-48T-PWR(config-if)#spanning-tree learning disable
```

```
5520-48T-PWR(config-if)#smlt 5
5520-48T-PWR(config-if)#exit
```

### VRRP and OSPF

```
5520-48T-PWR(config)#router vrrp enable
 5520-48T-PWR(config)#router ospf enable
5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip vrrp address 4 4.4.4.254
5520-48T-PWR(config-if)#ip vrrp 4 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit

5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip vrrp address 5 5.5.5.254
5520-48T-PWR(config-if)#ip vrrp 5 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit
```

### Aggregation switch 2 configuration

### IST, SMLT and SLT configuration

```
5520-48T-PWR(config)#vlan create 3 type port
5520-48T-PWR(config)#vlan create 4 type port
5520-48T-PWR(config)#vlan create 5 type port
5520-48T-PWR(config)#vlan port 1-5 tagging enable
5520-48T-PWR(config)#vlan member add 3 1-2
5520-48T-PWR(config)#vlan member add 4 1,2,4
5520-48T-PWR(config)#vlan member add 5 1,2,5
5520-48T-PWR(config)#vlan member remove 1 1-5
5520-48T-PWR(config)#ip routing

5520-48T-PWR(config)#interface vlan 3
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 3.3.3.2 255.255.255.0
5520-48T-PWR(config-if)#exit

5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 4.4.4.2 255.255.255.0
5520-48T-PWR(config-if)#exit

5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 5.5.5.2 255.255.255.0
5520-48T-PWR(config-if)#exit

5520-48T-PWR(config)#mlt 3 member 1-2
 5520-48T-PWR(config)#mlt spanning-tree 3 stp all learning disable
5520-48T-PWR(config)#mlt 3 enable
5520-48T-PWR(config)#interface mlt 3
5520-48T-PWR(config-if)#ist enable peer-ip 3.3.3.1 vlan 3
5520-48T-PWR(config-if)#exit

5520-48T-PWR(config)#interface fastEthernet 5
5520-48T-PWR(config-if)#spanning-tree learning disable
```

```
5520-48T-PWR(config-if)#smlt 5
5520-48T-PWR(config-if)#exit
```

### VRRP and OSPF

```
5520-48T-PWR(config)#router vrrp enable
5520-48T-PWR(config)#router ospf enable
5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip vrrp address 4 4.4.4.254
5520-48T-PWR(config-if)#ip vrrp 4 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit
```

```
5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip vrrp address 5 5.5.5.254
5520-48T-PWR(config-if)#ip vrrp 5 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit
```

### Edge switch configuration (5000 Series)

```
5510-48T(config)#vlan create 5 type port
5510-48T(config)#vlan member add 5 5-7
5510-48T(config)#vlan port 5-6 tagging enable
5510-48T(config)#vlan member remove 1 5-7
5510-24T(config)#mlt 5 member 5-6
5510-24T(config)#mlt spanning-tree 5 stp all learning disable
5510-24T(config)#mlt 5 enable
```

# SLPP

Simple Loop Prevention Protocol (SLPP) is a new feature designed to detect loops in a SMLT network. Not intended to replace STP as a comprehensive loop detection mechanism, SLPP acts as a secondary mechanism for detection and prevention of looping in a SMLT environment and can only be configured on SMLT networks. Since SMLT requires that STP be disabled on IST, SMLT and SLT ports for normal operation, loops may be introduced to a network. SLPP was designed to prevent such loops and resulting traffic disruptions.

When enabled, SLPP causes the switch to send a periodic SLPP PDU on the transmitting VLAN at a user defined or default (500 ms) transmission interval. If a loop is active in the network, the SLPP PDU is returned to the switch and the affected port is shutdown after the specified number of PDU has been received (Default is 5). If a port is shutdown as the result of a detected loop, it must be manually returned to an active state by the network administrator unless auto enable is configured. SLPP only sends a PDU to VLANs specified in the transmitting list configured by the user.

> **Note:**
>
> When configured in addition to STP, STP operation will take precedence leaving SLPP as a supplementary measure for loop detection.

# Link Aggregation Control Protocol over SMLT

Link Aggregation Control Protocol (LACP) over SMLT results in better recovery for SMLT and SLT-configured trunks in fail-over scenarios such as when a stack link breaks.

LACP dynamically creates and removes trunk groups. In the absence of STP on the SMLT network, configuration errors can easily introduce a loop. To limit loops, IST links do not support LACP: only SMLT and SLT links support LACP.

To prevent the formation of a loop, you must configure the same speed (10/100/1000) for LAC ports on an edge switch and LAC ports on an SMLT aggregation switch. If port speeds do not match, multiple LAC trunks form which can create a loop on the network.

Two SMLT aggregation switches act as a single, logical LACP peer to the edge switch; therefore, both switches must use the same Link Aggregation Control (LAC) system-ID in transmit Protocol Data Units (PDU) for SMLT and SLT ports. You can configure the LAC system-ID.

Avaya recommends that you enable SLPP to protect the network from broadcast storms.

# SMLT with Routing protocol support

This feature uses Open Shortest Path First (OSPF) to distribute routes across the SMLT/SLT network. This route distribution reduces the administrative load route distribution in a large network and routes some Layer (L) 3 traffic across the IST depending on which port the traffic was received and on which route the OSPF selects as the best one.

Only Ethernet Routing Switch 5600 units support this feature except units on hybrid stacks if SMLT is configured on the ERS 5600 units.

# SMLT consistency with the Ethernet Routing Switch 8800/8600

The SMLT consistency with the Ethernet Routing Switch 8800/8600 configuration feature reduces the confusion of the configuration of SMLT on the Ethernet Routing Switch Series 5000 with that of the Ethernet Routing Switch 8800/8600. In release 6.2 or later, when you enable SMLT, the following actions occur automatically:

1. The current Spanning Tree Protocol (STP) administrative state of Inter Switch Trunk (IST), SMLT, and Split Link Trunk (SLT) ports is saved on the NVRAM.
2. STP is disabled on IST, SMLT, and SLT ports.

# IEEE 802.3ad Link Aggregation

With IEEE 802.3ad-based link aggregation, you can aggregate one or more links together to form Link Aggregation Groups (LAG) so that a MAC client can treat the Link Aggregation Group as if it were a single link. Link aggregation increases the aggregate throughput of the interconnection between the devices while also providing link redundancy.

Although IEEE 802.3ad-based link aggregation and Multi-Link Trunking (MLT) features provide similar services, MLT is statically defined, whereas IEEE 802.3ad-based link aggregation is dynamic and provides more functionality.

Link Aggregation Control Protocol (LACP), defined by the IEEE 802.3ad standard, allows a switch to learn the presence and capabilities of a remote switch by exchanging information with the remote switch before a trunk group is formed. Either switch can accept or reject the aggregation request with the far end on a per-port basis. A link that cannot join a trunk group operates as an individual link.

The main purpose of LACP is to manage switch ports and their port memberships to link aggregation trunk groups (LAGs). LACP can dynamically add or remove LAG ports, depending on their availability and states. By default, Link Aggregation is set to disabled on all ports

Link aggregation employs the following principles and concepts:

- A MAC client communicates with a set of ports through an Aggregator, which presents a standard IEEE 802.3 service interface to the MAC client. The Aggregator binds to one or more ports within a system.

- The Aggregator is responsible for distributing frame transmissions from the MAC client to the various ports, and to collect received frames from the ports and pass them to the MAC client transparently.

- A system can contain multiple aggregators, serving multiple MAC clients. A given port will bind to (at most) a single Aggregator at any time. A MAC client is served by a single Aggregator at a time.

- The binding of ports to aggregators within a system is managed by the Link Aggregation Control function for that system, which is responsible for determining which links can be aggregated, aggregating them, binding the ports within the system to an appropriate Aggregator, and monitoring conditions to determine when a change in aggregation is needed.

  The network manager can control the determination and binding directly through the manipulation of the state variables of Link Aggregation (for example, Keys). In addition, automatic determination, configuration, binding, and monitoring can occur through the use of a Link Aggregation Control Protocol (LACP).

  The LACP uses peer exchanges across the links to determine, on an ongoing basis, the aggregation capability of the various links, and continuously provides the maximum level of aggregation capability achievable between a given pair of systems.

- Each port is assigned a unique, globally administered MAC address.

The MAC address is used as the source address for frame exchanges that are initiated by entities within the Link Aggregation sublayer itself (for example, LACP and Marker protocol exchanges).

- Each Aggregator is assigned a unique, globally administered MAC address, which is used as the MAC address of the aggregation from the perspective of the MAC Client, both as a source address for transmitted frames and as the destination address for received frames.

The MAC address of the Aggregator can be one of the MAC addresses of a port in the associated Link Aggregation Group.

# Link aggregation rules

The 5000 Series switch link aggregation groups operate under the following rules:

- Link aggregation groups are formed using LACP.
- All ports in a link aggregation group must be connected to the same far-end system.
- All ports in a link aggregation group must be operating in full-duplex mode.
- All ports in a link aggregation group must be configured to the same port speed.
- All ports in a link aggregation group must be in the same VLANs.
- In stack mode, ports in a link aggregation group can be on different units to form a distributed LAG (DLAG).
- LACPDUs are transmitted and received on all ports in the link aggregation group.
- Link aggregation is compatible with the Spanning Tree Protocol (STP).
- Link aggregation group(s) must be in the same STP groups.
- STP BPDUs are transmitted and received only on the first link in the group.
- A maximum of 32 link aggregation groups are supported.
- A maximum of 8 active links are supported per LAG.
- Unlimited standby links that are supported per LAG (for example, if a switch or stack is configured with one LAG, all nonactive LAG link ports can be configured as standby ports for that LAG).

The maximum number of LAGs is 32, and the maximum number of active links per group is eight. Link Aggregation allows more than eight links to be configured in one LAG. The first eight high-priority links are active links, and together, they form a trunk group. The ninth low-priority link remains in standby mode. When one of the active links goes down, the standby link becomes active and is added to the trunk group.

The failover process is as follows:

- The down link is removed from the trunk group.
- The highest priority standby link is added to the trunk group.

There can be a temporary delay in traffic flow due to the switching of links. If the active link goes down and no standby link exists, the traffic is rerouted to the remaining active links with a minimal delay in time.

# LACP port mode

The IEEE 802.3ad standard specifies that links that are not successful candidates for aggregation (for example, links to devices that cannot perform aggregation, or links that are manually set as non-aggregatable) can continue to operate as individual LACP links. However, LACP-enabled, STP-disabled ports that operate as individual links can potentially cause network loops.

You can specify the desired behavior of non-aggregatable LACP links on the switch:

- **Default mode:** In the default mode, if an LACP-enabled port is connected to a non-LACP partner port and the link fails to converge with the link partner, the port state moves to the forwarding state. This is the standard behavior from earlier software releases. The default mode is compatible with standard LACP.

- **Advance mode:** In the Advance mode, if an LACP-enabled port is connected to a non-LACP partner port and the link fails to converge with the link partner, the port state remains in the blocking state. This behavior is applied only to LACP-enabled ports that have STP disabled and prevents potential loops from forming in the network.

> **Note:**
> The Advance mode is not compatible with IEEE 802.3 ad standard LACP.

The Advance mode is also useful when a trunk port is removed from a trunk configuration. Currently, an active LACP trunk port can be removed from the trunk configuration if the link partner disables LACP or if PDU reception times out. Each LACP mode handles this scenario as follows:

- **Default mode:** The default mode implementation removes the active LACP trunk port from the active trunk configuration, and the port functions as a regular standalone active port. The port state is determined by STP when you enable STP, but is set to forwarding when you disable STP on the port.

- **Advance mode**: In the Advance mode, LACP-enabled ports that have STP disabled remain in the blocking state. This prevents potential loops from forming in the network.

# Chapter 6:  VLACP Fundamentals

## VLACP

Many enterprise networks require that trunk links provide subsecond failover to the redundant link when a failure occurs at the local or remote endpoint. This requirement can be met when both ends of the link are informed of any loss of communication.

Virtual Link Aggregation Control Protocol (VLACP), an LACP extension, is a Layer 2 handshaking protocol that provides end-to-end failure detection between two physical Ethernet interfaces. It allows the switch to detect unidirectional or bidirectional link failures.

## Virtual LACP (VLACP) overview

While Ethernet has been extended to detect remote link failures through functions such as Remote Fault Indication and Far End Fault Indication mechanisms, a limitation of these functions is that they terminate at the next Ethernet hop. Therefore, failures cannot be determined on an end-to-end basis.

Figure 32: Problem description (1 of 2) on page 120 provides an illustration of these limitations. While the Enterprise networks shown can connect their aggregated Ethernet trunk groups through a service provider network connection (for example, through a VPN), far-end failures cannot be signaled with Ethernet-based functions that operate end-to-end through the service provider cloud.

In Figure 32: Problem description (1 of 2) on page 120, the MLT (between Enterprise switches S1 and S2) extends through the service provider (SP) network.
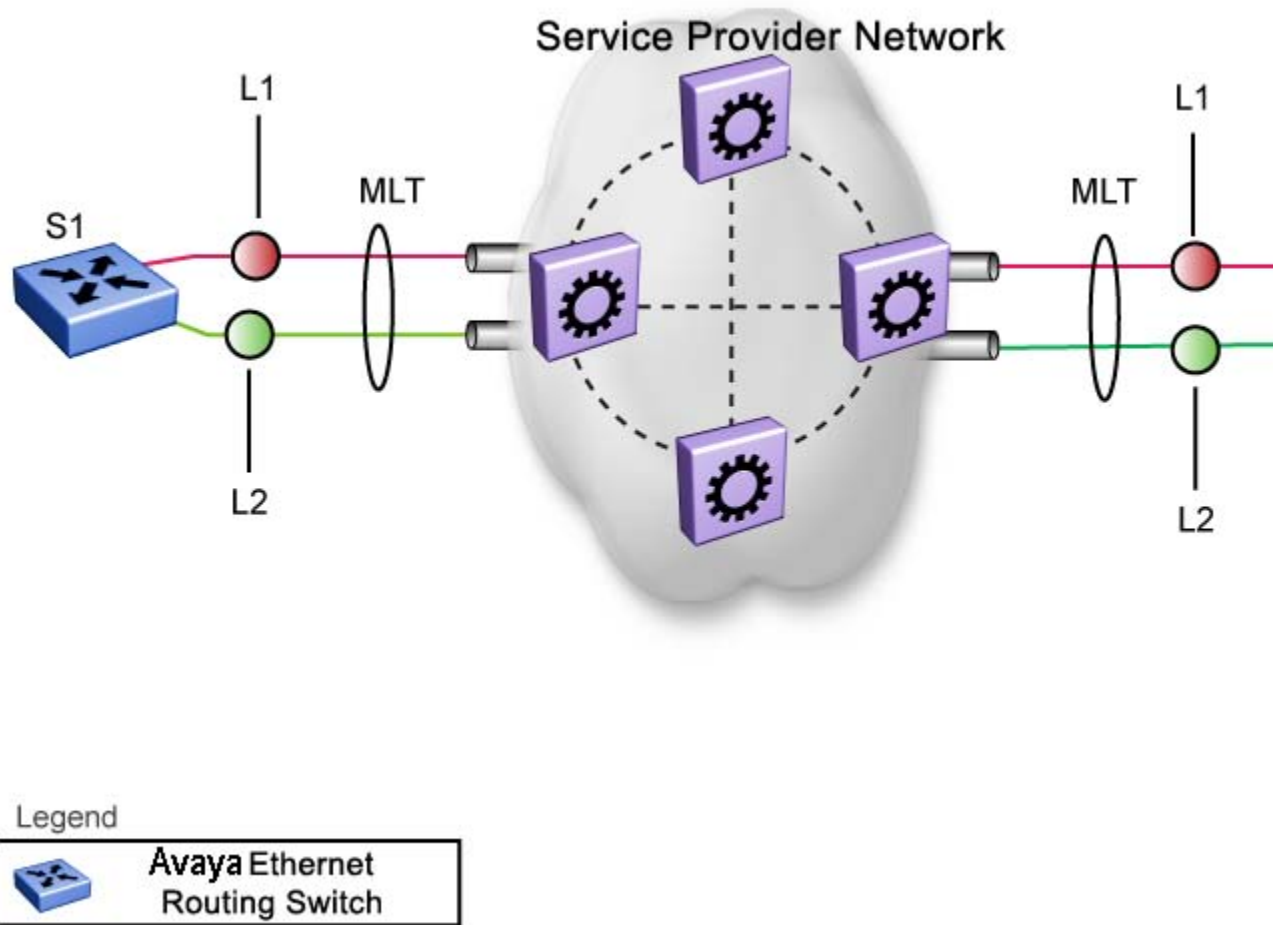
**Figure 32: Problem description (1 of 2)**

As shown in , if the L2 link on S1 (S1/L2) fails, the link-down failure is not propagated over the SP network to S2. Thus, S2 continues to send traffic over the S2/L2 link, which is black-holed because the S1/L2 link has failed.

Service Provider Network
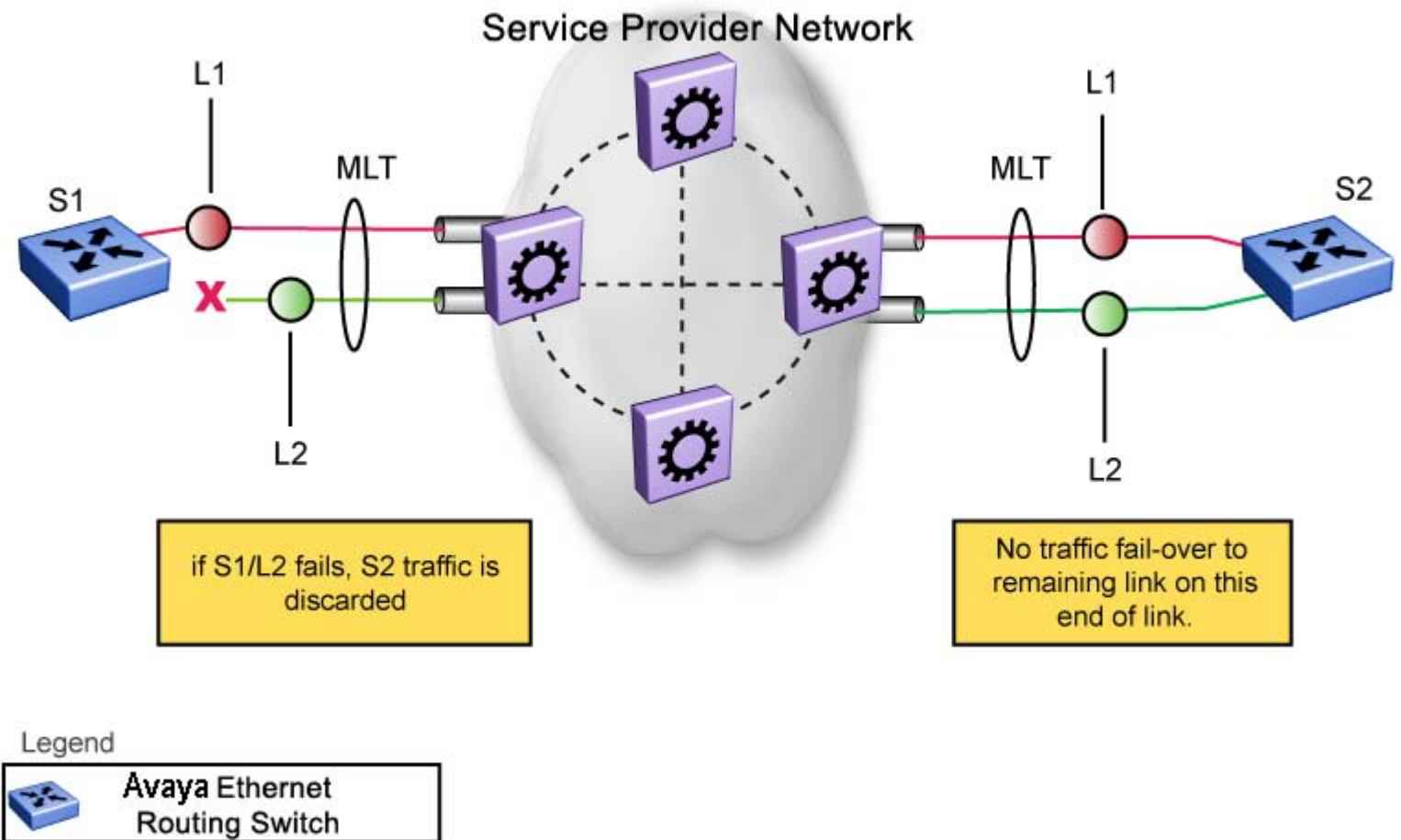
**Figure 33: Problem description (2 of 2)**

Note that LACP, as defined by IEEE, is a protocol that exists between two bridge endpoints; therefore, the LACPDUs are terminated at the next (SP) interface.

Avaya has developed an extension to LACP, which is called *Virtual LACP (VLACP)*. This extension can provide an end-to-end failure detection mechanism. With VLACP, far-end failures can be detected allowing an MLT to fail over properly when end-to-end connectivity is not guaranteed for certain links in an aggregation group. VLACP prevents the failure scenario shown in Figure 33: Problem description (2 of 2) on page 121.

# VLACP features

This section provides a summary of some of the key features of VLACP as implemented on the Ethernet Routing Switch 5000 Series:

- VLACP is configured per port. A port can be an individual port or a member of an MLT.

- When you set VLACP parameters for a trunk port, the settings are applied to all trunk members.

- For VLACP to operate properly, there must be a logical point-to-point connection (Layer 2 tunnel) between the two endpoints.

- VLACP does not work for point-to-multipoint connections.

- On each port that has VLACP enabled, VLACPDUs are sent periodically. If VLACPDUs are not received on a particular link, that link is taken down after a configurable timeout period.

- For the current software release, VLACP is supported on Ethernet interfaces only.

- VLACP can run independently as a port-to-port protocol or on top of MLT or LACP protocol.

- VLACP packets are untagged because they operate at the port level and not the VLAN level.

- The Destination Mac Address used in VLACPDUs is configurable. The MAC Address must be a multicast MAC Address so that it is always flooded. This allows the exchange of VLACPDUs from end to end.

- Both VLACP partners must have same multicast address, timers, and ethertype configured for VLACP to work properly.

- A unicast MAC address (destination MAC address) can be configured per port for end-to-end connectivity between units, when VLACP packets travel through an ISP network.

- The VLACP PDU transmission interval changes when an LACP partner is lost. This aids detection in certain failure scenarios.

- VLACP PDU messages are processed so as to prevent false VLACP state recovery.

- VLACP defaults to an IEEE reserved multicast MAC address for sourcing LACP PDU packets.

Troubleshooting

Error logs are created for the following failures and errors:

- An incorrect PDU, such as wrong destination MAC addresses received

- An inability to enable VLACP on a port due to unallowable Destination MAC addresses

- A port index that is out of range
- A port was blocked by VLACP (a log message is also generated when the port is unblocked)

# Chapter 7: ADAC Fundamentals

The 5000 Series switch supports the Auto-Detection and Auto-Configuration (ADAC) of Avaya IP Phones. With ADAC, you can automatically configure the switch to support and prioritize IP Phone traffic.

When ADAC is enabled and an Avaya IP Phone is connected to the switch, the switch automatically configures the VLAN, port, and Quality of Service (QoS) settings necessary for the transmission of signal and voice between the Avaya IP Phone and the switch.

ADAC can configure the switch whether the switch is directly connected to the Call Server (through the Call Server port) or is indirectly connected to the Call Server using a network uplink (through the Uplink port).

ADAC has three separate operating modes to meet the requirements of different networks:

- **Untagged-Frames-Basic**:

  Use this mode when you want a basic configuration only and the IP Phones are sending untagged traffic.

- **Untagged-Frames-Advanced**:

  Use this mode when you want an advanced configuration and the IP Phones are sending untagged traffic. In this mode, ADAC creates a Voice VLAN that includes the Call Server or Uplink port, as applicable, and all telephony ports. All tagging, PVID settings, and traffic prioritization are configured automatically.

- **Tagged Frames:**

  Use this mode when you want an advanced configuration and the IP Phones are sending tagged traffic. You can also use tagged frames to support devices other than IP Phones. This mode provides the same configuration as the Untagged-Frames-Advanced mode, but with tagged frames. As with the Untagged-Frames-Advanced mode, ADAC creates a Voice VLAN that includes the Call Server or Uplink port, as applicable, and all telephony ports. All tagging, PVID settings, and traffic prioritization are configured automatically.

## ADAC operation

The following sections provide detailed explanations of ADAC operation.

# Auto-Detection of Avaya IP Phones

When a Avaya IP Phone is connected to a switch and is powered on, the switch automatically detects the IP Phone, and then begins the auto-configuration of the IP Phone. An ADAC lookup is also performed each time a MAC address is learned, migrated, or aged-out and removed.

When you enable auto-detection on a port, the port also becomes operationally enabled. Similarly, when you disable auto-detection on a port, the port is operationally disabled. A port can also be operationally disabled if the port maximum of 32 devices is reached. If the port limit is reached, a trap will be sent (if ADAC traps are enabled) and autoconfiguration will also be removed. To put the port back into the operational state, disable and then reenable auto-detection on the affected port. ADAC supports a maximum of 32 devices (both IP phones and non-phones) per port.

There are two ways to use ADAC to automatically detect IP Phones. You can enable one or the other or both of these methods on a port-by-port basis, as long as at least one detection mechanism remains enabled.

The detection mechanism can be selected

- before enabling auto-detection on the port, or
- if ADAC is globally disabled.

The two methods of auto-detection are by MAC address or using LLDP (IEEE 802.1ab). Auto-detection by MAC address is based on using predefined MAC addresses to determine that the specified port is connected to a Avaya IP phone. For more information and the list of defined MAC address ranges, see Auto-Detection by MAC address on page 126.

Auto-detection by LLDP allows the system to detect IP phones with MAC addresses outside the list of default MAC address ranges as long as they can be identified as an IP phone by LLDP, regardless of their MAC addresses. For more information about auto-detection by LLDP, see Auto-Detection by LLDP (IEEE 802.1ab) on page 128.

You can enable either of these detection mechanisms or both on each individual port. At least one of these detection methods must be enabled on each port.

# Auto-Detection by MAC address

When this feature is enabled on a port, the switch checks all MAC addresses of packets received on the port. If a received MAC address falls within the range of known Avaya IP Phone MAC addresses, ADAC determines that the specified port is connected to a Avaya IP Phone and initiates the required configuration. ADAC is supported for a maximum of 32 devices per port, but in most cases, there will be only one IP phone and one PC on each port.

The 5000 Series switch has a default range of MAC addresses configured to be recognized as Avaya IP Phones by ADAC.

shows a list of the default MAC address ranges.

**Table 18: Default ADAC MAC address ranges**

| Lower End | Higher End |
|---|---|
| 00-0A-E4-01-10-20 | 00-0A-E4-01-23-A7 |
| 00-0A-E4-01-70-EC | 00-0A-E4-01-84-73 |
| 00-0A-E4-01-A1-C8 | 00-0A-E4-01-AD-7F |
| 00-0A-E4-01-DA-4E | 00-0A-E4-01-ED-D5 |
| 00-0A-E4-02-1E-D4 | 00-0A-E4-02-32-5B |
| 00-0A-E4-02-5D-22 | 00-0A-E4-02-70-A9 |
| 00-0A-E4-02-D8-AE | 00-0A-E4-02-FF-BD |
| 00-0A-E4-03-87-E4 | 00-0A-E4-03-89-0F |
| 00-0A-E4-03-90-E0 | 00-0A-E4-03-B7-EF |
| 00-0A-E4-04-1A-56 | 00-0A-E4-04-41-65 |
| 00-0A-E4-04-80-E8 | 00-0A-E4-04-A7-F7 |
| 00-0A-E4-04-D2-FC | 00-0A-E4-05-48-2B |
| 00-0A-E4-05-B7-DF | 00-0A-E4-06-05-FE |
| 00-0A-E4-06-55-EC | 00-0A-E4-07-19-3B |
| 00-0A-E4-08-0A-02 | 00-0A-E4-08-7F-31 |
| 00-0A-E4-08-B2-89 | 00-0A-E4-09-75-D8 |
| 00-0A-E4-09-BB-9D | 00-0A-E4-09-CF-24 |
| 00-0A-E4-09-FC-2B | 00-0A-E4-0A-71-5A |
| 00-0A-E4-0A-9D-DA | 00-0A-E4-0B-61-29 |
| 00-0A-E4-0B-BB-FC | 00-0A-E4-0B-BC-0F |
| 00-0A-E4-0B-D9-BE | 00-0A-E4-0C-9D-0D |
| 00-13-65-FE-F3-2C | 00-13-65-FF-ED-2B |
| 00-15-9B-FE-A4-66 | 00-15-9B-FF-24-B5 |
| 00-16-CA-00-00-00 | 00-16-CA-01-FF-FF |
| 00-16-CA-F2-74-20 | 00-16-CA-F4-BE-0F |
| 00-17-65-F6-94-C0 | 00-17-65-F7-38-CF |
| 00-17-65-FD-00-00 | 00-17-65-FF-FF-FF |
| 00-18-B0-33-90-00 | 00-18-B0-35-DF-FF |

| Lower End | Higher End |
|-----------|------------|
| 00-19-69-83-25-40 | 00-19-69-85-5F-FF |

You can change these default MAC address ranges using ACLI or EDM.

ADAC checks a MAC address against the supported ranges only when the MAC address is learned on the port. If you change the supported MAC address ranges, this has no effect on the previously learned MAC addresses. For example, if the address of a configured device is no longer in an ADAC range, the IP phone remains configured until its MAC address is aged out (by disconnecting the cable, for example) or until ADAC is disabled, either globally or on the port.

In a similar fashion, if the MAC address of an IP Phone—a MAC address that's not recognized by ADAC—is learned on a port and then is later added to the supported ranges, the IP Phone won't be detected and configured until the address is aged out or ADAC is disabled. The maximum number of ranges that ADAC supports is 128.

The maximum number of ranges that ADAC supports is 128.

# Auto-Detection by LLDP (IEEE 802.1ab)

Auto-detection by LLDP extends the auto-detection that relies on MAC addresses. This feature allows devices identified as IP phones through LLDP to be detected by ADAC even if their MAC addresses are outside the list of ADAC MAC address ranges.

LLDP-based auto-detection supports a maximum of 16 devices per port.

## Detailed configuration example

The following commands provide a detailed configuration example.

- Default a DUT.

- Disable on port 5 MAC detection.

```
5530-24TFD(config-if)#in fa 5
5530-24TFD(config-if)#no adac detection mac
5530-24TFD(config-if)#sho adac detection interface 5
Unit/   MAC       LLDP
Port    Detection Detection
-----   --------- ---------
5       Disabled  Enabled
```

- Enable ADAC on port 5 and globally.

```
5520-48T-PWR(config)#adac enable
5520-48T-PWR(config)#in fa 5
5520-48T-PWR(config-if)#adac enable
```

- Define the uplink port, and voice VLAN port, then change operating mode to Untagged Frames Advanced.

```
5520-48T-PWR(config)#adac voice-vlan 200
5520-48T-PWR(config)#adac uplink-port 10
5520-48T-PWR(config)#adac op-mode untagged-frames-advanced
```

- Verify that above settings were applied.

```
5520-48T-PWR(config)#sho adac
ADAC Global Configuration
-------------------------------------
ADAC Admin State:  Enabled
ADAC Oper State:  Enabled
Operating Mode:  Untagged Frames Advanced
Traps Control Status:  Enabled
Voice-VLAN ID:  200
Call Server Port:  None
Uplink Port: 10
```

- Connect your phone on port 5 and verify that it was detected and configuration applied.

```
5520-48T-PWR(config-if)#sho adac in 5
               Auto        Oper      Auto
Port  Type  Detection  State     Configuration  T-F PVID   T-F Tagging
----  ----  ---------  --------  -------------  ---------  --------------
5     T     Enabled    Enabled   Applied        No Change  Untag PVID Only
```

# Auto-Configuration of Avaya IP Phones

The ADAC port participation can be set independently by enabling or disabling ADAC for particular ports.

When a new MAC address of an IP phone is learned on a port with ADAC enabled, ADAC immediately performs the auto-Configuration for that port (this operation is dependent on the configured ADAC operating mode and on whether other MAC addresses are learned on that port). This includes the required configuration of ports, VLANs, and QoS settings and involves minimal intervention by the user.

Auto-configuration is automatically removed or applied based on the port state, the state of the MAC addresses and the phones detected on the port.

The ports are polled every two seconds for their auto-configuration state and to see whether or not auto-configuration should be applied based on the current ADAC settings, both the global setting and the port setting. Auto-configuration will be applied on the port when the port is operational (operational state is enabled) and if one of these conditions is true:

- Op-mode = Untagged-Frames-Basic or Untagged-Frames-Advanced, at least one IP phone is detected on the port, and no non-IP phones are detected on the port

- Op-mode = Tagged-Frames and at least one IP phone is detected on the port

Auto-configuration is removed if any of these conditions becomes true:

- auto-detect becomes disabled on the port

- the ports operational state becomes disabled

- Op-mode = Untagged-Frames-Basic or -Advanced, and at least one non-IP device is detected on the port

- there are no IP phones detected on the port and the link is down.

If the link is still up but there are no IP phones on the port, auto-configuration is disabled after an aging period of about 90 seconds.

If all MAC addresses belonging to Avaya IP Phones on a port age out, the Auto-Configuration settings are removed from the port.

# Initial user settings

Before enabling the ADAC feature, you must set the operating mode according to how the IP Phones are configured to send frames: tagged or untagged.

When running ADAC in Untagged-Frames-Advanced or Tagged-Frames operating modes, you must also specify:

- the ID of the VLAN to be used for voice packets

- at least one of the following:

    - Call Server port, if connected directly to the switch

    - Uplink port, if used

**Note:**

To properly enable the ADAC feature, the VLAN ID for the Voice-VLAN must not be a preexisting VLAN.

Tag voice traffic entering the Uplink port with the Voice VLAN ID. This configuration must be made on all switches on the path to the Call Server.

## Port Restrictions

The following restrictions apply to the Call Server, Uplink, and Telephony ports.

The **Call Server port** must not be:

- part of a trunk (MLT, LAG)

- a Monitor Port in port mirroring

- a NSNA port

- a Telephony port

- the Uplink port
- an EAP port

The **Uplink port** must not be:

- a Monitor Port in port mirroring
- an NSNA port
- a Telephony port
- an EAP port
- the Call Server port

The **Telephony port** must not be:

- part of a trunk (MLT, LAG)
- a Monitor Port in port mirroring
- an IGMP static router port
- an NSNA port
- the Call Server port
- the Uplink port

# Operating modes

ADAC can be configured to apply settings depending on how the Avaya IP Phones are configured to send traffic (tagged or untagged) and depending on the desired complexity level of the Auto-Configuration. The following sections provide detailed descriptions of the configurations that are applied in each ADAC operating mode.

- QoS settings used by ADAC on page 131
- Untagged-Frames-Basic operating mode on page 132
- Untagged-Frames-Advanced operating mode on page 132
- Tagged-Frames operating mode on page 134

## QoS settings used by ADAC

ADAC QoS configuration is applied to:

- traffic coming from the IP Phones
- traffic coming from the Call Server port
- traffic coming from the Uplink port

To configure the switch appropriately for IP Phones, the ADAC operating modes use two QoS policies, each associated with one of the following classifiers:

- **all-IP-traffic**

  The all-IP-traffic classifier filters all IPv4 traffic and remarks it with DSCP 0x2E and 802.1p priority 0x06.

- **tagged-with-VoiceVLAN-traffic**

  The tagged-with-VoiceVLAN-traffic classifier filters only the traffic tagged with the Voice VLAN ID and remarks it with DSCP 0x2E and 802.1p priority 0x06.

## Untagged-Frames-Basic operating mode

In the Untagged-Frames-Basic operating mode, the Call Server and Uplink ports are not used, so QoS settings are applied only for traffic coming from the IP Phones. The VLAN configuration is minimal.

To properly configure the Untagged-Frames-Basic mode, you must perform the following:

- Configure the IP Phones to send untagged frames.
- Connect only IP Phones to a port. (You cannot connect a device that is not an Avaya IP Phone to the same port.)

### QoS configuration

In the Untagged-Frames-Basic mode, Auto-Configuration performs the following QoS configuration:

- Adds the telephony ports to the all-IP-traffic classifier (because only IP Phones are connected to the telephony ports).

### VLAN configuration

In the Untagged-Frames-Basic mode, Auto-Configuration also performs the following VLAN configuration:

- Tagging of Telephony ports is set to Untagged.

## Untagged-Frames-Advanced operating mode

To properly configure the Untagged-Frames-Advanced operating mode, you must perform the following:

- Configure the IP Phones to send untagged frames.
- Connect only IP Phones to a port. (You cannot connect a device that is not an Avaya IP Phone to the same port.)

- Specify the Voice-VLAN ID and either the Call Server port or the Uplink port, as applicable.
- If the switch is not directly connected to the Call Server, ensure that the telephony packets coming from the Call Server through the Uplink port are tagged with the Voice-VLAN ID.

### QoS configuration

In the Untagged-Frames-Advanced mode, Auto-Configuration performs the following QoS configuration:

- For traffic coming from the Telephony ports:
  - Adds the telephony ports to the all-IP-traffic classifier (because only IP Phones are connected to the telephony ports).
- For traffic coming from the Call Server port (if any):
  - Adds the Call Server port to the all-IP-traffic classifier (because only Call Server traffic enters that port).
- For traffic coming from the Uplink port (if any):
  - Adds the Uplink port to the tagged-with-VoiceVLAN-traffic classifier. (As the Uplink port connects to the network, packets with different tagging can enter this port; this ensures that only voice traffic is remarked.)

### VLAN configuration

In the Untagged-Frames-Advanced mode, Auto-Configuration also performs the following VLAN configurations:

- Telephony port:
  - Membership = adds to Voice-VLAN; removes from other VLANs (The port does not need to be a member of other VLANs.)
  - Tagging = Untagged
  - PVID = Voice-VLAN
- Call Server port (if any):
  - Membership = adds to Voice-VLAN; not removed from other VLANs
  - Tagging = Untagged
  - PVID = Voice-VLAN
- Uplink port (if any):
  - Membership = adds to Voice-VLAN; not removed from other VLANs
  - Tagging = Tagged
  - PVID = no change (All VLAN changes made by ADAC are as if VCC=flexible, so the Auto-PVID setting is ignored.)

# Tagged-Frames operating mode

To properly configure the Tagged-Frames operating mode, you must perform the following:

- Configure the IP Phones to send tagged frames with the ID of the Voice-VLAN.

- Connect at least one Avaya IP Phone to a telephony port. (In this mode, other devices can be connected to the same port; for example, when a PC is connected directly to the IP phone.)

- Ensure that the Filter Unregistered Frames option is set to disabled on the ADAC-enabled ports. (Otherwise, no source MAC address can be learned for incoming packets tagged with the Voice VLAN ID, meaning that no phone can be detected.)

- Specify the Voice-VLAN ID and either the Call Server port or the Uplink port, as applicable.

- If the switch is not directly connected to the Call Server, ensure that the telephony packets coming from the Call Server through the Uplink port are tagged with the Voice-VLAN ID.

## QoS configuration

In the Tagged-Frames mode, Auto-Configuration performs the following QoS configuration:

- For traffic coming from the telephony ports:

  - Adds the telephony ports to the tagged-with-VoiceVLAN-traffic classifier. (In this way, only the voice traffic is remarked.)

- For traffic coming from the Call Server port (if any):

  - Adds the Call Server port to the all-IP-traffic classifier (because only Call Server traffic enters that port).

- For traffic coming from the Uplink port (if any):

  - Adds the Uplink port to the tagged-with-VoiceVLAN-traffic classifier. (As the Uplink port connects to the network, packets with different tagging can enter this port; applying this classifier ensures that only voice traffic is remarked.)

In this way, all traffic tagged with the Voice-VLAN ID is prioritized.

## VLAN configuration

In the Tagged-Frames mode, Auto-Configuration also performs the following VLAN configurations:

- Telephony port:

  - Membership = adds to Voice-VLAN; not removed from other VLANs

  - Tagging = UntagPVIDOnly

- PVID = no change or changed to Default-VLAN(1) if the current value equals the Voice-VLAN (must be different from the Voice-VLAN ID)

- Call Server port (if any):

    - Membership = adds to Voice-VLAN; not removed from other VLANs

    - Tagging = Untagged

    - PVID = Voice-VLAN

- Uplink port (if any):

    - Membership = adds to Voice-VLAN; not removed from other VLANs

    - Tagging = Tagged

    - PVID = no change (All VLAN changes made by ADAC are as if VCC =flexible, so the Auto-PVID setting is ignored.)

## Dynamic VLAN auto-configuration

The following describes the details of the ADAC VLAN configuration:

- The ADAC Voice VLAN is created and removed automatically.

- All membership to the ADAC Voice VLAN is dynamic, meaning that the settings are not saved to NVRAM. The dynamic settings will be lost on reboot or when ADAC is disabled.

- From the moment ADAC is enabled on a port set as a telephony port or a call server port, (but not an uplink port), all VLAN configuration is dynamic (including user configuration). When removing the configuration for a port (for example, when changing a port so that it is no longer a call server port or a telephony port), the configuration from NVRAM is restored. After that, the user configuration will be permanent again. For an uplink port, any user configuration made while ADAC was enabled on the port is saved.

- For telephony ports, the NVRAM VLAN configuration is restored in two cases: when the ADAC configuration is removed due to the removal of the IP Phone, or when ADAC is disabled for that port.

- The VLAN Configuration Control (VCC) rules, other than those for the Flexible mode, are skipped internally by ADAC configuring VLANs. Any VLAN settings made automatically by ADAC follow the rules of the Flexible mode, regardless of the current value of VCC. Any settings that you make manually on ADAC ports follow the current VCC mode, as for a non-ADAC port.

- If you change the preset values of Tagging and PVID when ADAC is running in Tagged-Frames mode, future auto-configurations will apply the new values. Changing the preset has no effect on current configured Tagging and PVID values.

- With Release 6.2, you can change the nonADAC VLANs on a port without disabling ADAC.

# ADAC and stacking

In a stack, global ADAC settings of the base unit are applied across the stack, except for port settings (for Call Server port, Uplink port and Telephony ports).

The ADAC port states are taken from each unit. Therefore, unit ports have the same ADAC status in a stack as they do in standalone mode.

If two or more units each have a configured Call Server port in standalone mode and are then joined together in a stack, the Call Server port with the lowest interface number in the stack is elected as the stack Call Server port.

This same scenario also occurs for the Uplink port.

The Ethernet Routing Switch 5000 Series supports up to 8 ADAC uplinks and 8 call-server links — individual ports or any combination of MLT, DMLT or LAG — for each switch or stack.

## Lost Call Server Port or Uplink Port

If ADAC is operating in either the Untagged-Frames-Advanced or Tagged-Frames operating mode and you reset the unit on which the Call Server or Uplink port is located, the feature loses the valid Call Server or Uplink port. In this case, the feature is temporarily disabled until the unit with the Call Server or Uplink port rejoins the stack and the configuration becomes valid again. While the unit is in a temporarily disabled state, the Voice-VLAN is not deleted if it was created first.

If the ADAC global configuration is changed on the base unit while the feature is temporarily disabled, the feature stays disabled regardless of where the Call Server or Uplink port are located when their unit rejoins the stack. Changing Auto-Detection on Telephony ports has no effect on the global settings.

## Uplink port as part of MLT in a stack

To set the Uplink port to be part of a distributed MLT in a stack, you must first configure and enable the MLT, and then you can set one of the MLT members as the Uplink port.

If the unit containing the Uplink port in a stack is removed from the stack, the lowest port from the same MLT becomes the new Uplink port.

After rebooting a stack, each unit that has a port member belonging to the Uplink MLT is configured as an Uplink port on the unit. After joining the stack, the lowest Uplink port is elected as the stack Uplink port.

When you disable the MLT, the Uplink configuration is removed for all trunk members except for the original Uplink port.

# ADAC and LACP enabled on an Uplink port

To set the Uplink port as LACP-enabled, you must first configure and enable LACP on the port, and then you can set the port as the Uplink port.

Due to the dynamic configuration of VLANs, you are not allowed to:

- enable LACP on a preconfigured Uplink port
- enable LACP on a port with the same admin key as the ADAC Uplink ports
- change the admin key of any member of the ADAC Uplink ports
- set the admin key for a LACP-enabled port to the same value as the Uplink port

When ADAC sets the configuration for the Uplink port, the VLAN and QoS configuration is applied for all LACP-enabled (active or passive) ports belonging to the same LAG as the Uplink port.

Any changes to the LAG mode, from Active to Passive or from Passive to Active, have no effect on ADAC.

# Uplink port as part of LACP in a stack

In a stack, LAGs containing the Uplink port operate similarly to MLTs containing the Uplink port.

If the unit containing the Uplink port in a stack is removed from the stack, the lowest port from the same LAG becomes the new Uplink port.

After rebooting a stack, each unit that has a port member belonging to the Uplink LAG is configured as an Uplink port on the unit. After joining the stack, the lowest Uplink port is elected as the stack Uplink port.

When you disable the LAG, the Uplink configuration is removed for all trunk members except for the original Uplink port.

After you remove the LAG, you cannot reenable the configuration for the Uplink port. You must remove the Uplink, reconfigure the LAG, and then set the Uplink port again.

# ADAC and EAP configuration

ADAC and EAP are mutually exclusive on the Call Server port and the Uplink port.

However, on telephony ports, you can enable both ADAC and EAP, provided the following conditions are met:

- The ports must be configured to allow non-EAP MAC addresses.
- Guest VLAN must not be allowed on the ports.

To enable ADAC on an EAP port, follow these steps.

1. On the switch, globally enable support for non-EAP MAC addresses. (In ACLI, use the `eap multihost allow-non-eap-mac` command.)

2. On each telephony port, enable support for non-EAP MAC addresses. (In ACLI, use the `eap multihost port <port> allow-non-eap-mac` command.)

3. On each telephony port, enable EAP Multihost. (In ACLI, use the `eap multihost port <port> enable` command.)

4. On the telephony ports, ensure that Guest VLAN is disabled. (In ACLI, use the `show eap guest-vlan` command.)

5. On the switch, enable EAP globally. (In ACLI, use the `eap enable` command.)

6. Configure and enable ADAC on the ports.

When you configure ADAC and EAP, the following restrictions apply:

• When ADAC is enabled, you cannot enable or disable EAP or EAP Multihost on the port.

• You can enable ADAC on the port only if:

  - EAP is disabled per port

    OR

  - EAP and Multihost are enabled per port

EAP does not change the VLAN configuration for ADAC-enabled ports. ADAC changes to the VLAN configuration take priority.

## ADAC user Restrictions

After ADAC is enabled, you cannot:

• Delete the Voice-VLAN.

• Remove auto-configured ports from Voice-VLAN.

• View or remove any QoS setting made by ADAC (auto-configured settings).

• Set the Voice-VLAN as Management VLAN.

You can:

• Add ports to and remove ports from the Voice-VLAN. (Configuration is dynamic.)

• Change the tagging and PVID of all ports in the Voice-VLAN. (Configuration is dynamic.)

# Disabling ADAC

Disabling the ADAC feature deletes all configurations, including the Voice-VLAN, and restores the pre-ADAC port configurations saved in NVRAM for all ADAC-enabled ports (Telephony, Call Server, and Uplink).

# Chapter 8: Configuring VLANs using the ACLI

## Creating and Managing VLANs using the ACLI

The Command Line Interface commands detailed in this section allow for the creation and management of VLANs. Depending on the type of VLAN being created or managed, the command mode needed to execute these commands can differ.

This section contains information about the following topics:

## Displaying VLAN information

Use the following procedure to display the number, name, type, protocol, user PID, state of a VLAN and whether it is a management VLAN.

## Procedure steps

To display VLAN information, use the following command from Privileged EXEC mode.

```
show vlan [configcontrol] [dhcp-relay <1-4094>] [igmp
{ <1-4094> | unknown-mcast-allow-flood | unknown-mcast-no-
flood}] [interface { info | vids}] [ip <vid>] [mgmt] [multicast
< membership>] [type {port | protocol-ipEther2| protocol-
ipx802.3 | protocol-ipx802.2 | protocol-ipxSnap | protocol-
ipxEther2 | protocol-decEther2 | protocol-snaEther2 | protocol-
Netbios | protocol-xnsEther2 | protocol-vinesEther2 | protocol-
ipv6Ether2 | protocol-Userdef |protocol-RarpEther2] [vid
<1-4094>]
```

## Variable definitions

| Variable | Value |
| --- | --- |
| vid <1-4094> | Enter the number of the VLAN to display. |
| type | Enter the type of VLAN to display:<br><br>• port - port-based<br><br>• protocol - protocol-based (see following list) |
| protocol-ipEther2 | Specifies an ipEther2 protocol-based VLAN. |
| protocol-ipx802.3 | Specifies an ipx802.3 protocol-based VLAN. |
| protocol-ipx802.2 | Specifies an ipx802.2 protocol-based VLAN. |
| protocol-ipxSnap | Specifies an ipxSnap protocol-based VLAN. |
| protocol-ipxEther2 | Specifies an ipxEther2 protocol-based VLAN. |
| protocol-decEther2 | Specifies a decEther2 protocol-based VLAN. |
| protocol-snaEther2 | Specifies an snaEther2 protocol-based VLAN. |
| protocol-Netbios | Specifies a NetBIOS protocol-based VLAN. |
| protocol-xnsEther2 | Specifies an xnsEther2 protocol-based VLAN. |
| protocol-vinesEther2 | Specifies a vinesEther2 protocol-based VLAN. |
| protocol-ipv6Ether2 | Specifies an ipv6Ether2 protocol-based VLAN. |
| protocol-Userdef | Specifies a user-defined protocol-based VLAN. |
| protocol-RarpEther2 | Specifies a RarpEther2 protocol-based VLAN. |

# Displaying VLAN interface information

Use the following procedure to display VLAN settings associated with a port, including tagging information, PVID number, priority, and filtering information for tagged, untagged, and unregistered frames.

## Procedure steps

To display VLAN interface information, use the following command from Privileged EXEC mode.

```
show vlan interface info [<portlist>]
```

# Displaying VLAN port membership

Use the following procedure to display port memberships in VLANs.

## Procedure steps

To display VLAN port memberships, use the following command from Privileged EXEC mode.

```
show vlan interface vids [<portlist>]
```

# Setting the management VLAN

Use the following procedure to set a VLAN as the management VLAN.

## Procedure steps

To set the management VLAN, use the following command from Global Configuration mode.

```
vlan mgmt <1-4094>
```

# Resetting the management VLAN to default

Use the following procedure to reset the management VLAN to VLAN1.

## Procedure steps

To reset the management VLAN to default, use the following command from Global Configuration mode.

```
default vlan mgmt
```

# Creating a VLAN

Use the following procedure to create a VLAN. A VLAN is created by setting the state of a previously nonexistent VLAN.

## Procedure steps

To create a VLAN, use the following command from Global Configuration mode.

```
vlan create <1-4094> [name <line>] type {port | protocol-
ipEther2 | protocol-ipx802.3 | protocol-ipx802.2 | protocol-
ipxSnap | protocol-ipxEther2 | protocol-decEther2 | protocol-
snaEther2 | protocol-Netbios | protocol-xnsEther2 | protocol-
vinesEther2 | protocol-ipv6Ether2 | protocol-Userdef
<4096-65534> | protocol-RarpEther2}
```

## Variable definitions

| Variable | Value |
|---|---|
| <1-4094> | Enter the number of the VLAN to create. |
| name <line> | Enter the name of the VLAN to create. |
| type | Enter the type of VLAN to create: |

| Variable | Value |
|---|---|
| | • port - port-based |
| | • protocol - protocol-based (see following list) |
| protocol-ipEther2 | Specifies an ipEther2 protocol-based VLAN. |
| protocol-ipx802.3 | Specifies an ipx802.3 protocol-based VLAN. |
| protocol-ipx802.2 | Specifies an ipx802.2 protocol-based VLAN. |
| protocol-ipxSnap | Specifies an ipxSnap protocol-based VLAN. |
| protocol-ipxEther2 | Specifies an ipxEther2 protocol-based VLAN. |
| protocol-decEther2 | Specifies a decEther2 protocol-based VLAN. |
| protocol-snaEther2 | Specifies an snaEther2 protocol-based VLAN. |
| protocol-Netbios | Specifies a NetBIOS protocol-based VLAN. |
| protocol-xnsEther2 | Specifies an xnsEther2 protocol-based VLAN. |
| protocol-vinesEther2 | Specifies a vinesEther2 protocol-based VLAN. |
| protocol-Userdef <4096-65534> | Specifies a user-defined protocol-based VLAN. |
| protocol-ipv6Ether2 | Specifies an ipv6Ether2 protocol-based VLAN. |

# Deleting a VLAN

Use the following procedure to delete a VLAN.

## Procedure steps

To delete a VLAN, use the following command from Global Configuration mode.

```
vlan delete <2-4094>
```

# Modifying VLAN MAC address flooding

Use the following procedure to remove MAC addresses from the list of addresses for which flooding is allowed. This procedure can also be used as an alternate method of deleting a VLAN.

## Procedure steps

To modify VLAN MAC address flooding, or to delete a VLAN, use the following command from Global Configuration mode.

```
no vlan [<2-4094>][igmp unknown-mcast-allow-flood <H.H.H>]
```

# Configuring VLAN name

Use the following procedure to configure or modify the name of an existing VLAN.

## Procedure steps

To configure the VLAN name, use the following command from Global Configuration mode.

```
vlan name <1-4094> <line>
```

# Enabling automatic PVID

Use the following procedure to enable the automatic PVID feature.

## Procedure steps

To enable automatic PVID, use the following command from Global Configuration mode.

```
[no] auto-pvid
```

Use the **no** form of this command to disable

# Configuring VLAN port settings

Use the following procedure to configure VLAN-related settings for a port.

# Procedure steps

To configure VLAN port settings, use the following command from Global Configuration mode.

```
vlan ports [<portlist>] [tagging {enable | disable | tagAll |
untagAll | tagPvidOnly | untagPvidOnly}] [pvid <1-4094>]
[filter-untagged-frame {enable | disable}] [filter-
unregistered-frames {enable | disable}] [priority <0-7>] [name
<line>]
```

# Variable definitions

| Variable | Value |
|---|---|
| <portlist> | Enter the port numbers to be configured for a VLAN. |
| tagging {enable\|disable\|tagAll\| untagAll\| tagPvidOnly\| untagPvidOnly} | Enables or disables the port as a tagged VLAN member for egressing packet. |
| pvid <1-4094> | Sets the PVID of the port to the specified VLAN. |
| filter-untagged-frame {enable\| disable} | Enables or disables the port to filter received untagged packets.<br><br>**Note:**<br>If you are using Ethernet Routing Switch 5510, Avaya recommends that you disable the filter-untagged-frame variable to ensure that topology (SONMP) packets, STP, LACP, and VLACP function correctly. |
| filter-unregistered-frames {enable \| disable} | Enables or disables the port to filter received unregistered packets. Enabling this feature on a port means that any frames with a VID to which the port does not belong to are discarded. |
| priority <0-7> | Sets the port as a priority for the switch to consider as it forwards received packets. |
| name <line> | Enter the name you want for this port.<br><br>**Note:**<br>This option can only be used if a single port is specified in the <portlist>. |

# Configuring VLAN members

Use the following procedure to add or delete a port from a VLAN.

## Procedure steps

To configure VLAN members, use the following command from Global Configuration mode.

```
vlan members [add | remove] <1-4094> <portlist>
```

## Variable definitions

| Variable | Value |
|---|---|
| add \| remove | Adds a port to or removes a port from a VLAN. <br><br> **Note:** <br> If this parameter is omitted, set the exact port membership for the VLAN; the prior port membership of the VLAN is discarded and replaced by the new list of ports. |
| <1-4094> | Specifies the target VLAN. |
| portlist | Enter the list of ports to be added, removed, or assigned to the VLAN. |

# Configuring VLAN Configuration Control

VLAN Configuration Control (VCC) allows a switch administrator to control how VLANs are modified. VLAN Configuration Control is a superset of the existing AutoPVID functionality and incorporates this functionality for backwards compatibility. VLAN Configuration Control is globally applied to all VLANs on the switch.

VLAN Configuration Control offers four options for controlling VLAN modification:

- Strict
- Automatic

- AutoPVID
- Flexible

**Note:**

The factory default setting is Strict.

VLAN Configuration Control is only applied to ports with the tagging modes of **Untag All** and **Tag PVID Only**.

To configure VCC using the ACLI, refer to the following commands:

- Displaying VLAN Configuration Control settings on page 149
- Modifying VLAN Configuration Control settings on page 149

# Displaying VLAN Configuration Control settings

Use the following procedure to display the current VLAN Configuration Control setting.

### Procedure steps

To display VLAN Configuration Control settings, use the following command from Global Configuration mode.

```
show vlan configcontrol
```

# Modifying VLAN Configuration Control settings

Use the following procedure to modify the current VLAN Configuration Control setting. This command applies the selected option to all VLANs on the switch.

### Procedure steps

To modify VLAN Configuration Control settings, use the following command from Global Configuration more

```
vlan configcontrol <vcc_option>
```

### Variable definitions

| Variable | Value |
|---|---|
| <vcc_option> | This parameter denotes the VCC option to use on the switch. The valid values are:<br><br>• automatic -- Changes the VCC option to Automatic.<br><br>• autopvid -- Changes the VCC option to AutoPVID. |

| Variable | Value |
|---|---|
| | • flexible -- Changes the VCC option to Flexible. |
| | • strict -- Changes the VCC option to Strict. This is the default VCC value. |
| | For more information about these options, refer to [Configuring VLAN Configuration Control](#) on page 148. |

# Managing the MAC address forwarding database table

This section shows you how to view the contents of the MAC address forwarding database table, as well as setting the age-out time for the addresses. The following topics are covered:

- [Displaying MAC address forwarding table](#) on page 150
- [Configuring MAC address retention](#) on page 151
- [Setting MAC address retention time to default](#) on page 151

The MAC flush feature is a direct way to flush MAC addresses from the MAC address table. The MAC flush commands allow flushing of:

- a single MAC address (see [Removing a single address from the MAC address table](#) on page 153)
- all addresses from the MAC address table (see [Clearing the MAC address table](#) on page 152
- a port or list of ports (see [Clearing the MAC address table on a FastEthernet interface](#) on page 152)
- a trunk (see [Clearing the MAC address table on a trunk](#) on page 152)
- a VLAN (see [Clearing the MAC address table on a VLAN](#) on page 152)

MAC flush deletes dynamically learned addresses. MAC flush commands may not be executed instantly when the command is issued. Since flushing the MAC address table is not considered an urgent task, MAC flush commands are assigned the lowest priority and placed in a queue.

The MAC flush commands are supported in ACLI, SNMP, or EDM.

## Displaying MAC address forwarding table

Use the following procedure to display the current contents of the MAC address forwarding database table. You can filter the MAC Address table by port number. The MAC address table can store up to 16000 addresses.

**Procedure steps**

To displaying the MAC address forwarding table, use the following command from Privileged EXEC mode

```
show mac-address-table [vid <1-4094>] [aging-time] [address
<H.H.H>] [port <portlist>]
```

**Variable definitions**

| Variable | Value |
|---|---|
| vid <1-4094> | Enter the number of the VLAN for which you want to display the forwarding database. Default is to display the management VLAN's database. |
| aging-time | Displays the time in seconds after which an unused entry is removed from the forwarding database. |
| address <H.H.H> | Displays a specific MAC address if it exists in the database. Enter the MAC address you want displayed. |

# Configuring MAC address retention

Use the following procedure to set the time during which the switch retains unseen MAC addresses.

**Procedure steps**

To configure unseen MAC address retention, use the following command from Global Configuration mode.

```
mac-address-table aging-time <10-1 000 000>
```

**Variable definitions**

| Variable | Value |
|---|---|
| vid <10-1 000 000> | Enter the aging time in seconds that you want for MAC addresses before they expire. |

# Setting MAC address retention time to default

Use the following procedure to set the retention time for unseen MAC addresses to 300 seconds.

**Procedure steps**

To set the MAC address retention time to default, use the following command from Global Configuration mode.

```
default mac-address-table aging-time
```

# Clearing the MAC address table

Use the following procedure to clear the MAC address table.

### Procedure steps

To flush the MAC address table, use the following command from Privileged EXEC mode.

```
clear mac-address-table
```

# Clearing the MAC address table on a VLAN

Use the following procedure to flush the MAC addresses for the specified VLAN.

### Procedure steps

To flush the MAC address table for a specific VLAN, use the following command from Privileged EXEC mode.

```
clear mac-address-table interface vlan <vlan #>
```

# Clearing the MAC address table on a FastEthernet interface

Use the following procedure to flush the MAC addresses for the specified ports. This command does not flush the addresses learned on the trunk.

### Procedure steps

TO clear the MAC address table on a FastEthernet interface, use the following command from Privileged EXEC mode.

```
clear mac-address-table interface FastEthernet <port-list|ALL>
```

# Clearing the MAC address table on a trunk

Use the following procedure to flush the MAC addresses for the specified trunk. This command flushes only addresses that are learned on the trunk.

**Procedure steps**

To clear the MAC address table on a trunk, use the following command from Privileged EXEC mode.

```
clear mac-address-table interface mlt <trunk_number>
```

## Removing a single address from the MAC address table

Use the following procedure to flush one MAC address from the MAC address table.

**Procedure steps**

To flush a single MAC address, use the following command from Privileged EXEC mode.

```
clear mac-address-table address <H.H.H>
```

# IP Directed Broadcasting

IP directed broadcasting takes the incoming unicast Ethernet frame, determines that the destination address is the directed broadcast for one of its interfaces, and then forwards the datagram onto the appropriate network using a link-layer broadcast.

IP directed broadcasting in a VLAN forwards direct broadcast packets in two ways:

- Through a connected VLAN subnet to another connected VLAN subnet.
- Through a remote VLAN subnet to the connected VLAN subnet.

By default, this feature is disabled.

The following ACLI commands are used to work with IP directed broadcasting:

-

## Enabling IP directed broadcast

Use the following procedure to enable IP directed broadcast.

**Procedure steps**

To enable IP directed broadcast, use the following command from Global Configuration mode.

```
[no] ip directed-broadcast enable
```

Use the **no** form of this command to disable.

*Comments? infodev@avaya.com*

# Chapter 9: Configuring STP using the ACLI

## Setting the STP mode using the ACLI

Use the following procedure to set the STP operational mode to STPG (Avaya Multiple Spanning Tree Protocol), RSTP (802.1w Rapid Spanning Tree Protocol), or MSTP (802.1s Multiple Spanning Tree Protocol).

## Procedure steps

To set the STP mode, use the following command from Global Configuration mode.

```
spanning-tree op-mode {stpg | rstp | mst}
```

## Configuring STP BPDU Filtering using the ACLI

Use the following procedure to configure STP BPDU Filtering on a port. This command is available in all STP modes (STPG, RSTP, and MSTP).

## Procedure steps

1. To enable STP BPDU filtering, use the following command from Interface Configuration mode.

   ```
   [no] spanning-tree bpdu-filtering [port <portlist>] [enable]
   [timeout <10-65535 | 0> ]
   ```

   Use the no form of this command to disable.

2. To set the STP BPDU Filtering properties on a port to their default values, use the following command from the Interface Configuration command mode:

```
default spanning-tree bpdu-filtering [port <portlist>]
[enable] [timeout]
```

3. To show the current status of the BPDU Filtering parameters, use the following command from the Privileged EXEC mode:

```
show spanning-tree bpdu-filtering [<interface-type>][port
<portlist>]
```

## Variable definitions

| Variable | Value |
|---|---|
| port <portlist> | Specifies the ports affected by the command. |
| enable | Enables STP BPDU Filtering on the specified ports. The default value is disabled. |
| timeout <10-65535 \| 0 > | When BPDU filtering is enabled, this indicates the time (in seconds) during which the port remains disabled after it receives a BPDU. The port timer is disabled if this value is set to 0. The default value is 120 seconds. |

# Creating and Managing STGs using the ACLI

To create and manage Spanning Tree Groups, you can refer to the Command Line Interface commands listed in this section. Depending on the type of Spanning Tree Group that you want to create or manage, the command mode needed to execute these commands can differ.

In the following commands, the omission of any parameters that specify a Spanning Tree Group results in the command operating against the default Spanning Tree Group (Spanning Tree Group 1).

To configure STGs using the ACLI, refer to the following:

# Configuring path cost calculation mode

Use the following procedure to set the path cost calculation mode for all Spanning Tree Groups on the switch.

## Procedure steps

To configure path cost calculation mode, use the following command from Privileged EXEC mode.

```
spanning-tree cost-calc-mode {dot1d | dot1t}
```

# Configuring STG port membership mode

Use the following procedure to set the STG port membership mode for all Spanning Tree Groups on the switch.

## Procedure steps

To configure STG port membership mode, use the following command from Privileged EXEC mode.

```
spanning-tree port-mode {auto | normal}
```

# Displaying STP configuration information

Use the following procedure to display spanning tree configuration information that is specific to either the Spanning Tree Group or to the port.

## Procedure steps

To display STP configuration information, use the following command from Privileged EXEC mode.

```
show spanning-tree [stp <1-8>] {config | port| port-mode |
vlans}
```

## Variable definitions

| Variable | Value |
|---|---|
| stp <1-8> | Displays specified Spanning Tree Group configuration; enter the number of the group to be displayed. |
| config \| port \| port-mode \| vlans | Displays spanning tree configuration for:<br><br>• config--the specified (or default) Spanning Tree Group<br><br>• port--the ports within the Spanning Tree Group<br><br>• port-mode--the port mode<br><br>• vlans--the VLANs that are members of the specified Spanning Tree Group |

# Creating a Spanning Tree Group

Use the following procedure to create a Spanning Tree Group.

## Procedure steps

To create a Spanning Tree Group, use the following command from Global Configuration mode.

```
spanning-tree stp <1-8> create
```

# Deleting a Spanning Tree Group

Use the following procedure to delete a Spanning Tree Group.

## Procedure steps

To delete a Spanning Tree Group, use the following command from Global Configuration mode.

```
spanning-tree stp <1-8> delete
```

# Enabling a Spanning Tree Group

Use the following procedure to enable a Spanning Tree Group.

## Procedure steps

To enable a Spanning Tree Group, use the following command from Global Configuration mode.

```
spanning-tree stp <1-8> enable
```

# Disabling a Spanning Tree Group

Use the following procedure to disable a Spanning Tree Group.

## Procedure steps

To disable a Spanning tree Group, use the following command from Global Configuration mode.

```
spanning-tree stp <1-8> disable
```

# Configuring STP values

Use the following procedure to set STP values by STG.

## Procedure steps

To configure STP values, use the following command from Global Configuration mode.

```
spanning-tree [stp <1-8>] [forward-time <4-30>] [hello-time
<1-10>] [max-age <6-40>] [priority {0*0000 | 0*1000| 0*2000 |
```

```
0*3000 | ... | 0*E000 | 0*F000}] [tagged-bpdu {enable |
disable}] [tagged-bpdu-vid <1-4094>] [multicast-address
<H.H.H>] [add-vlan] [remove-vlan]
```

## Variable definitions

| Variable | Value |
|---|---|
| stp <1-8> | Specifies the Spanning Tree Group; enter the STG ID. |
| forward-time <4-30> | Enter the forward time of the STG in seconds; the range is 4 -- 30, and the default value is 15. |
| hello-time <1-10> | Enter the hello time of the STG in seconds; the range is 1 --10, and the default value is 2. |
| max-age <6-40> | Enter the max-age of the STG in seconds; the range is 6 -- 40, and the default value is 20. |
| priority {0x000 | 0x1000 | 0x2000 | 0x3000 | .... | 0xE000 | 0xF000} | Sets the spanning tree priority (in Hex); if 802.1T compliant, this value must be a multiple of 0x1000. |
| tagged-bpdu {enable | disable} | Sets the BPDU as tagged or untagged. The default value for Spanning Tree Group 1 (default group) is untagged; the default for the other groups is tagged. |
| tagged-bpdu-vid <1-4094> | Sets the VLAN ID (VID) for the tagged BPDU. The default value is 4001 -- 4008 for STG 1 -- 8, respectively. |
| multicast-address <H.H.H> | Sets the spanning tree multicast address. |
| add-vlan | Adds a VLAN to the Spanning Tree Group. |
| remove-vlan | Removes a VLAN from the Spanning Tree Group. |

## Restoring default Spanning Tree values

Use the following procedure to restore default spanning tree values for the Spanning Tree Group.

## Procedure steps

To restore Spanning Tree values to default, use the following command from Global Configuration mode.

```
default spanning-tree [stp <1-8>] [forward-time] [hello-time]
[max-age] [priority] [tagged-bpdu] [multicast address]
```

## Variable definitions

| Variable | Value |
|---|---|
| stp <1-8> | Disables the Spanning Tree Group; enter the STG ID. |
| forward-time | Sets the forward time to the default value of 15 seconds. |
| hello-time | Sets the hello time to the default value of 2 seconds. |
| max-age | Sets the maximum age time to the default value of 20 seconds. |
| priority | Sets spanning tree priority (in Hex); if 802.1T compliant, this value must be a multiple of 0x1000. |
| tagged-bpdu | Sets the tagging to the default value. The default value for Spanning Tree Group 1 (default group) is untagged; the default for the other groups is tagged. |
| multicast address | Sets the spanning tree multicast MAC address to the default. |

# Adding a VLAN to a STG

Use the following procedure to add a VLAN to a specified Spanning Tree Group.

## Procedure steps

To add a VLAN to a STG, use the following command from Global Configuration mode.

```
spanning-tree [stp <1-8>] add-vlan <1-4094>
```

# Removing a VLAN from a STG

Use the following procedure to remove a VLAN from a specified Spanning Tree Group.

## Procedure steps

To remove a VLAN from a STG, use the following command from Global Configuration mode.

```
spanning-tree [stp <1-8>] remove-vlan <1-4094>
```

# Configuring STP and MSTG participation

Use the following procedure to set the Spanning Tree Protocol (STP) and multiple Spanning Tree Group (STG) participation for the ports within the specified Spanning Tree Group.

## Procedure steps

To configure STP and MSTG participation, use the following command from Interface Configuration mode.

```
[no] spanning-tree [port <portlist>] [stp <1-8>] [learning
{disable | normal | fast}] [cost <1-65535>] [priority]
```

Use the **no** form of this command to disable.

## Variable definitions

| Variable | Value |
|---|---|
| port <portlist> | Enables the spanning tree for the specified port or ports; enter port or ports you want enabled for the spanning tree.<br><br>**Note:**<br>If you omit this parameter, the system uses the port number you specified when you issued the interface command to enter the Interface Configuration mode. |
| stp <1-8> | Specifies the spanning tree group; enter the STG ID. |
| learning {disable\|normal\|fast} | Specifies the STP learning mode:<br><br>• disable -- disables FastLearn mode<br><br>• normal -- changes to normal learning mode<br><br>• fast -- enables FastLearn mode |

| Variable | Value |
|---|---|
| cost <1-65535> | Enter the path cost of the spanning tree; range is 1 -- 65535. |
| priority | Sets the spanning tree priority for a port as a hexadecimal value. If the Spanning Tree Group is 802.1T compliant, this value must be a multiple of 0x10. |

# Resetting Spanning Tree values for ports to default

Use the following procedure to set the spanning tree values for the ports within the specified Spanning Tree Group to the factory default settings.

## Procedure steps

To reset Spanning Tree values to default, use the following command from Interface Configuration mode.

```
default spanning-tree [port <portlist>] [stp <1-8>] [learning]
[cost] [priority]
```

## Variable definitions

| Variable | Value |
|---|---|
| port <portlist> | Enables spanning tree for the specified port or ports; enter port or ports to be set to factory spanning tree default values.<br><br>**Note:**<br>If this parameter is omitted, the system uses the port number specified when the interface command was used to enter Interface Configuration mode. |
| stp <1-8> | Specifies the Spanning Tree Group to set to factory default values; enter the STG ID. This command places the port into the default STG. The default value for STG is 1. |
| learning | Sets the spanning tree learning mode to the factory default value.<br>The default value for learning is Normal mode. |
| cost | Sets the path cost to the factory default value. |

| Variable | Value |
|---|---|
|  | The default value for path cost depends on the type of port. |
| priority | Sets the priority to the factory default value.<br>The default value for the priority is 0x8000. |

# Managing RSTP using the ACLI

Use the following command to configure RSTP:

# Configuring RSTP parameters

Use the following procedure to set the RSTP parameters which include forward delay, hello time, maximum age time, default path cost version, bridge priority, transmit holdcount, and version for the bridge.

## Procedure steps

To configure RSTP parameters, use the following command from Global Configuration mode.

```
spanning-tree rstp [ forward-time <4 - 30>] [hello-time <1 -
10>] [max-age <6 - 40>] [pathcost-type {bits16 | bits32}]
[priority {0000|1000|2000| ...| F000}] [tx-holdcount <1 - 10>]
[version {stp-compatible | rstp}]
```

## Variable definitions

| Variable | Value |
|---|---|
| forward-time <4- 30> | Sets the RSTP forward delay for the bridge in seconds; the default is 15. |

| Variable | Value |
|---|---|
| hello-time <1- 10> | Sets the RSTP hello time delay for the bridge in seconds; the default is 2. |
| max-age <6 - 40> | Sets the RSTP maximum age time for the bridge in seconds; the default is 20. |
| pathcost-type {bits16 \| bits32} | Sets the RSTP default path cost version; the default is bits32. |
| priority {0000 \| 1000 \| ... \| F000} | Sets the RSTP bridge priority (in hex); the default is 8000. |
| tx-hold count | Sets the RSTP Transmit Hold Count; the default is 3. |
| version {stp-compatible \| rstp} | Sets the RSTP version; the default is rstp. |

# Configuring RSTP on a port

Use the following procedure to set the RSTP parameters, which include path cost, edge-port indicator, learning mode, point-to-point indicator, priority, and protocol migration indicator on the single or multiple port.

## Procedure steps

To configure RSTP on a port, use the following command from Interface Configuration mode.

```
spanning-tree rstp [port <portlist>] [cost <1 - 200000000>]
[edge-port {false | true}] [learning {disable | enable}] [p2p
{auto | force-false | force-true}] [priority {00 | 10 | ... |
F0}] [protocol-migration {false | true}]
```

## Variable definitions

| Variable | Value |
|---|---|
| port <portlist> | Filter on list of ports. |
| cost <1 - 200000000> | Sets the RSTP path cost on the single or multiple ports; the default is 200000. |
| edge-port {false \| true} | Indicates whether the single or multiple ports are assumed to be edge ports. This parameter sets the Admin value of edge port status; the default is false. |

| Variable | Value |
|---|---|
| learning {disable \| enable} | Enables or disables RSTP on the single or multiple ports; the default is enable. |
| p2p {auto \| force-false \| force-true} | Indicates whether the single or multiple ports are to be treated as point-to-point links. This command sets the Admin value of P2P Status; the default is force-true. |
| priority {00 \| 10 \|... \| F0} | Sets the RSTP port priority on the single or multiple ports; the default is 80. |
| protocol-migration {false \| true} | Forces the single or multiple port to transmit RSTP BPDUs when set to true, while operating in RSTP mode; the default is false. |

# Displaying RSTP configuration

Use the following procedure to display the Rapid Spanning Tree Protocol (RSTP) related bridge-level configuration details.

## Procedure steps

To display RSTP configuration details, use the following command from Privileged EXEC mode.

```
show spanning-tree rstp {config | status | statistics}
```

## Variable definitions

| Variable | Value |
|---|---|
| config | Displays RSTP bridge-level configuration. |
| status | Displays RSTP bridge-level role information. |
| statistics | Displays RSTP bridge-level statistics. |

# Displaying RSTP port configuration

Use the following procedure to display the Rapid Spanning Tree Protocol (RSTP) related port-level configuration details.

## Procedure steps

To display RSTP port configuration, use the following command from Privileged EXEC mode.

```
show spanning-tree rstp port {config | status | statistics |
role} [<portlist>]
```

## Variable definitions

| Variable | Value |
|---|---|
| config | Displays RSTP port-level configuration. |
| status | Displays RSTP port-level role information. |
| statistics | Displays RSTP port-level statistics. |
| role | Displays RSTP port-level status. |

# Managing MSTP using the ACLI

## Configuring MSTP parameters

Use the following procedure to set the MSTP parameters, which include maximum hop count, maximum number of instances allowed, forward delay time, hello time, maximum age time, default path cost version, priority, transmit hold count, and version for the Cist Bridge.

## Procedure steps

To configure MSTP parameters, use the following command from Global Configuration mode.

```
spanning-tree mstp [max-hop <600 - 4000>] [forward-time <4 -
30>] [max-age <6 - 40>] [pathcost-type {bits16 | bits32}]
[priority {0000 | 1000 | 2000 | ... | F000}] [tx-hold count <1
- 10>] [version {stp-compatible | rstp| mstp}] [add-vlan <1 -
4094>] [remove-vlan <1 - 4094>]
```

## Variable definitions

| Variable | Value |
|---|---|
| max-hop <600 - 4000> | Sets the MSTP maximum hop count for the CIST bridge; the default is 2000. |
| forward-time <4 - 30> | Sets the MSTP forward delay for the CIST bridge in seconds; the default is 15. |
| max-age <6 - 40> | Sets the MSTP maximum age time for the CIST bridge in seconds; the default is 20. |
| pathcost-type {bits16 | bits32} | Sets the MSTP default path cost version; the default is bits32. |
| priority {0000 | 1000| 2000 ... | F000} | Sets the MSTP bridge priority for the CIST Bridge; the default is 8000. |
| tx-holdcount<1 - 10> | Sets the MSTP Transmit Hold Count; the default is 3. |
| version {stp-compatible | rstp | mstp} | Sets the MSTP version for the Cist Bridge; the default is mstp. |
| add-vlan <1 - 4094> | Adds a VLAN to the CIST bridge. |
| remove-vlan <1 - 4094> | Removes the specified VLAN from the CIST bridge. |

## Configuring MSTP on a port

Use the following procedure to set the MSTP parameters, which include path cost, hello time, edge-port indicator, learning mode, point-to-point indicator, priority, and protocol migration indicator on the single or multiple ports for the Common Spanning Tree.

## Procedure steps

To configure MSTP on a port, use the following command from Interface Configuration mode.

```
spanning-tree mstp [port <portlist>] [cost <1 - 200000000>]
[edge-port {false | true}][hello-time <1 - 10>] [learning
{disable | enable}][p2p {auto | force-false | force-true}]
[priority {00 | 10 | < | F0}] [protocol-migration {false |
true}]
```

## Variable definitions

| Variable | Value |
|---|---|
| port <portlist> | Enter a list or range of port numbers. |
| cost <1 - 200000000> | Sets the MSTP path cost on the single or multiple ports for the CIST; the default is 200000. |
| hello-time <1 - 10> | Sets the MSTP hello time on the single or multiple ports for the CIST; the default is 2. |
| edge-port {false | true} | Indicates whether the single or multiple ports are assumed to be edge ports. This parameter sets the Admin value of edge port status; the default is false. |
| learning {disable | enable} | Enables or disables MSTP on the single or multiple ports; the default is enable. |
| p2p {auto | force-false | force-true} | Indicates whether the single or multiple ports are treated as point-to-point links. This command sets the Admin value of P2P Status; the default is force-true. |
| priority {00 | 10 |... | F0} | Sets the MSTP port priority on the single or multiple ports; the default is 80. |
| protocol-migration {false | true} | Forces the single or multiple ports to transmit MSTP BPDUs when set to true, while operating in MSTP mode; the default is false. |

## Configuring MSTP region parameters

Use the following procedure to set the MSTP parameters, which include config ID selector, region name, and region version.

## Procedure steps

To configure MSTP region parameters, use the following command from Global Configuration mode.

```
spanning-tree mstp region [config-id-sel <0 - 255>] [region-
name <1 - 32 chars>][region-version <0 - 65535>]
```

## Variable definitions

| Variable | Value |
|---|---|
| [config-id-sel <0 - 255>] | Sets the MSTP config ID selector; the default is 0. |
| [region-name <1 - 32 chars>] | Sets the MSTP region name; the default is the bridge MAC address. |
| [region-version <0 - 65535>] | Sets the MSTP region version; the default is 0. |

# Configuring MSTP parameters

Use the following procedure to set the MSTP parameters, which include forward delay time, hello-time, maximum hop count, priority, and VLAN mapping for the bridge instance.

## Procedure steps

To configure MSTP parameters, use the following command from Global Configuration mode.

```
spanning-tree mstp msti <1 - 7> [priority{0000|1000|...|F000}]
[add-vlan <vid>] [remove-vlan <vid>] [enable]
```

## Variable definitions

| Variable | Value |
|---|---|
| <1 - 7> | Filter on MSTP instance. |
| priority {0000 | 1000 |... | F000} | Sets the MSTP priority for the bridge instance; the default is 8000. |

| Variable | Value |
|---|---|
| add-vlan <1 - 4094> | Maps the specified Vlan and MSTP bridge instance. |
| remove-vlan <1 - 4094> | Unmaps the specified Vlan and MSTP bridge instance. |
| enable | Enables the MSTP bridge instances. |

# Disabling a MSTP bridge instance

Use the following procedure to disable a MSTP bridge instance.

## Procedure steps

To disable a MSTP bridge instance, use the following command from Global Configuration mode.

```
no spanning-tree mstp msti <1 - 7> enable
```

# Deleting a MSTP bridge instance

Use the following procedure to delete a MSTP bridge-instance.

## Procedure steps

To delete a MSTP bridge instance, use the following command from Global Configuration mode.

```
no spanning-tree mstp msti <1 - 7>
```

# Displaying MSTP status

Use the following procedure to display Multi Spanning Tree Protocol (MSTP) related status information known by the selected bridge.

## Procedure steps

To display MSTP status, use the following command from Privileged EXEC mode.

```
show spanning-tree mstp {config | status | statistics}
```

## Variable definitions

| Variable | Value |
|---|---|
| config | Displays the MSTP-related bridge-level VLAN and region information. |
| status | Displays the MSTP-related bridge-level status information known by the selected bridge. |
| statistics | Displays the MSTP-related bridge-level statistics. |

# Displaying MSTP Cist port information

Use the following procedure to display Multi Spanning Tree Protocol (MSTP) Cist Port information maintained by every port of the Common Spanning Tree.

## Procedure steps

To display MSTP Cist port information, use the following command from Privileged EXEC mode.

```
show spanning-tree mstp port {config | role | statistics }
[<portlist>]
```

## Variable definitions

| Variable | Value |
|---|---|
| <portlist> | Enter a list or range of port numbers. |
| config | Displays the MSTP CIST port information maintained by every port of the Common Spanning Tree. |
| role | Displays MSTP CIST related port role information maintained by every port. |
| statistics | Displays the MSTP CIST Port statistics maintained by every port. |

# Displaying MSTP MSTI settings

Use the following procedure to display MSTP MSTI settings.

## Procedure steps

To display MSTP MSTI settings, use the following command from Global Configuration mode.

```
show spanning-tree mstp msti [config] [statistics] [port
{config | role | statistics}] <1 - 7>
```

## Variable definitions

| Variable | Value |
|---|---|
| config | Displays the MSTP instance-specific configuration and the VLAN mapping port. |
| statistics | Displays MSTP instance-specific statistics. |
| port {config \| role \| statistics} | Displays MSTP instance-specific port information:<br><br>• config: displays MSTI port configuration<br><br>• role: displays MSTI port role information<br><br>• statistics: displays MSTI port statistics |
| <1 - 7> | Specifies the MSTI instance for which to display the statistics. |

# Chapter 10: Configuring MLT using the ACLI

The Command Line Interface commands detailed in this section allow for the creation and management of Multi-Link trunks. Depending on the type of Multi-Link trunk being created or managed, the command mode needed to execute these commands can differ.

## Displaying MLT configuration and utilization

Use the following procedure to display Multi-Link Trunking (MLT) configuration and utilization.

### Procedure steps

To display MLT configuration and utilization, use the following command from Privileged EXEC mode.

```
show mlt [utilization <1-32>]
```

## Configuring a Multi-Link trunk

Use the following procedure to configure a Multi-Link trunk (MLT).

### Procedure steps

To configure a Multi-Link trunk, use the following command from Global Configuration mode.

```
mlt <id> [name <trunkname>] [enable | disable] [member
<portlist>] [learning {disable | fast | normal}] [bpdu {all-
ports | single-port}] loadbalance {basic | advance}
```

## Variable definitions

| Variable | Value |
|---|---|
| id | Enter the trunk ID; the range is 1 to 32. |
| name <trunkname> | Specifies a text name for the trunk; enter up to 16 alphanumeric characters. |
| enable \| disable | Enables or disables the trunk. |
| member <portlist> | Enter the ports that are members of the trunk. |
| learning <disable \| fast \| normal> | Sets STP learning mode. |
| bpdu {all-ports \| single-port} | Sets trunk to send and receive BPDUs on either all ports or a single port. |
| loadbalance {basic \| advance} | Sets the MLT load-balancing mode: - basic: MAC-based load-balancing - advance: IP-based load-balancing |

# Disabling a MLT

Use the following procedure to disable a Multi-Link trunk (MLT), clearing all the port members.

## Procedure steps

To disable a MLT, use the following command from Global Configuration mode.

```
no mlt [<id>]
```

# Displaying MLT properties

Use the following procedure to display the properties of Multi-Link trunks (MLT) participating in Spanning Tree Groups (STG).

## Procedure steps

To display MLT properties, use the following command from Global Configuration mode.

```
show mlt spanning-tree <1-32>
```

# Configuring STP participation for MLTs

Use the following procedure to set Spanning Tree Protocol (STP) participation for Multi-Link trunks (MLT).

## Procedure steps

To configure STP participation for MLTs, use the following command from Global Configuration mode.

```
mlt spanning-tree <1-32> [stp <1-8, ALL>] [learning {disable |
normal | fast}]
```

## Variable definitions

| Variable | Value |
|---|---|
| <1 - 32> | Specifies the ID of the MLT to associate with the STG. |
| stp <1 - 8> | Specifies the spanning tree group. |
| learning {disable \| normal \| fast} | Specifies the STP learning mode:<br><br>• disable -- disables learning<br><br>• normal -- sets the learning mode to normal<br><br>• fast -- sets the learning mode to fast |

# Configuring SMLT using the ACLI

To configure SMLT using the ACLI, refer to the following:

> **Note:**
>
> To configure SMLT on the 5000 Series switch, an Advanced License must be purchased that allows this feature to be used.

# Setting command mode to MLT Interface mode

> **Important:**
>
> For SMLT to function properly, you must manually disable STP on all SMLT, IST, and SLT ports in all spanning tree groups or instances to which the ports belong. You must also disable STP on all edge switch MLT ports that are connected to the SMLT or SLT.

Use the following procedure to set ACLI command mode to MLT Interface mode from which you can configure SMLTs and ISTs.

> **Note:**
>
> You create SLTs from the config-if command mode. For details, see Creating a SLT on a port on page 180.

## Procedure steps

To set the command mode, use the following command from Global Configuration mode.

```
interface mlt [<1-32>]
```

# Creating a SMLT

> **Important:**
>
> For SMLT to function properly, you must manually disable STP on all SMLT, IST, and SLT ports in all spanning tree groups or instances to which the ports belong. You must also disable STP on all edge switch MLT ports that are connected to the SMLT or SLT.

Use the following procedure to create a SMLT from an existing MLT.

## Procedure steps

To create a SMLT, use the following command from Interface Configuration mode.

```
smlt <1-32>
```

> **Note:**
>
> Before you can create an SMLT, you must first create and enable an MLT (see Configuring a Multi-Link trunk on page 175).

# Creating a IST

> **Important:**
>
> For SMLT to function properly, you must manually disable STP on all SMLT, IST, and SLT ports in all spanning tree groups or instances to which the ports belong. You must also disable STP on all edge switch MLT ports that are connected to the SMLT or SLT.

Use the following procedure to create a IST from an existing MLT.

## Procedure steps

To create a IST, use the following command from MLT Interface Configuration mode.

```
ist [enable] [peer-ip <A.B.C.D>] [vlan <1-4096>]
```

The peer IP address is the IP address of the IST VLAN on the peer aggregation switch. A VLAN created on the redundant aggregation switch must also be created on the second aggregation switch. The IST treats the two switches as a single switch. To allow the two switches to communicate, you must assign an IP address to both VLANs.

## Variable definitions

| Variable | Value |
|----------|-------|
| enable | Enables the IST on the MLT specified by the interface mlt command. |
| vlan <1-4096> | Specifies a VLAN ID for the IST. |
| peer-ip <A.B.C.D> | Specifies the peer IP address for the IST. |

# Creating a SLT on a port

**Important:**

For SMLT to function properly, you must manually disable STP on all SMLT, IST, and SLT ports in all spanning tree groups or instances to which the ports belong. You must also disable STP on all edge switch MLT ports that are connected to the SMLT or SLT.

Use the following procedure to create a SLT on a port.

## Procedure steps

To create a SLT on a port, use the following command from Interface Configuration mode.

```
smlt [port <portlist>] <1-512>
```

## Variable definitions

| Variable | Value |
|----------|-------|
| port <portlist> | Specifies the port to configure as an SLT. |
| <1-512> | Specifies the ID for the SLT. |

# Disabling SMLT

Use the following procedure to disable a SMLT.

## Procedure steps

To disable a SMLT, use the following command from Interface Configuration mode.

```
no smlt <1-32>
```

# Disabling IST

Use the following procedure to disable a IST and clear the IST settings.

## Procedure steps

To disable a IST, use the following command from Interface Configuration mode.

```
no ist [enable] [peer-ip]
```

## Variable definitions

| Variable | Value |
|----------|-------|
| enable | Disables the IST on the MLT specified by the interface mlt command. |
| vlan <1-4096> | Clears the VLAN ID from the IST. |
| peer-ip <A.B.C.D> | Clears the peer IP address from the IST. |

# Disabling a SLT on a port

Use the following procedure to disable a SLT on a port.

## Procedure steps

To disable a SLT on a port, use the following command from Interface Configuration mode.

```
no smlt [port <portlist>]
```

# Resetting SMLT to default

Use the following procedure to reset a SMLT to default.

## Procedure steps

To reset a SMLT to default, use the following command from Interface Configuration mode.

```
default smlt <1-32>
```

# Resetting a IST to default

Use the following procedure to reset a IST to default settings.

## Procedure steps

To reset a IST to default settings, use the following command from MLT Interface Configuration mode.

```
default ist [enable] [peer-ip]
```

## Variable definitions

| Variable | Value |
|----------|-------|
| enable | Disables the IST on the MLT specified by the interface mlt command. |
| peer-ip <A.B.C.D> | Clears the peer IP address from the IST. |

# Resetting a SMLT to default

Use the following procedure to reset SLT settings on a port to default.

## Procedure steps

To reset a SMLT to default, use the following command from Interface Configuration mode.

```
default smlt [port <portlist>] <1-512>
```

# Displaying IST parameters

Use the following procedure to display the IST parameters on the switch.

## Procedure steps

To display IST parameters, use the following command from Privileged EXEC mode.

```
show ist
```

# Displaying IST statistics

Use the following procedure to display IST statistics on the switch.

## Procedure steps

To display IST statistics, use the following command from Privileged EXEC mode.

```
show ist stat
```

# Displaying SLT and SMLT configurations

Use the following procedure to display SMLT and SLT configurations on the switch.

## Procedure steps

To display SLT and SMLT configurations, use the following command from Interface Configuration mode.

```
show smlt [<interface-type>]
```

## Variable definitions

| Variable | Value |
|---|---|
| <interface-type> | Interface types are<br><br>• mlt: Displays only the MLT-based SMLTs mlt id <1-32><br><br>• fastethernet: Displays only the SLTs slt-id <1-512> |

# Configuring SLPP using the ACLI

This section provides procedures used to configure Simple Loop Prevention Protocol (SLPP) using the ACLI.

## Configuring SLPP transmitting list

Use the following procedures to add a VLAN to the SLPP transmitting list.

## Procedure steps

To add a VLAN to the SLPP transmitting list, use the following command from Global Configuration mode:

```
[no] slpp vid <1-4095>
```

Use the **no** form of this command to remove a VLAN from the list.

## Enabling SLPP

Use the following procedure to globally enable SLPP.

## Procedure steps

To globally enable SLPP, use the following command from Global Configuration mode:

```
[no] slpp enable
```

Use the **no** form of this command to disable SLPP.

# Configuring SLPP PDU transmit interval

Use the following procedure to configure the SLPP PDU transmit interval in milliseconds. The default setting is 500 ms.

## Procedure steps

To configure the SLPP PDU transmit interval, use the following command from Global Configuration mode:

```
slpp tx-interval <500-5000>
```

# Configuring SLPP PDU ether type

Use the following procedure to configure the SLPP PDU ether type value. The default value is 0x8104.

> **Note:**
> Values 0x0000 and 0x8100 are disallowed.

## Procedure steps

To configure the SLPP ether type value, use the following command from Global Configuration mode:

```
slpp ethertype <0x0 - 0xffff>
```

# Configuring SLPP port auto enable

Use the following procedure to configure the auto enable timer for ports shut down by SLPP. If the timeout value is 0 (not active), the port will remain disabled until manually enabled by the user. The default value is 0.

## Procedure steps

To configure the auto enable timer, use the following command from Global Configuration mode:

```
slpp timeout <1-65535>
```

# Enabling SLPP PDU receive function per port

Use the following procedure to enable the SLPP PDU received function on a port.

## Procedure steps

To enable the SLPP PDU received function, use the following command from Global Configuration mode:

```
[no] slpp [port-portList] [packet-rx <enable>]
```

Use the **no** form of this command to disable the function.

# Configuring the SLPP PDU receipt threshold

Use the following procedure to configure the number of SLPP PDUs, in the range 1 to 500, that must be received prior to shutting down a port as a result of looping. The default threshold is 5.

## Procedure steps

To configure the SLPP PDU receipt threshold, use the following command from Global Configuration mode:

```
[no] slpp [port-portList] [1-500 <enable>]
```

Use the **no** form of this command to reset to default (1).

# Link Aggregation Control Protocol over SMLT using the ACLI

These sections describe commands for Release 6.2 that assist in the configuration of Link Aggregation Control Protocol (LACP) over SMLT. For more information about the procedure to configure LACP over SMLT, see LACP over SMLT configuration example on page 295.

## LACP over SMLT using the ACLI Navigation

- Configuring an SMLT MAC address on page 187
- Configuring the default SMLT MAC address on page 188
- Binding an MLT group to an administrative key and to an SMLT on page 188
- Freeing an MLT group on page 189

## Configuring an SMLT MAC address

Use the following procedure to configure the SMLT MAC address.

### Prerequisites

- Configure an SMLT. For more information, see Creating a SMLT on page 179.

### Procedure steps

To set the SMLT MAC address, use the following command in Interface Configuration mode:

```
lacp smlt-sys-id<H.H.H>
```

**Important:**

For information about how to use this command in the procedure to configure LACP over SMLT, see LACP over SMLT configuration example on page 295.

## Variable definitions

The following table defines parameters for the `lacp smlt-sys-id <H.H.H>` command.

| Variable | Value |
|---|---|
| <H.H.H> | Sets the SMLT MAC address. |

# Configuring the default SMLT MAC address

Use the following procedure to configure the default SMLT MAC address to return to the MAC address of the switch.

## Procedure steps

To configure the default SMLT MAC address, use the following command in Interface Configuration mode:

```
default lacp smlt-sys-id
```

# Binding an MLT group to an administrative key and to an SMLT

Use the following procedure y to bind an MLT group to an administrative key and to an SMLT.

## Prerequisites

- Configure an SMLT. For more information, see Creating a SMLT on page 179.
- Assign an administrative key to selected ports. For more information, see Configuring the LACP administrative key on page 195
- Enable LACP on the selected ports. For more information, see Configuring LACP operating mode on page 195.

## Procedure steps

To bind an MLT group to an administrative key and to an SMLT, use the following command in Global Configuration mode:

```
lacp key <1-4095> mlt <1-32> smlt <1-512>
```

**Important:**

For more information about how to use this command in the procedure to configure LACP over SMLT, see LACP over SMLT configuration example on page 295.

## Variable definitions

The following table defines parameters that you can use to Bind an MLT group to an administrative key and to an SMLT.

| Variable | Value |
|----------|-------|
| <1-4095> | Sets the administrative key value in the range of 1 to 4095. |
| mlt <1-32> | Sets the ID of the MLT in the range of 1–32. |
| smlt <1-512> | Sets the ID of the SMLT in the range of 1–512. |

# Freeing an MLT group

Use the following procedure to free an MLT group from an administrative key and from an SMLT.

## Procedure steps

To free an MLT group from an administrative key and from an SMLT, use the following command in Global Configuration mode:

```
default lacp key <1-4095> mlt
```

## Variable definitions

The following table defines optional parameters that you can use to free an MLT group from an administrative key and from an SMLT.

| Variable | Value |
|----------|-------|
| <1-4095> | Sets the administrative key value in the range of 1 to 4095 |

# Troubleshooting IST problems

Use the following procedure to troubleshooting IST problems and single-user problems.

## Procedure steps

1. Ensure that Global IP Routing is enabled.

2. Ensure that peers can ping each other.

3. Enter the `show ist stat` command to display the IST message count.

   The hello count should increment.

4. Enter the `show mlt` command to display all the MLTs in the switch and their properties, including running type, members, and status. Check the SMLT/SLT numbering: switches connected by SMLT must have the same SMLT IDs.

5. Ensure that the IST is up and running by using the `show ist` command.

6. If the IST is not running, ensure that:

   a. The correct VLAN ID exists on both sides of the IST

   b. The IST configuration contains the correct local and peer IP addresses

7. If IST is running, check whether the SMLT port is operating by using the `show smlt` command.

   a. If the current type is SMLT, the status is correct.

   b. If the current type is NORMAL, the link is running in a normal (single) mode and not in SMLT mode. The reasons for this can be as follows:

      • The remote SMLT link is not operational.

      • The ID is not configured on the other switch. To determine this, check to see whether the SMLT IDs match.

      • The IST is not up and running.

# Chapter 11: Configuring LACP and VLACP using the ACLI

This section contains information on the following topics:

## Configuring Link Aggregation using the ACLI

This section describes the commands necessary to configure and manage Link Aggregation using the Command Line Interface (ACLI).

To configure Link Aggregation using the ACLI, refer to the following:

## Displaying LACP system settings

Use the following procedure to display system-wide LACP settings.

## Procedure steps

To display system settings, use the following command from Privileged EXEC mode.

```
show lacp system
```

# Displaying LACP per port configuration

Use the following procedure to display information on the per-port LACP configuration. Select ports either by port number or by aggregator value.

## Procedure steps

To display per port configuration, use the following command from Privileged EXEC mode.

```
show lacp port [<portList> | aggr <1-65535>]
```

## Variable definitions

| Variable | Value |
|----------|-------|
| <portList> | Enter the specific ports for which to display LACP information. |
| aggr <1-65535> | Enter the aggregator value to display ports that are members of it. |

# Displaying LACP port mode

Use the following procedure to display the current port mode (default or advanced).

## Procedure steps

To display the port mode, use the following command from Privileged EXEC mode.

```
show lacp port-mode
```

# Displaying LACP port statistics

Use the following procedure to displayLACP port statistics. Select ports either by port number or by aggregator value.

## Procedure steps

To display port statistics, use the following command from Privileged EXEC mode.

```
show lacp stats [<portList> | aggr <1-65535>]
```

## Variable definitions

| Variable | Value |
|----------|-------|
| <portList> | Enter the specific ports for which to display LACP information. |
| aggr <1-65535> | Enter the aggregator value to display ports that are members of it. |

# Clearing LACP port statistics

Use the following procedure to clear existing LACP port statistics.

## Procedure steps

To clear statistics, use the following command from Interface Configuration mode.

```
lacp clear-stats <portList>
```

# Displaying LACP port debug information

Use the following procedure to display port debug information.

## Procedure steps

To display port debug information, use the following command from Privileged EXEC mode.

```
show lacp debug member [<portList>]
```

# Displaying LACP aggregators

Use the following procedure to display LACP aggregators or LACP trunks.

## Procedure steps

To display aggregators, use the following command from Privileged EXEC mode.

```
show lacp aggr <1-65535>
```

# Configuring LACP system priority

Use the following procedure to configure the LACP system priority. It is used to set the system-wide LACP priority. The factory default priority value is 32768.

## Procedure steps

To configure system priority, use the following command from Global Configuration mode.

```
lacp system-priority <0-65535>
```

# Enabling LACP port aggregation mode

Use the following procedure to enable the port aggregation mode.

## Procedure steps

To enable the port aggregation mode, use the following command from Interface Configuration mode.

```
[no] lacp aggregation [port <portList>] enable
```

Use the **no** form of the command to disable.

# Configuring the LACP administrative key

Use the following procedure to configure the administrative LACP key for a set of ports.

## Procedure steps

To set the administrative key, use the following command from Interface Configuration mode.

```
lacp key [port <portList>] <1-4095>
```

## Variable definitions

| Variable | Value |
|----------|-------|
| port <portList> | The ports to configure the LACP key for. |
| <1-4095> | The LACP key to use. |

# Configuring LACP operating mode

Use the following procedure to configure the LACP mode of operations for a set of ports.

## Procedure steps

To configure the operating mode, use the following command from Interface Configuration mode.

```
lacp mode [port <portList>] {active | passive | off}
```

## Variable definitions

| Variable | Value |
|----------|-------|
| port <portList> | The ports for which the LACP mode is to be set. |

| Variable | Value |
|----------|-------|
| {active \| passive \| off} | The type of LACP mode to set for the port. The LACP modes are:<br><br>• active -- The port will participate as an active Link Aggregation port. Ports in active mode send LACPDUs periodically to the other end to negotiate for link aggregation.<br><br>• passive -- The port will participate as a passive Link Aggregation port. Ports in passive mode send LACPDUs only when the configuration is changed or when its link partner communicates first.<br><br>• off -- The port does not participate in Link Aggregation.<br><br>LACP requires at least one end of each link to be in active mode. |

# Configuring per port LACP priority

Use the following procedure to configure the per-port LACP priority for a set of ports.

## Procedure steps

To configure priority, use the following command from Interface Configuration mode.

```
lacp priority [port <portList>] <0-65535>
```

## Variable definitions

| Variable | Value |
|----------|-------|
| port <portList> | The ports for which to configure LACP priority. |
| <0-65535> | The priority value to assign. |

# Configuring LACP periodic transmission timeout interval

Use the following procedure to configure the LACP periodic transmission timeout interval for a set of ports.

## Procedure steps

To configure the interval, use the following command from Interface Configuration mode.

```
lacp timeout-time [port <portList>] {long | short}
```

## Variable definitions

| Variable | Value |
|---|---|
| port <portList> | The ports for which to configure the timeout interval. |
| {long \| short} | Specify the long or short timeout interval. |

# Configuring LACP port mode

Use the following procedure to configure the LACP port mode on the switch.

## Procedure steps

To configure the port mode, use the following command from Global Configuration mode.

```
lacp port-mode {default | advance}
```

## Variable definitions

| Variable | Value |
|---|---|
| default | Default LACP port mode. |
| advance | Advanced LACP port mode. |

# Configuring VLACP using the ACLI

To configure VLACP using the ACLI, refer to the following commands:

**Note:**

When you set VLACP parameters for a trunk port, the settings are applied to all trunk members.

- Enabling VLACP globally on page 198
- Configuring VLACP multicast MAC address on page 198
- Configuring VLACP port parameters on page 198
- Displaying VLACP status on page 201
- Displaying VLACP port configuration on page 201

# Enabling VLACP globally

Use the following procedure to globally enable VLACP for the device.

## Procedure steps

To enable VLACP, use the following command from Global Configuration mode.

```
[no] vlacp enable
```

Use the **no** form of this command to disable.

# Configuring VLACP multicast MAC address

Use the following procedure to set the multicast MAC address used by the device for VLACPDUs.

## Procedure steps

To configure the multicast MAC address, use the following command from Global Configuration mode.

```
[no] vlacp macaddress <macaddress>
```

Use the **no** form of this command to delete the address.

# Configuring VLACP port parameters

Use the following procedure to configure VLACP parameters on a port.

## Procedure steps

To configure parameters, use the following command from Interface Configuration mode.

```
[no] vlacp port <slot/port> [enable | disable] [timeout <long/
short>] [fast-periodic-time <integer>] [slow-periodic-time
<integer>] [timeout-scale <integer>] [funcmac-addr <mac>]
[ethertype <hex>]
```

Use the **no** form of this command to remove parameters.

## Variable definitions

| Variable | Value |
|---|---|
| <slot/port> | Specifies the slot and port number. |
| enable\|disable | Enables or disables VLACP. |
| timeout <long/short> | Specifies whether the timeout control value for the port is a long or short timeout.<br><br>• long sets the port timeout value to: (timeout-scale value) × (slow-periodic-time value).<br><br>• short sets the port's timeout value to: (timeout-scale value) × (fast-periodic-time value).<br><br>For example, if the timeout is set to short while the timeout-scale value is 3 and the fast-periodic-time value is 400 ms, the timer expires after 1200 ms.<br>Default is long. |
| fast-periodic-time <integer> | Specifies the number of milliseconds between periodic VLACPDU transmissions using short timeouts.<br>The range is 400-20000 milliseconds. Default is 500. |
| slow-periodic-time <integer> | Specifies the number of milliseconds between periodic VLACPDU transmissions using long timeouts.<br>The range is 10000-30000 milliseconds. Default is 30000. |
| timeout-scale <integer> | Sets a timeout scale for the port, where timeout = (periodic time) × (timeout scale).<br>The range is 1-10. Default is 3. |

| Variable | Value |
|---|---|
| | Note: With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. However, if the timeout-scale is set to less than 3, the port timeout value does not take into account the normal travel time of the VLACPDU. The port expects to receive a VLACPDU at the same moment the partner port sends it. Therefore, the delayed VLACPDU results in the link being blocked, and then enabled again when the packet arrives. To prevent this scenario from happening, set the timeout-scale to a value larger than 3. VLACP partners must also wait 3 synchronized VLACPDUs to have the link enabled. If VLACP partner miss 3 consecutive packets from the other partner, sets the link as VLACP down. |
| funcmac-addr <mac> | Specifies the address of the far-end switch/stack configured to be the partner of this switch/stack. If none is configured, any VLACP-enabled switch communicating with the local switch through VLACP PDUs is considered to be the partner switch.<br>Note: VLACP has only one multicast MAC address, configured using the vlacp macaddress command, which is the Layer 2 destination address used for the VLACPDUs. The port-specific funcmac-addr parameter does not specify a multicast MAC address, but instead specifies the MAC address of the switch or stack to which this port is sending VLACPDUs. You are not always required to configure funcmac-addr. If not configured, the first VLACP-enabled switch that receives the PDUs from a unit assumes that it is the intended recipient and processes the PDUs accordingly.<br>If you want an intermediate switch to drop VLACP packets, configure the funcmac-addr parameter to the desired destination MAC address. With funcmac-addr configured, the intermediate switches do not misinterpret the VLACP packets. |
| ethertype <hex> | Sets the VLACP protocol identification for this port. Defines the ethertype value of the VLACP frame. The range is 8101-81FF. Default is 8103. |

# Displaying VLACP status

Use the following procedure to display the status of VLACP on the switch.

## Procedure steps

To display VLACP status, use the following command from Privileged EXEC mode.

```
show vlacp
```

# Displaying VLACP port configuration

Use the following procedure to display the VLACP configuration details for a port or list of ports.

## Procedure steps

To display port configuration, use the following command from Privileged EXEC mode.

```
show vlacp interface <slot/port>
```

where **<slot/port>** specifies a port or list of ports.

Among other properties, the **show vlacp interface** command displays a column called HAVE PARTNER , with possible values of yes or no .

If HAVE PARTNER is yes when ADMIN ENABLED and OPER ENABLED are true , then that port has received VLACPDUs from a port and those PDUs were recognized as valid according to the interface settings.

If HAVE PARTNER is no , when ADMIN ENABLED is true and OPER ENABLED is FALSE , then the partner for that port is down (that port received at least one correct VLACPDU, but did not receive additional VLACPDUs within the configured timeout period). In this case VLACP blocks the port. This scenario is also seen if only one unit has VLACP enabled and the other has not enabled VLACP.

The **show vlacp interface** command is in the privExec command mode.

> **Note:**
> If VLACP is enabled on an interface, the interface will not forward traffic unless it has a valid VLACP partner. If one partner has VLACP enabled and the other is not enabled, the unit

with VLACP enabled will not forward traffic, however the unit with VLACP disabled will continue to forward traffic.

# Chapter 12: Configuring ADAC using the ACLI

## Configuring ADAC for Avaya IP Phones using the ACLI

You can configure ADAC-related settings using the ACLI.

This section covers the following commands:

## Configuring global ADAC settings

Use the following procedure to configure the global ADAC settings for the device.

### Procedure steps

To configure settings, use the following command from Global Configuration mode.

```
[no] adac [enable] [op-mode <untagged-frames-basic | untagged-
frames-advanced| tagged-frames>] [traps enable] [voice-vlan
```

```
<1-4094>] [uplink-port <portlist>] [call-server-port
<portlist>]
```

## Variable definitions

| Variable | Value |
|---|---|
| enable | Enables ADAC on the device. |
| op-mode *<untagged-frames-basic\| untagged-frames-advanced \| tagged-frames >* | Sets the ADAC operation mode to one of the following:<br><br>• untagged-frames-basic: IP Phones send untagged frames, and the Voice VLAN is not created.<br><br>• untagged-frames-advanced: IP Phones send untagged frames, and the Voice VLAN is created.<br><br>• tagged-frames: IP Phones send tagged frames. |
| traps enable | Enables ADAC trap notifications. |
| voice-vlan *<1-4094>* | Sets the Voice VLAN ID. The assigned VLAN ID must not previously exist. |
| uplink-port *<slot/port>* | Sets the Uplink port. |
| uplink-port *<portlist>* | Sets a maximum of 8 ports as Uplink ports. |
| call-server-port *<slot/port>* | Sets the Call Server port. |
| call-server-port *<ports>* | Sets a maximum of 8 ports as Call Server ports. |

# Restoring default ADAC settings

Use the following procedure to restore the default ADAC settings on the device.

## Procedure steps

To restore settings, use the following command from Global Configuration mode.

```
default adac [enable] [op-mode] [traps enable] [voice-vlan]
[uplink-port] [call-server-port]
```

## Variable definitions

| Variable | Value |
|----------|-------|
| enable | Restores the default ADAC administrative state (disabled). |
| call-server-port | Restores the default Call Server port (none). |
| op-mode | Restores the default ADAC operation mode (Untagged Frames Basic). |
| traps enable | Restores the default state for ADAC notifications (enabled). |
| uplink-port | Restores the default Uplink port (none). |
| voice-vlan | Restores the default Voice-VLAN ID (none). |

# Configuring ADAC per port settings

Use the following procedure to set the per port ADAC settings for the device.

## Procedure steps

To configure settings, use the following command from Interface Configuration mode.

```
[no] adac [port <portlist>] {[enable] [tagged-frames-pvid
(<1-4094>|no-change)] [tagged-frames-tagging (tagAll|
tagPvidOnly|untagPvidOnly|no-change)]}
```

## Variable definitions

| Variable | Value |
|----------|-------|
| port *<portlist>* | Ports to which to apply the ADAC configuration. |
| enable | Enables ADAC on the port or ports listed. |

| Variable | Value |
|---|---|
| tagged-frames-pvid *<1-4094>* \| *no-change* | Sets Tagged-Frames PVID on the port or ports listed. Use *no-change* to keep the current setting. |
| tagged-frames-tagging *tagAll* \| *tagPvidOnly* \| *untagPvidOnly* \| *no-change* | Sets Tagged-Frames Tagging to<br><br>• tagAll<br><br>• tagPvidOnly<br><br>• untagPvidOnly<br><br>Use *no-change* to keep the current setting. |

# Resetting ADAC per port settings to default

Use the following procedure to set the per port ADAC defaults for the specified ports.

## Procedure steps

To reset settings, use the following command from Interface Configuration mode.

```
default adac [port <portlist>] [enable] [tagged-frames-pvid]
[tagged-frames-tagging]
```

## Variable definitions

| Variable | Value |
|---|---|
| port *<portlist>* | Ports on which to apply the ADAC defaults. |
| enable | Restores the port to the default ADAC state: **Disabled**. |
| tagged-frames-pvid | Restores Tagged-Frames PVID on the port or ports to the default setting: **no-change**. |
| tagged-frames-tagging | Restores Tagged-Frames Tagging to default setting: **Untag PVID Only**. |

# Configuring autodetection method

Use the following procedure to set the auto-detection method, by MAC address or using LLDP (IEEE 802.1ab).

## Procedure steps

To configure the autodetection method, use the following command from Interface Configuration mode.

```
[no] adac detection [port <port-list>] {[mac][lldp]}
```

## Variable definitions

| Variable | Value |
|---|---|
| port <portlist> | Specifies the port or ports for which to set the detection mode. |
| mac | Enables MAC-based detection. The default setting is MAC enabled. |
| lldp | Enables LLDP (802.1ab) detection. The default setting is LLDP enabled. |

# Resetting autodetection method to default

Use the following procedure to reset the auto-detection method to its defaults. The default is to have both MAC and LLDP enabled.

## Procedure steps

To reset the autodetection method to default, use the following command from Interface Configuration mode.

```
default adac detection [port <port-list>] {[mac][lldp]}
```

## Variable definitions

| Variable | Value |
|---|---|
| port <portlist> | Specifies the port or ports to be returned to the default; both MAC and LLDP are enabled. |
| mac | MAC is enabled by default. |

| Variable | Value |
|---|---|
| lldp | LLDP is enabled by default. |

# Configuring autodetection for ports

Use the following procedure to enable Auto-Detection on specified ports.

## Procedure steps

To configure autodetection, use the following command from Interface Configuration mode.

```
[no] adac port <port-list> enable
```

# Restoring ADAC port settings

Use the following procedure to restore the default ADAC setting (disabled) for the specified ports.

## Procedure steps

To restore ADAC port settings, use the following command from Global Configuration mode.

```
default adac [port <port-list>] enable
```

# Adding a range to ADAC MAC address table

Use the following procedure to add a specified range to the table of MAC addresses recognized as Avaya IP Phones by the Auto-Detection process.

## Procedure steps

To add a range, use the following command from Global Configuration mode.

```
[no] adac mac-range-table low-end <MACaddress> high-end
<MACaddress>
```

Use the **no** form of the command to delete a range.

**Note:**

If the low-end and high-end MAC address values are not provided, the switch deletes all existing MAC address ranges from the switch.

# Restoring ADAC MAC range table

Use the following procedure to restore all supported MAC address ranges on the switch to their default values.

## Procedure steps

To restore the ADAC MAC range table, use the following command in Global Configuration mode.

```
default adac mac-range-table
```

# Displaying global ADAC settings

Use the following procedure to display the global ADAC settings for the device.

## Procedure steps

To display global ADAC settings, use the following command from Privileged EXEC mode.

```
show adac
```

# Displaying ADAC port settings

Use the following procedure to display the ADAC settings for a particular port.

## Procedure steps

To display ADAC port settings, use the following command from Privileged EXEC mode.

```
show adac interface <interface-type> <slot/port>
```

# Displaying ADAC MAC ranges

Use the following procedure to display the ADAC MAC ranges configured on the switch.

## Procedure steps

To display ADAC MAC ranges, use the following command from Privileged EXEC mode.

```
show adac mac-range-table
```

# Displaying configured detection mechanism

Use the following procedure to display the detection mechanism configured per port.

## Procedure steps

To display the detection mechanism, use the following command from Privileged EXEC mode.

```
show adac detection interface [<interface-type>][<interface-id>]
```

# ADAC UFA configuration example

Figure 34: ADAC UFA configuration example on page 211 shows an example of ADAC configured in Untagged-Frames-Advanced (UFA) op-mode. (Call-server-port is used in this example, because the server is directly connected to the 5000 series switch.)
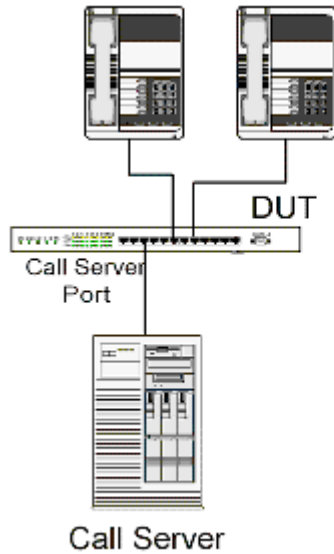
**Figure 34: ADAC UFA configuration example**

Auto-Configuration (AC) is applied for call-server-port and telephony ports. On telephony ports, AC is applied only when Avaya IP Phones are detected. (Auto-detection is based on MAC Address.) VLAN configuration is made according to the selected op-mode (UFA):

• Telephony port:

- - Membership = remove from all other VLANs, and add to Voice-VLAN (since there is no reason for the port to be member of more than the Voice VLAN)

- Tagging = Untagged

- PVID = Voice-VLAN

• Call Server port:

- Membership = add to Voice-VLAN

- Tagging = Untagged

- PVID = Voice-VLAN

To configure the example shown in Figure 34: ADAC UFA configuration example on page 211, you must perform the following tasks:

1. Configure the call-server port.

2. Configure voice-VLAN.

3. Configure Untagged-Frames-Advanced (UFA) op-mode.

4. Enable ADAC on all ports to which IP phones connect.

5. Configure IP phones to send untagged traffic.

Configuring ADAC using the ACLI

6. Enable the LLDP-MED Capabilities TLV on the ports used by IP phones.

7. Enable the LLDP-MED Network Policy TLV for transmission.

   This prevents configuration mismatches by enabling the IP Phone to obtain its policy settings directly from the switch.

# ADAC configuration commands

The following section describes the detailed ACLI commands required to carry out the configuration shown in Figure 34: ADAC UFA configuration example on page 211.

```
(config)#adac  call-server-port  7
(config)#adac  voice-vlan  2
(config)#adac  enable  op-mode  untagged-frames-advanced
(config)#interface  fastEthernet  all
(config)#interface  fastEthernet  16,24 enable
(config-if)#lldp tx-tlv port 16,24 med med-capabilities
(config-if)#lldp tx-tlv port 16,24 med network-policy
```

# Verifying new ADAC settings

The following section includes commands used to view ADAC configuration settings and the expected responses for each.

## Auto configuration settings

```
(config)#show adac interface 7,16,24


Port  Auto-Detection  Auto-Configuration
----  --------------  ------------------
7       Disabled         Applied
16      Enabled          Applied
24      Enabled          Applied
```

## VLAN settings

```
(config)#show vlan


Id  Name  Type      Protocol        User PID Active IVL/SVL Mgmt ---
-------------------- -------- ---------------- -------- ------
1   VLAN #1            Port      None      0x0000  Yes    IVL     Yes       Port
Members: 1-15,17-23
2   Voice_VLAN         Port      None      0x0000  Yes    IVL     No        Port
Members: 7,16,24
```

212    Configuration — VLANs, Spanning Tree, and Link Aggregation                    September 2013
Comments? infodev@avaya.com

```
(config)#show vlan interface info 7,16,24
```

```
Filter     Filter
Untagged Unregistered Port  Frames  Frames  PVID PRI    Tagging    Name ---- --------
------------ ---- --- ------------ ----------------
7    No       Yes       2    0   UntagAll      Port 7
16   No       Yes       2    0   UntagAll      Port 16
24   No       Yes       2    0   UntagAll      Port 24
```

## ADAC settings

```
(config)#show running-config
```

```
 !...
! *** ADAC *** Note information in this section.
!
no adac enable
no adac mac-range-table
interface FastEthernet ALL
adac port 24 enable
no adac port 1-23 enable
exit
adac mac-range-table low-end 00-0A-E4-01-10-20 high-end
00-0A-E4-01-23-A7
adac mac-range-table low-end 00-0A-E4-01-70-EC high-end
00-0A-E4-01-84-73
adac mac-range-table low-end 00-0A-E4-01-A1-C8 high-end
00-0A-E4-01-AD-7F
adac mac-range-table low-end 00-0A-E4-01-DA-4E high-end
00-0A-E4-01-ED-D5
adac mac-range-table low-end 00-0A-E4-02-1E-D4 high-end
00-0A-E4-02-32-5B
adac mac-range-table low-end 00-0A-E4-02-5D-22 high-end
00-0A-E4-02-70-A9
adac mac-range-table low-end 00-0A-E4-02-D8-AE high-end
00-0A-E4-02-FF-BD
adac mac-range-table low-end 00-0A-E4-03-87-E4 high-end
00-0A-E4-03-89-0F
adac mac-range-table low-end 00-0A-E4-03-90-E0 high-end
00-0A-E4-03-B7-EF
adac mac-range-table low-end 00-0A-E4-04-1A-56 high-end
00-0A-E4-04-41-65
adac mac-range-table low-end 00-0A-E4-04-80-E8 high-end
00-0A-E4-04-A7-F7
adac mac-range-table low-end 00-0A-E4-04-D2-FC high-end
00-0A-E4-05-48-2B
adac mac-range-table low-end 00-0A-E4-05-B7-DF high-end
00-0A-E4-06-05-FE
adac mac-range-table low-end 00-0A-E4-06-55-EC high-end
00-0A-E4-07-19-3B
adac mac-range-table low-end 00-0A-E4-08-0A-02 high-end
```

```
00-0A-E4-08-7F-31
adac mac-range-table low-end 00-0A-E4-08-B2-89 high-end
00-0A-E4-09-75-D8
adac mac-range-table low-end 00-0A-E4-09-BB-9D high-end
00-0A-E4-09-CF-24
adac mac-range-table low-end 00-0A-E4-09-FC-2B high-end
00-0A-E4-0A-71-5A
adac mac-range-table low-end 00-0A-E4-0A-9D-DA high-end
00-0A-E4-0B-61-29
adac mac-range-table low-end 00-0A-E4-0B-BB-FC high-end
00-0A-E4-0B-BC-0F
adac mac-range-table low-end 00-0A-E4-0B-D9-BE high-end
00-0A-E4-0C-9D-0D
adac traps enable
adac voice-vlan 2
adac call-server-port 7
no adac uplink-port
adac enable
```

# Chapter 13: Configuring VLANs using Enterprise Device Manager

The following sections detail how to create and manage a VLAN using the Enterprise Device Manager (EDM). VLAN creation and management is performed in the VLANs dialog box.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the VLAN dialog box:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **VLANs**.

This section contains information about the following topics:

# VLAN Basic configuration

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the VLAN Basic tab:

### Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **VLANs**.
3. Select the **Basic** tab.

### Variable definitions

The following table outlines the parameters of the **Basic** tab.

**Table 19: VLAN Basic tab parameters**

| Variable | Value |
|---|---|
| Id | The VLAN ID for the VLAN. |
| Name | Name of the VLAN. |
| Ifindex | Displays port numbers. |
| Color | An administratively assigned color code for the VLAN. The value of this object is used by the VLAN Manager GUI tool to select a color when it draws this VLAN on the screen. |
| Type | Indicates the type of VLAN: byPort or byProtocolId. |
| PortMembers | Ports that are members of the VLAN. |
| ActiveMembers | Set of ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. |
| StgId | Identifies the spanning tree group to which the VLAN belongs. This field is only available when the switch is running in Avaya STPG mode. |
| MstpInstance | This field is only available when the switch is running in MSTP mode. |
| ProtocolId | Protocol for protocol-based VLANs. This value is taken from the Assigned Numbers RFC. For port-based VLANs, None is the displayed value. |
| UserDefinedPid | When rcVlanProtocolId is set to usrDefined(15) in a protocol-based VLAN, this field represents the 16-bit user-defined protocol identifier. |
| Encap | The type of encapsulation. Options are ethernet2 and llc. |
| MacAddress | The unique hardware address of the device. |
| Routing | Specifies whether routing is enabled (true) or disabled (false) on the VLAN. |

This section contains information about the following:

# Creating a VLAN

The new VLAN is created and displayed in the VLANs Basic tab. To add or remove ports from the VLAN, the VLAN must be modified.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to create a VLAN:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **VLANs**.
3. Select the **Basic** tab.
4. Click **Insert**.

   The Insert Basic dialog box appears with the Type field set to byPort.

5. Enter the identifier for the VLAN in the **Id** field. This value must be a unique number between 2 and 4094.
6. Optionally, enter a name for the VLAN in the **Name** field.
7. Optionally, assign a color identifier to the VLAN in the **Color** field.
8. Enter the value of the Spanning Tree Group to which the VLAN will belong in the **StgId** field.
9. When in Avaya STPG mode, use the **StgId** menu to choose the spanning tree group to which the VLAN is to belong. When in MSTP mode, use the **MstpInstance** list to select the CIST or MSTI instance to which the VLAN is to belong.
10. Select the type of VLAN in the **Type** field.

    a. If the VLAN is to be port-based, select the **byPort** option button.

    b. If the VLAN is to be protocol-based, select the **byProtocolId** option button. This selection enables the **ProtocolId** field. From this field select the protocol on which this VLAN will be based. If it is to be based on a

user-defined protocol, select the **usrDefined** option button and enter the custom PID in the **UserDefinedPid** field.

11. Click **Insert**.

# Modifying a VLAN

After a VLAN is created, four types of information can be modified without the need to recreate the VLAN:

1. VLAN Name
2. Color Identifier
3. Member Ports
4. Routing status

To change the VLAN name, color identifier, or routing status, click in the appropriate fields in the VLANs Basic tab and then click **Apply** .

**Prerequisites**

• Open one of the supported Web browsers.

• Access the switch.

• Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to change VLAN member ports:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VALN tree, double-click **VLANs**.
3. Select the **Basic** tab.
4. In the row that represents the VLAN that is to be modified, double-click in the **PortMembers** field.

   The Port Members screen appears.
5. Click the buttons that correspond to the ports that are to be added or deleted from the VLAN. Click **All** to select all switch ports.
6. Click **OK**.
7. Click **Apply**.

# Deleting VLANs

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete a VLAN:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **VLANs**.
3. Select the **Basic** tab.
4. Select the VLAN to be deleted.
5. Click **Delete**.

   The EDM deletes the selected VLAN.

# Clearing DHCP statistics counters on a VLAN

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to clear DHCP statistics counters:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **VLANs**.
3. Select the **Basic** tab.
4. Highlight the VLAN for which DHCP statistics counters are to be cleared.
5. Click **IP**.

   The IP VLAN screen appears.
6. Select the **DCHP** tab.
7. From the **DHCP** tab, select **clear** in the **ClearCounters** field and press **Apply**.

**Variable definitions**

The following table outlines the parameters of the **DHCP Graph** button.

**Table 20: DHCP Graph button parameters**

| Variable | Value |
|---|---|
| NumRequests | The total number of DHCP requests seen on this interface. |
| NumReplies | The total number of DHCP replies seen on this interface. |

# Configuring VLAN Snoop

Use the Snoop tab on the VLANs dialog box to enable or disable IGMP snooping on a switch.

For information on this tab and on the IGMP snooping feature, refer to *Avaya Ethernet Routing Switch 5000 Series Configuration — IP Routing Protocols*, NN47200-503.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the VLAN Snoop tab:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **VLANs**.
3. Select the **Snoop** tab.

**Variable definitions**

The following table outlines the parameters of the **Snoop** tab.

**Table 21: VLAN Snoop tab parameters**

| Variable | Value |
|---|---|
| Id | Specifies the ID of the VLAN. |
| Name | Specifies the name of the VLAN. |
| ReportPorxyEnable | A flag to note whether IGMP Report Proxy is enabled on this VLAN. |
| Enable | A flag to note whether IGMP Snooping is enabled on this VLAN. |

| Variable | Value |
|---|---|
| Robustness | Allows tuning for the expected packet loss on a subnet. If a subnet is expected to be *lossy*, the Robustness variable may be increased. IGMP is robust to (Robustness - 1) packet losses. |
| QueryInterval | Specifies the interval (in seconds) between IGMP Host-Query packets transmitted on this interface. |
| MRouterPorts | Specifies the set of ports in this VLAN that provide connectivity to an IP Multicast router. |
| Ver1MRouterPorts | Specifies the version 1 ports in this VLAN that provide connectivity to an IP Multicast router. |
| Ver2RouterPorts | Specifies the version 2 ports in this VLAN that provide connectivity to an IP Multicast router. |
| ActiveMRouterPorts | Specifies the active ports. |
| ActiveQuerier | Specifies the IP address of multicast querier router |
| QuerierPort | Specifies the port on which the multicast querier router was heard. |
| MRouterExpiration | Specifies the multicast querier router aging time out |

# Configuring VLAN Ports

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the VLAN Ports tab:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **VLANs**.
3. Select the **Ports** tab.
4. Click **Apply** after making any changes.

## Variable definitions

The following table outlines the parameters of the **Ports** tab.

**Table 22: VLAN Ports tab parameters**

| Variable | Value |
|---|---|
| VlanIds | The VLANIDs of which this port is a member. |
| DiscardUntaggedFrames | This field only applies to trunk ports. It acts as a flag used to determine how to process untagged frames received on this port. When the flag is set, the frames are discarded by the forwarding process. When the flag is reset, the frames are assigned to the VLAN specified by rcVlanPortDefaultVlanId. |
| FilterUnregisteredFrames | This field only applies to access ports. It acts as a flag used to determine how to process unregistered frames received on this port. When the flag is set, the frames are discarded by the forwarding process. When the flag is reset, the frames are processed normally. |
| DefaultVlanId | The VLAN ID assigned to untagged frames received on a trunk port. |
| userPriority | Set the port priority value from the list as a value between 0 and 7. |
| Tagging | Indicates the type of VLAN port. A trunk port can be a member of more than one VLAN. An access port can be a member of only VLAN, if no membership conflict exists.<br>There are four types of VLAN port:<br><br>• tagAll(trunk)<br><br>• untagAll(access)<br><br>• tagPvidOnly<br><br>• untagPvidOnly |

# VLAN NSNA Configuration

This section contains information about VLAN NSNA Configuration.

## Navigation

This section contains information about the following:

# Viewing VLAN NSNA

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the NSNA tab:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **VLANs**.
3. Select the **NSNA** tab.

**Variable definitions**

The following table outlines the parameters of the **NSNA** tab.

**Table 23: VLAN NSNA tab parameters**

| Variable | Value |
|---|---|
| Id | Specifies the VLAN identification number. |
| NsnaColor | Specifies the NSNA VLAN color. |
| FilterSetName | Specifies the filter set name.<br><br>**Note:**<br>NsnaColor field must be only red, yellow, or green. |
| YellowSubnetType | Specifies the Ethernet type for the Yeloow VLAN subnet.<br><br>**Note:**<br>NsnaColor field must be set to yellow. |
| YellowSubnet | Specifies the Yellow VLAN subnet.<br><br>**Note:**<br>NsnaColor field must be set to yellow. |
| YellowSubnetMask | Specifies the Yellow VLAN subnet mask.<br><br>**Note:**<br>NsnaColor field must be set to yellow.. |

# Configuring NSNA per VLAN

> **Important:**
> VLANs that you plan to configure as NSNA VLANs must be empty (that is, they have no port members assigned). NSNA VLANs cannot be associated with non-NSNA ports; therefore you cannot assign non-NSNA ports manually to enabled NSNA VLANs.
>
> Dumb and static devices that cannot authenticate through tunnel guard can be connected to NSNA dynamic ports. To ensure network access for these devices, add the MAC addresses to the SNAS MAC database.

For more information about NSNA, refer to *Avaya Ethernet Routing Switch 5000 Series Configuration - Security*, NN47200-501.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to configure NSNA per VLAN:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **VLANs**.
3. Select the **NSNA** tab.
4. Select a VLAN to modify.
5. Double click the **NsnaColor** field. A menu appears.
6. Select one of the following options from the menu:
   - none
   - red
   - green
   - yellow
   - voip

   > **Important:**
   > Although each switch can have multiple Yellow, Green, and VoIP VLANs, each switch must have only one Red VLAN.

7. In the other columns, enter parameters compatible with the NsnaColor selection.
8. Click **Apply**.

# Deleting an NSNA VLAN

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.
- NSNA must be globally disabled before you can delete an NSNA VLAN.

Use the following procedure to delete an NSNA VLAN:

**Procedure steps**

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Security**.
3. From the Security tree, double-click **NSNA**.
4. Select the **Globals** tab.
5. Clear the **Enabled** check box.
6. From the navigation tree, double-click **VLAN**.
7. From the VLAN tree, double click **VLANs**.
8. Select the **NSNA** tab.
9. Select the VLAN to delete and double click the **NsnaColor** field.
10. From the list, select **none**.
11. Click **Apply**.
12. Select the **Basic** tab.
13. Select the VLAN to delete (the VLAN for which the NsnaColor was changed to none).
14. Click **Delete**.

# Filtering an NSNA VLAN

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to filter an NSNA VLAN:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **VLANs**.
3. Select the **NSNA** tab.
4. Click **Filter**. The VLAN, NSNA - Filter dialog opens.
5. Set the filter parameters.
6. Click **Filter**.

## Variable definitions

The following table outlines the parameters of the **MAC Multicast Filter Table** tab.

**Table 24: MAC Multicast Filter Table tab parameters**

| Variable | Value |
|---|---|
| AllowedAddressVlanId | Specifies the allowed address of the VLAN ID. |
| AllowedAddressMacAddr | Specifies the allowed address for the MAC address. |

# Enabling AutoPVID

A Port VLAN ID can be automatically assigned to any port by enabling the AutoPVID functionality on the switch.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to enable AutoPVID:

**Procedure steps**

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Chassis**.
4. Select the **System** tab.
5. In the **AutoPVID** field, select **enabled**.
6. Click **Apply**.

# MAC address table maintenance using the Device Manager

You can flush the MAC address table using Enterprise Device Manager. For more information about the MAC address table, see Managing the MAC address forwarding database table on page 150.

## Flushing the MAC address table

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to flush dynamically learned MAC addresses from the MAC address forwarding table:

**Procedure steps**

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Bridge**.
4. Select the **MAC Flush** tab.
5. Click **FlushMacAddrTableAll** or type the MAC address, VLAN, trunk, port, or portlist in the corresponding box.
6. Click **Apply**.

## Variable definitions

**Table 25: MAC Flush tab parameters**

| Variable | Value |
|---|---|
| FlushMacAddrTableAll | Flushes all MAC addresses from MAC address table. |
| FlushMacAddrTableByPortlist | Flushes the MAC addresses for port(s) specified from the MAC address table. |
| FlushMacAddrTableByVlan | Flushes the MAC addresses for the VLAN specified from the MAC address table. |

| Variable | Value |
|---|---|
| FlushMacAddrTableByTrunk | Flushes the MAC addresses for the Multi-Link Trunk specified from the MAC address table. |
| FlushMacAddrTableByAddress | Flushes the specified MAC addresses from MAC address table. |

# Selecting VLAN configuration control using EDM

Use the following procedure to select configuration control for a VLAN.

## Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **VLANs**.
3. In the work area, click the **Settings** tab.
4. In the **ManagementVlanID** box, type a value.
5. In the **VlanConfigControl** section, click a button.
6. On the toolbar, click **Apply**.

**Variable Definitions**

Use the data in this table to select VLAN configuration control.

| Variable | Value |
|---|---|
| ManagementVlanId | Specifies the identifier of the management VLAN. Values range from 1 to 4094. |
| VlanConfigControl | Specifies the VLAN configuration control options. The available options are:<br>• automatic—This selection automatically adds an untagged port to a new VLAN and automatically removes it from any previous VLAN membership. The PVID of the port is automatically changed to the VID of the VLAN it joins. Since the port is first added to the new VLAN and then removed from any previous membership, the Spanning Tree Group participation of the port is not disabled as long as the VLANs involved are in the same Spanning Tree Group.<br>• autopvid—This selection functions in the same manner as previous AutoPVID functionality. When an untagged port is added to a new VLAN, the port is added to the new VLAN and the PVID assigned to the new VID without removing it from |

| Variable | Value |
|---|---|
| | any previous VLAN memberships. Using this option, an untagged port can have membership in multiple VLANs.<br>• flexible—This selection functions in a similar manner to disabling AutoPVID functionality. When this option is used, an untagged port can belong to an unlimited number of VLANs. Any new additions of an untagged port to a new VLAN does not change the PVID of that port.<br>• strict—The factory default, this selection restricts the addition of an untagged port to a VLAN if it is already a member of another VLAN. To add an untagged port to a new VLAN, the switch administrator must remove the port from all other VLANs of which it is a member before adding it to the new VLAN. The PVID of the port is changed to the new VID to which it was added. |

# Chapter 14: Configuring Spanning Tree using Enterprise Device Manager

The following sections detail how to create and manage an STP using the Enterprise Device Manager (EDM). STP creation and management is performed in the Spanning Tree folder.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Spanning Tree folder:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.

To configure the Spanning Tree using Enterprise Device Manager, refer to the following:

## Spanning Tree Globals dialog box

You can use the Enterprise Device Manager (EDM) screens detailed in this section to create and manage Spanning Tree Groups.

> **Note:**
> The STG dialog boxes and tabs described in this section are accessible only when the STP mode is set to Avaya STPG.

This section contains information about the Spanning Tree Globals tab.

**Prerequisites**

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Spanning Tree Globals dialog box:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.

2. From the VLAN tree, double-click **Spanning Tree**.

3. From the Spanning Tree folder, double-click **Globals**.

This section contains information about the following topics:

-

-

# Setting the STP mode

**Prerequisites**

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to set the STP operational mode:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.

2. From the VLAN tree, double-click **Spanning Tree**.

3. From the Spanning Tree folder, double-click **Globals**.

4. In the **SpanningTreeAdminMode** field, select the STP mode. The available modes are:

   - avayaStpg

   - rstp

   - mstp

5. Click **Apply**.

   A warning message appears reminding you that you must reset the switch for the change to take effect.

6. Click **Yes**.

7. Click **Close**.

8. To reset the switch, choose **Edit > Chassis**.

9. From the System tab, choose the **reboot** option and click **Apply**.

## Variable definitions

The following table outlines the parameters of the **Globals** tab.

**Table 26: Spanning Tree Globals tab parameters**

| Variable | Value |
|---|---|
| SpanningTreeAdminMode | Indicates the desired spanning-tree mode of the system. The specific values are as follows:<br><br>• avayaStpg(1)—The older proprietary mode, which supports multiple spanning tree groups.<br><br>• rstp(3)—IEEE 802.1w mode<br><br>• mstp(4)—IEEE 802.1s mode |
| SpanniingTreeOperMode | This object indicates the current spanning-tree mode of the system. The specific values are as follows:<br><br>• avayaStpg(1)—The older proprietary mode, which supports multiple spanning tree groups.<br><br>• rstp(3)—IEEE 802.1w mode<br><br>• mstp(4)—IEEE 802.1s mode |

# Configuring STP BPDU filtering for specific ports using EDM

You can configure STP BPDU filtering in either STG, RSTP, or MSTP operational mode.

STP BPDU-Filtering is not supported on MLT ports.

Use this procedure to configure STP BPDU filtering for one or more ports.

1. On the **Device Physical View** select a port, or click and drag to select a group of ports.

2. Right-click the port or port group of ports.

3. From the drop-down menu, click **Edit**.

4. On the work area, click the **STP BPDU-Filtering** tab.

5. If you selected a group of ports on the Device Physical View, perform the following actions for each port in the list:

   • To select a port to edit, click the cell in the **rcPortIndex** column.

   • In the port row, double-click the cell in the **Admin Enabled** column.

- Click the arrow to reveal the list.
- Select a value from the list—**true** to enable STP BPDU filtering for the port, or **false** to disable STP BPDU filtering for the port.
- In the port row, double-click the cell in the **Timeout** column.
- Type a value in the dialog box.

6. If you selected a single port on the Device Physical View:

- Click the **AdminEnabled** checkbox.
- Enter a value in the **Timeout** box.

7. On the toolbar, click **Apply**.

## Variable definitions

The following table outlines the parameters of the **STP BPDU-Filtering** tab.

**Table 27: STP BPDU-Filtering tab parameters**

| Variable | Value |
|----------|-------|
| rcPortIndex | Indicates the switch and port number. |
| AdminEnabled | Enables and disables BPDU filtering on the port. |
| OperEnabled | Indicates the current operational status of BPDU filtering on the port: true (enabled) or false (disabled). |
| Timeout | When BPDU filtering is enabled, this parameter indicates the time, in 1/100 seconds, during which the port remains disabled after it receives a BPDU. The port timer is disabled if this value is set to 0. The default value is 12000 (120 seconds). |
| TimerCount | Displays the time remaining for the port to stay in the disabled state after receiving a BPDU. |

# Spanning Tree STG configuration

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

This section contains information about the following topics:

# Configuring STG Global properties

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to configure the STG global properties:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **STG**.
4. Select the **Globals** tab.
5. Select the STP path cost calculation mode:
   - ieee802dot1dCompatible
   - ieee802dot1tCompatible
6. Select the STP port mode:
   - normal
   - auto
7. Check the SpanningTreeAdminCompatibility box to enable 802.1d port learning.
8. Click **Apply**.

## Variable definitions

The following table outlines the parameters of the **Globals** tab.

**Table 28: STG Globals tab parameters**

| Variable | Value |
|----------|-------|
| SpanningTreePathCostCalculationMode | This object indicates the current spanning-tree path cost calculation mode. The value ieee802dot1dCompatible is valid only when the switch is running in Avaya STPG mode. |
| SpanningTreePortMode | This object sets the STG port membership mode for all Spanning Tree Groups on the switch. |
| SpanningTreeAdminCompatibility | This field Indicates whether the learning mode of a port stays in the Forwarding state or changes to the Disabled state when the port operation status goes down. If the box is checked, the port goes to the disabled state when down. |
| SpanningTreeOperCompatibility | This field indicates the operational compatibility mode for features controlled by the associated object. |

# Creating an STG

The new STG is displayed in the STG Configuration tab.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to create a Spanning Tree Group:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **STG**.
4. Click the **Configuration** tab.
5. Click **Insert**.

   The Insert Configuration dialog box appears.
6. In the fields provided, fill in the information for the new STG.
7. Click **Insert**.

# Variable definitions

The following table outlines the parameters of the **Configuration** tab.

**Table 29: STG Configuration tab parameters**

| Variable | Value |
| --- | --- |
| Id | Enter an integer between 1 and 8 that identifies the STG; 1 is the default STG. |
| BridgeAddress | Displays the MAC address used by this bridge; it is usually the smallest MAC address of all ports in the bridge. |
| NumPorts | Displays the number of ports controlled by this bridging entity. |
| ProtocolSpecification | Displays the version of spanning tree that is running. |
| Priority | Enter the first two octets of the 8-octet bridge ID; the range is 0 to 65 535. |
| BridgeMaxAge | Enter the maximum time you want to allow before the specified STG times out, in seconds; the range is 600 to 4 000. |
| BridgeHelloTime | Enter the maximum time between hellos, in seconds; the range is 100 to 1 000. |
| BridgeForwardDelay | Enter the maximum delay in forwarding, in seconds; the range is 400 to 3 000. |
| EnableStp | Enables or disables the spanning tree group. |
| TaggedBpduAddress | The address for the tagged BPDU. |
| TaggedBpduVlanId | Enter the VLAN ID for tagged BPDUs. |

# Adding a VLAN to an STG

When using Enterprise Device Manager, a VLAN can only be added to an STG at the time the VLAN is created.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to add a VLAN to an STG:

**Procedure steps**

1. If it does not already exist, create the STG to which you want to add the VLAN.

See [Creating an STG](#) on page 236 for more information about creating STGs.

2. Create the VLAN, making sure to select the desired **Id** on the Insert VLAN screen.

3. Open the VLAN dialog box and view the **Basic** tab to confirm that the **Id** field for the VLAN is the correct STG.

# Moving a VLAN between STGs

You cannot use Enterprise Device Manager to move VLANs between STGs on the Avaya Ethernet Routing Switch 5000 Series. Instead, delete the VLAN to be moved and add a replacement VLAN in the STG to which you want to move the VLAN.

# Deleting an STG

### Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete an STG:

### Procedure steps

1. From the navigation tree, double-click **VLAN**.

2. From the VLAN tree, double-click **Spanning Tree**.

3. From the Spanning Tree folder, double-click **STG**.

4. On the **Configuration** tab, select the STGs to be deleted.

5. Click **Delete**.

# Displaying STG Status

### Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to display the status of an STG:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **STG**.
4. Select the **Status** tab.

   The status of all current STGs is displayed.

# Variable definitions

The following table outlines the parameters of the **Status** tab.

**Table 30: STG Status tab parameters**

| Variable | Value |
|----------|-------|
| Id | Displays the STG ID. |
| BridgeAddress | Displays the MAC address used by this bridge. |
| NumPorts | Displays the number of ports controlled by this bridging entity. |
| ProtocolSpecification | Displays the version of spanning tree that is running. |
| TimeSinceTopology Change | Displays the time, in hundredths of seconds, since the last topology change. |
| TopChanges | Displays the number of topology changes since the switch was reset. |
| DesignatedRoot | Displays the MAC address of the STP designated root. |
| RootCost | Displays the cost of the path to the root. |
| RootPort | Displays the port number of the port with the lowest-cost path from this bridge to the root bridge. |
| MaxAge | Displays the maximum age, in hundredths of a second, of STP information learned from any port in the network before the information is discarded. |
| HelloTime | Displays the amount of time, in hundredths of seconds, between Hello messages. |
| HoldTime | Displays the interval, in hundredths of seconds, during which no more than two Hello messages can be transmitted. |
| ForwardDelay | Displays the interval, in hundredths of seconds, during which the switch stays in Listening or Learning mode, before moving to Forwarding mode. This value is also used to age dynamic entries in the Forwarding Database. |

# Displaying STG ports

### Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to display the STG port status:

### Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **STG**.
4. Select the **Ports** tab.
5. View the information and, if desired, change the information in the Ports tab by entering updated information and by using the menus provided.
6. Click **Apply**.

## Variable definitions

The following table outlines the parameters of the **Ports** tab.

**Table 31: STG Ports tab parameters**

| Variable | Value |
|---|---|
| <Untitled Column> | Displays the unit and port number. |
| StgId | Displays the STG ID number. |
| Priority | Specifies the port priority |
| State | Displays the STP state of the port: Disabled, Blocking, Listening, Learning, Forwarding. |
| EnableStp | Enables or disables STP on the port: True is enabled, and False is disabled. |
| FastStart | Enables or disables Fast Start STP on the port: True is enabled, and False is disabled. |
| AdminPathCost | Sets the PathCost value. The field displays 0 if no user-configured value exists. |
| PathCost | Displays the contribution of this port to the cost path of the spanning tree root. |

| Variable | Value |
|---|---|
| DesignatedRoot | Displays the MAC address of the STP designated root. |
| DesignatedCost | Displays the path cost of the designated port of the segment connected to this port. |
| DesignatedBridge | Displays the MAC address of the designated bridge this port considers the designated bridge for this segment. |
| DesignatedPort | Displays the port ID of the designated bridge for this port segment. |
| ForwardTransitions | Displays the number of times the port transitioned from STP Learning to Forwarding state. |

# Configuring STG port properties

The STG tab displays the spanning tree parameters for a port.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to view the STG tab:

**Procedure steps**

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Ports**.
4. Select the **STG** tab.

# Variable definitions

The following table outlines the parameters of the **Ports** tab.

**Table 32: Chassis Ports tab parameters**

| Variable | Value |
|---|---|
| StgId | The spanning tree group ID to which the VLAN belongs. |
| Priority | The value of the priority field that is contained in the first (in network byte order) octet of the (2-octet long) Port ID. The other octet of the Port ID is derived from the value of dot1dStpPort. |

| Variable | Value |
|---|---|
| State | The current port state as defined by application of the Spanning Tree Protocol. This state controls the action a port takes when it receives a frame. If the bridge detects a port that is malfunctioning, it places that port into the broken state. For ports that are disabled (see EnableStp), this object has a value of Disabled. |
| EnableStp | Select True or False to enable or disable STP. |
| FastStart | Select True or False to enable or disable FastStart. |
| AdminPathCost | The administrative value of the PathCost. This is the value that has been configured by the user, or 0 if no user-configured value exists. If you specify the path cost in the PathCost field, the value in this field is modified as well. |
| PathCost | The contribution of this port to the cost of paths toward the spanning tree root, which includes this port. The IEEE 802.1D-1990 standard recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN. |
| DesignatedRoot | The unique Bridge Identifier of the bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached. |
| DesignatedCost | The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs. |
| DesignatedBridge | The Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port segment. |
| DesignatedPort | The Port Identifier of the port on the Designated Bridge for this port segment. |
| ForwardTransitions | The number of times this port has transitioned from the Learning state to the Forwarding state. |

# Spanning Tree RSTP dialog box

The Rapid Spanning Tree protocol (RSTP or IEEE 802.1w) reduces the recovery time after a network breakdown. It also maintains a backward compatibility with the IEEE 802.1d which was the Spanning Tree implementation prior to RSTP. In certain configurations, the recovery time of RSTP can be reduced to less than 1 second.

RSTP also reduces the amount of flooding in the network by enhancing the way the Topology Change Notification (TCN) packet is generated.

**Note:**

The RSTP dialog boxes and tabs described in this section are accessible only when the STP mode is set to RSTP.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to view the RSTP dialog box:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **RSTP**.

This section contains information on the following topics:

- Viewing RSTP Globally on page 243
- RSTP Ports tab on page 245
- Viewing the RSTP Status on page 247
- Graphing RSTP Port Statistics on page 248

# Viewing RSTP Globally

The Globals tab in the RSTP dialog box provides general information about RSTP when RSTP is the active mode.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to view the RSTP Globals tab:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **RSTP**.
4. Select the **Globals** tab.

# Variable definitions

The following table outlines the parameters of the **Globals** tab.

**Table 33: RSTP Globals tab parameters**

| Variable | Value |
|---|---|
| PathCostDefault | Sets the version of the Spanning Tree default Path Costs that the Bridge uses.<br>The value of 16-bit uses the 16-bit default Path Costs from IEEE Std. 802.1D-1998.<br>A value of 32-bit uses the 32-bit default Path Costs from IEEE Std. 802.1t. |
| TXHoldCount | The value used by the Port Transmit state machine to limit the maximum transmission rate. The value can range from 1 to 10. |
| Version | The version of the Spanning Tree Protocol the bridge is currently running:<br>• stpCompatible: indicates that the bridge uses the Spanning Tree Protocol specified in IEEE 802.1D.<br>• rstp: indicates that the bridge uses the Rapid Spanning Tree Protocol specified in IEEE 802.1w. |
| Priority | The value of the writable portion of the Bridge Identifier comprising the first two octets. The values that are set for Priority must be in steps of 4096. |
| BridgeMaxAge | The value in 1/100 seconds that all bridges use for MaxAge when this bridge acts as the root. The value must be a multiple of 100. The range is 600 to 4000. |
| BridgeHelloTime | The value in 1/100 seconds that all bridges use for HelloTime when this bridge acts as the root. The value must be a multiple of 100. The range is 100 to 1000. |
| BridgeForward Delay | The value in 1/100 seconds that all bridges use for ForwardDelay when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of BridgeMaxAge. The value must be a multiple of 100. The range is 400 to 3000. |
| DesignatedRoot | The unique identifier of the Bridge recorded as the Root in the Configuration BPDUs that are transmitted by the Designated Bridge for the segment to which the port is attached. Reference IEEE 802.1D-1990: Section 4.5.5.4. |
| RootCost | The cost of the path to the root as seen from this bridge. |

| Variable | Value |
|---|---|
| RootPort | The port number of the port that offers the lowest cost path from this bridge to the root bridge. |
| MaxAge | The maximum age of Spanning Tree Protocol information learned from the network on any port before being discarded. The maximum age is specified in units of hundredths of a second. This is the actual value that the bridge uses. |
| HelloTime | The amount of time required for transmission of the configuration BPDUs by the node on any port when it is the root of the spanning tree or trying to become the root. This is specified in units of hundredths of a second. This is the actual value that the bridge uses. |
| ForwardDelay | This time value, measured in units of hundredths of a second, controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state. |
| RstpUpCount | The number of times the RSTP Module has been enabled. A trap is generated on the occurrence of this event. |
| RstpDownCount | The number of times the RSTP Module has been disabled. A trap is generated on the occurrence of this event |
| NewRootIdCount | The number of times this Bridge has detected a Root Identifier change. A trap is generated on the occurrence of this event. |
| TimeSinceTopologyChange | The time (in hundredths of a second) since the TcWhile Timer for any port in this Bridge was non-zero for the Common Spanning Tree context. |
| TopChanges | The total number of topology changes detected by this bridge since the management entity was last reset or initialized. |

# RSTP Ports tab

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to view the RSTP Ports tab:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.

3. From the Spanning Tree folder, double-click **RSTP**.

4. Select the **Ports** tab.

## Variable definitions

The following table outlines the parameters of the **Ports** tab.

**Table 34: RSTP Ports tab parameters**

| Variable | Value |
|---|---|
| Port | The port number. |
| State | Used to identify a port state in this RSTP instance. The port state is cataloged as discarding, learning, and forwarding. |
| Priority | The value of the priority field which is contained in the first (in network byte order) octet of the (2 octet long) Port ID. |
| PathCost | The contribution of this port to the cost of paths towards the spanning tree root. |
| ProtocolMigration | Indicates the Protocol migration state of this port. Set this field to true to force the port to transmit RSTP BPDUs. Note: If this field is set to true and the port receives an 802.1d type BPDU, the port again begins transmitting 802.1d BPDUs. |
| AdminEdgePort | The administrative value of the Edge Port parameter. A value of true indicates that this port is assumed to be an edge-port and a value of false indicates that this port is assumed to be a nonedge-port. |
| OperEdgePort | The operational value of the Edge Port parameter. The object is initialized to false on reception of a BPDU. |
| AdminPointToPoint | The administrative point-to-point status of the LAN segment attached to this port.<br>• A value of forceTrue indicates that this port is always treated as being connected to a point-to-point link.<br>• A value of forceFalse indicates that this port is treated as having a shared media connection.<br>• A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means. |
| OperPointToPoint | The operational point-to-point status of the LAN segment attached to this port. This field indicates whether a port is considered to have a point-to-point connection. The value is determined by management or by auto-detection. |

| Variable | Value |
|---|---|
| Participating | This field specifies whether a port is participating in the 802.1w protocol. |
| DesignatedRoot | The bridge identifier of the old root of the Spanning Tree as determined by the Spanning Tree Protocol as executed by this node. |
| DesignatedCost | The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received BPDUs. |
| DesignatedBridge | The Bridge Identifier of the bridge which this port considers to be the Designated Bridge for this port segment. |
| DesignatedPort | The Port Identifier for the port segment which is on the Designated Bridge. |
| ForwardTransitions | The number of times this port has transitioned from the Learning state to the Forwarding state. |

# Viewing the RSTP Status

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to view the RSTP Status tab:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **RSTP**.
4. Select the **Status** tab.

# Variable definitions

The following table outlines the parameters of the **Status** tab.

**Table 35: RSTP Status tab parameters**

| Variable | Value |
|---|---|
| Port | The port number. |

| Variable | Value |
|---|---|
| Role | A role represents a functionality characteristic or capability of a resource to which policies are applied. |
| OperVersion | This indicates whether the Port is operationally in the RSTP mode or the STP-compatible mode; that is, whether the Port is transmitting RSTP BPDUs or Config/TCN BPDUs. |
| EffectivePortState | This is the effective Operational state of the port. This object is set to true only when the port is operationally up in the interface manager and when the force Port State and specified port state for this port is enabled. Otherwise, this object is set to false. |

# Graphing RSTP Port Statistics

You can use the RSTP Stats tab to graph RSTP port statistics.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the RSTP Stats tab for graphing:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **RSTP**.
4. Select the **Status** tab.
5. Select a port and click Graph to get the statistics for the RSTP Port.

   The RSTP Stats tab appears.

## Variable definitions

The following table outlines the parameters of the **RSTP Graph** dialog box.

**Table 36: RSTP Graph dialog box parameters**

| Variable | Value |
|---|---|
| RxRstBpduCount | The number of RST BPDUs that have been received on the port. |

| Variable | Value |
|---|---|
| RxConfigBpduCount | The number of Config BPDUs that have been received on the port. |
| RxTcnBpduCount | The number of TCN BPDUs that have been received on the port. |
| TxRstBpduCount | The number of RST BPDUs that have been transmitted by this port. |
| TxConfigBpduCount | The number of Config BPDUs that have been transmitted by this port. |
| TxTcnBpduCount | The number of TCN BPDUs that have been transmitted by this port. |
| InvalidRstBpduRxCount | The number of invalid RSTP BPDUs that have been received on this port. |
| InvalidConfigBpduRxCount | The number of invalid Configuration BPDUs that have been received on this port. |
| InvalidTcnBpduRxCount | The number of invalid TCN BPDUs that have been received on this port. |
| ProtocolMigrationCount | The number of times this Port has migrated from one STP protocol version to another. The relevant protocols are STP-COMPATIBLE and RSTP. |

# Spanning Tree MSTP dialog box

With the Multiple Spanning Tree Protocol (MSTP or IEEE 802.1s), you can configure multiple instances of RSTP on the same switch. Each MSTP instance can include one or more VLANs. The operation of the MSTP is similar to the current Avaya proprietary STG.

In the MSTP mode, the 5000 Series switches support a maximum of one Common and Internal Spanning Tree (CIST) and seven Multiple Spanning Tree Instances (MSTI).

Within the CIST, the Internal Spanning Tree component is used only by devices from the same region (for which a regional root is elected). The Common (External) Spanning Tree component of the CIST is used by devices from different regions or between devices with different STP modes.

> **Note:**
> The MSTP dialog boxes and tabs described in this section are accessible only when the STP mode is set to MSTP.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Spanning Tree MSTP dialog box:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **MSTP**.

This section contains information on the following topics:

# Viewing MSTP Globals

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to view the MSTP Globals tab:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **MSTP**.
4. Select the **Globals** tab.

# Variable definitions

The following table outlines the parameters of the **Globals** tab.

**Table 37: MSTP Globals tab parameters**

| Variable | Value |
|---|---|
| PathCostDefaultType | The version of the Spanning Tree default Path Costs that are used by this Bridge. A 16-bit value uses the 16-bit default path costs from IEEE Standard 802.1D-1998. A 32-bit value uses the 32-bit default path costs from IEEE Standard. 802.1t. |
| TxHoldCount | The value used by the Port Transmit state machine to limit the maximum transmission rate. |
| MaxHopCount | The Maximum Hop Count value in 1/100 seconds. The value must be a multiple of 100. The range is 100 to 4000. |
| NoOfInstancesSupported | Indicates the maximum number of spanning tree instances supported. |
| MstpUpCount | The number of times the MSTP Module is enabled. A trap is generated on the occurrence of this event. |
| MstpDownCount | The number of times the MSTP Module is disabled. A trap is generated on the occurrence of this event. |
| ForceProtocolVersion | Signifies the version of the Spanning Tree Protocol that the bridge is currently running.<br><br>• stpCompatible indicates that the bridge is using the Spanning Tree Protocol as specified in IEEE 802.1D.<br><br>• rstp indicates that the bridge is using the Rapid Spanning Tree Protocol as specified in IEEE 802.1w.<br><br>• mstp indicates that the bridge is running the Multiple Spanning Tree Protocol as specified in IEEE 802.1s. |
| BrgAddress | The bridge address is generated when events like protocol up or protocol down occurs. |
| Root | The bridge identifier of the root of the common spanning tree as determined by the Spanning Tree Protocol as executed by this node. This value is used as the CIST Root Identifier parameter in all Configuration BPDUs originated by this node. |
| RegionalRoot | The bridge identifier of the root of the Multiple Spanning Tree region as determined by the Spanning Tree Protocol as executed by this node. This value is used as the CIST Regional Root Identifier parameter in all Configuration Bridge PDUs originated by this node. |

| Variable | Value |
|---|---|
| RootCost | The cost of the path to the CIST Root as seen from this bridge. |
| RegionalRootCost | The cost of the path to the CIST Regional Root as seen from this bridge. |
| RootPort | The port number of the port which offers the lowest path cost from the bridge to the CIST Root Bridge |
| BridgePriority | The value of the writable portion of the Bridge Identifier comprising the first two octets. The values that are set for Bridge Priority must be in steps of 4096. |
| BridgeMaxAge | The value in hundredths of a second that all bridges use for MaxAge when this bridge acts as the root. The value must be a multiple of 100. The range is 600 to 4000. |
| BridgeForwardDelay | The value in hundredths of a second that all bridges use for ForwardDelay when this bridge acts as the root. IEEE 802.1D specifies that the range for this parameter is related to the value of BridgeMaxAge. The value must be a multiple of 100. The range is 400 to 3000. |
| HoldTime | This value determines the time interval during which no more than two Configuration BPDUs can be transmitted by this node. This value is measured in units of hundredths of a second. |
| MaxAge | The maximum age, in hundredths of a second, of the Spanning Tree Protocol information learned from the network on any port before being discarded. This value is the actual value that this bridge is currently using. |
| ForwardDelay | This value controls how fast a port changes its STP state when moving towards the Forwarding state. This value determines how long the port stays in a particular state before moving to the next state. This value is measured in units of hundredths of a second. |
| TimeSinceTopology Change | The time, in hundredths of a second, since the TcWhile Timer for any port in this Bridge was non-zero for the Common Spanning Tree context. |
| NewRootBridgeCount | The number of times this Bridge detects a Root Bridge change for the Common Spanning Tree context. A Trap is generated when this event occurs. |
| TopChanges | The number of times that at least one non-zero TcWhile Timer occurred on this Bridge for the Common Spanning Tree context. |
| RegionName | Specifies the region name of the configuration. By default, the Region Name is equal to the Bridge Mac Address. |

| Variable | Value |
|---|---|
| ConfigIdSel | The Configuration Identifier Format Selector used by the Bridge. This has a fixed value of 0 which indicates RegionName, RegionVersion, as specified in the standard. |
| RegionVersion | Denotes the version of the MST Region. |
| ConfigDigest | Signifies the Configuration Digest value for this Region. This is an MD5 digest value and hence must always be 16 octets long. |
| RegionConfigChange Count | The number of times a Region Configuration Identifier Change is detected. A trap is generated when this event occurs. |

# Viewinf MSTP CIST Ports

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to view the MSTP CIST Port tab:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **MSTP**.
4. Select the **CIST Port** tab.

# Variable definitions

The following table outlines the parameters of the **CIST Port** tab.

**Table 38: MSTP CIST Port tab parameters**

| Variable | Value |
|---|---|
| Port | The port number of the port containing Spanning Tree information. |
| PathCost | The contribution of this port to the cost of paths towards the CIST Root. |
| Priority | The four most significant bits of the Port Identifier of the Spanning Tree instance. It can be modified by setting the |

| Variable | Value |
|----------|-------|
|  | CistPortPriority value. The values that are set for Port Priority must be in steps of 16. |
| DesignatedRoot | This field specifies the unique Bridge Identifier of the bridge. Recorded as the CIST Root in the configuration BPDUs which are transmitted. |
| DesignatedCost | The path cost of the Designated Port of the segment connected to this port. |
| DesignatedBridge | The unique Bridge Identifier of the bridge which the port considers to be the Designated Bridge for the port segment. |
| DesignatedPort | The Port identifier of the port on the Designated Bridge which is designated for the port segment. |
| RegionalRoot | Displays the unique Bridge Identifier of the bridge. Recorded as the CIST Regional Root Identifier in the configuration BPDUs which are transmitted. |
| RegionalPathCost | The contribution of this port to the cost of paths towards the CIST Regional Root. |
| ProtocolMigration | Indicates the Protocol migration state of this port. When operating in MSTP mode, set this field to true to force the port to transmit MSTP BPDUs without instance information.<br><br>**Note:**<br>If this field is set to true and the port receives an 802.1d BPDU, the port begins transmitting 802.1d BPDUs. If the port receives an 802.1w BPDU, it begins transmitting 802.1w BPDUs. |
| AdminEdgeStatus | The administrative value of the Edge Port parameter. A value of true indicates that this port can be assumed to be an edge-port, and a value of false indicates that this port can be assumed to be a nonedge-port. |
| OperEdgeStatus | Signifies the operational value of the Edge Port parameter. This value is initialized to the value of AdminEdgeStatus and set to false when the port receives a BPDU. |
| AdminP2P | The administrative point-to-point status of the LAN segment attached to this port. A value of 0 indicates that this port is always treated as being connected to a point-to-point link. A value of 1 indicates that this port is treated as having a shared media connection. A value of 2 indicates that this port is considered to have a point-to-point link if it is an Aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation, or by management means. |
| OperP2P | This field indicates the operational point-to-point status of the LAN segment attached to the port. It also indicates whether a |

| Variable | Value |
|---|---|
| | port is considered to have a point-to-point connection. The value is determined by management or by auto-detection, as described in the AdminP2P object. |
| HelloTime | The amount of time between the transmission of Configuration BPDUs transmitted by this node on the port. Measured in units of hundredths of a second. |
| OperVersion | This indicates whether the Port is operationally in the MSTP, RSTP, or STP-compatible mode; that is, whether the port is transmitting MST BPDUs, RST BPDUs, or Config/TCN BPDUs. |
| EffectivePortState | The effective operational state of the port for CIST. This is set to true only when the port is operationally up in the Interface level and Protocol level for CIST. This is set to false for all other times. |
| State | The current state of the port as defined by the Common Spanning Tree Protocol. |
| ForcePortState | The current state of the port which can be changed to either Disabled or Enabled for the base Spanning Tree instance. |
| SelectedPortRole | Selected port role for the Spanning Tree instance. |
| CurrentPortRole | Current port role for the Spanning Tree instance. |

# Graphing MSTP CIST Port statistics

The CIST Port Stats tab shows CIST Port statistics.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the CIST Port Stats tab for graphing:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **MSTP**.
4. Select the **CIST Port** tab.
5. Select a port and click Graph to get the statistics for the CIST Port.

## Variable definitions

The following table outlines the parameters of the **CIST Port Graph** dialog box.

**Table 39: CIST Port Graph dialog box parameters**

| Variable | Value |
|---|---|
| ForwardTransitions | The number of times this port transitioned to the Forwarding State. |
| RxMstBpduCount | The number of MST BPDUs received on this port. |
| RxRstBpduCount | The number of RST BPDUs received on this port. |
| RxConfigBpduCount | The number of Configuration BPDUs received on this port. |
| RxTcnBpduCount | The number of TCN BPDUs received on this port. |
| TxMstBpduCount | The number of MST BPDUs transmitted from this port. |
| TxRstBpduCount | The number of RST BPDUs transmitted from this port. |
| TxConfigBpduCount | The number of Configuration BPDUs transmitted from this port. |
| TxTcnBpduCount | The number of TCN BPDUs transmitted from this port. |
| InvalidMstBpduRxCount | The number of Invalid MST BPDUs received on this port. |
| InvalidRstBpduRxCount | The number of Invalid RST BPDUs received on this port. |
| InvalidConfigBpdu RxCount | The number of Invalid Configuration BPDUs received on this port. |
| InvalidTcnBpduRxCount | The number of Invalid TCN BPDUs received on this port. |
| ProtocolMigrationCount | The number of times this port migrated from one STP protocol version to another. The relevant migration protocols are STP-COMPATIBLE and RSTP/MSTP. A trap is generated when the port migrates. |

# ViewingMSTP MSTI Bridges

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to view the MSTI Bridges tab:

### Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **MSTP**.
4. Select the **MSTI Bridges** tab.

## Variable definitions

The following table outlines the parameters of the **MSTI Bridges** tab.

**Table 40: MSTP MSTI Bridges tab parameters**

| Variable | Value |
|---|---|
| Instance | Spanning Tree Instance to which the information belongs. |
| RegionalRoot | Indicates the MSTI Regional Root Identifier value for the Instance. This value is used as the MSTI Regional Root Identifier parameter in all Configuration Bridge PDUs originated by this node. |
| Priority | The writable portion of the MSTI Bridge Identifier comprising the first two octets. The values that are set for Bridge Priority must be in steps of 4096. |
| RootCost | The cost of the path to the MSTI Regional Root as seen by this bridge. |
| RootPort | The number of the port which offers the lowest path cost from this bridge to the MSTI Region Root Bridge. |
| Enabled | Used to control whether the bridge instance is enabled or disabled. |
| TimeSinceTopology Change | The time (measured in hundredths of a second) since the TcWhile Timer for any port in this Bridge was non-zero for this Spanning Tree instance. |
| TopChanges | The number of times that at least one non-zero TcWhile Timer occurred on this Bridge for this Spanning Tree instance. |
| NewRootCount | The number of times this Bridge has detected a Root Bridge change for this Spanning Tree instance. A Trap is generated on the occurrence of this event. |
| InstanceUpCount | The number of times a new Spanning Tree instance was created. A Trap is generated on the occurrence of this event. |
| InstanceDownCount | The number of times a Spanning Tree instance was deleted. A Trap is generated on the occurrence of this event. |

# Inserting MSTP MSTI Bridges

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to insert an MSTI bridge:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **MSTP**.
4. Select the **MSTI Bridges** tab.
5. Click the **Insert** button.

   The Instance dialog box appears with the next available instance shown.
6. Click **Insert**.

   The next available instance appears in the MSTI Bridges tab.

# Deleting MSTP MSTI Bridges

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete an MSTI bridge:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **MSTP**.
4. Select the **MSTI Bridges** tab.
5. In the MSTI Bridges tab, click the Instance field for the MSTI bridge that you want to delete.
6. Click **Delete**.

The selected instance is deleted from the MSTI Bridges tab.

# Associating a VLAN with the CIST or an MSTI instance

You can use Enterprise Device Manager to associate a VLAN with the CIST or an MSTI instance.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to associate a VLAN with the CIST or an MSTI instance:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **VLANs**.
3. Select the **Basic**.
4. Click **Insert**.

   The VLAN, Insert Basic dialog box appears.
5. In the **MstpInstance** field, select the CIST or an MSTI instance from the menu.
6. Populate the other fields as required.
7. Click **Insert**.

# Modifying VLAN CIST or MSTI association

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to modify an existing VLAN association with a CIST or MSTI:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **VLANs**.
3. Select the **Basic**.
4. Double-click in the **MstpInstance** field.

The MstpInstance menu appears.

5. Select the CIST option or one of the MSTI options and click **Apply**.

This associates the VLAN with the option you selected.

# Viewing MSTP MSTI Ports

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to view the MSTI Port tab:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **MSTP**.
4. Select the **MSTI Port** tab.

# Variable definitions

The following table outlines the parameters of the **MSTI Port** tab.

**Table 41: MSTP MSTI Port tab parameters**

| Variable | Value |
|----------|-------|
| Port | Denotes the port number. |
| BridgeInstance | The number of times a Spanning Tree instance was deleted. A Trap is generated when this event occurs. |
| State | Indicates the current state of the port as defined by the Multiple Spanning Tree Protocol. The state of a port can be Forwarding or Discarding (Blocking). |
| ForcePortState | Signifies the current state of the port which can be changed to either Disabled or Enabled for the specific Spanning Tree instance. |
| PathCost | The contribution of this port to the cost of paths towards the MSTI Root which includes this port. |
| Priority | Indicates the four most significant bits of the Port Identifier for a given Spanning Tree instance. This value can be modified independently for each Spanning Tree instance |

| Variable | Value |
| --- | --- |
| | supported by the Bridge. The values set for Port Priority must be in steps of 16. |
| DesignatedRoot | The unique Bridge Identifier of the bridge recorded as the MSTI Regional Root in the configuration BPDUs that are transmitted. |
| DesignatedBridge | The unique Bridge Identifier of the bridge which this port considers to be the Designated Bridge for the port segment. |
| DesignatedPort | The Port identifier of the port on the Designated Bridge for this port segment. |
| DesignatedCost | The path cost of the Designated Port of the segment connected to this port. |
| CurrentPortRole | Current Port Role of the port for this spanning tree instance. |
| EffectivePortState | The effective operational state of the port for the specific instance. This is set to true only when the port is operationally up in the interface level and Protocol level for the specific instance. This is set to false at all other times. |

# Graphing MSTP MSTI Port Statistics

The MSTI Port tab can be used to graph MSTI port statistics.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the MSTI Port tab for graphing:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **MSTP**.
4. Select the **MSTI Port** tab.
5. Select a port and click **Graph** to get the statistics for the MSTI Port.

   The following table describes the fields in the MSTI Port Statistics fields.

# Variable definitions

The following table outlines the parameters of the **MSTI Port Graph** dialog box.

**Table 42: MSTP MSTI Port Graph dialog box parameters**

| Variable | Value |
|----------|-------|
| ForwardTransitions | Number of times this port transitioned to the Forwarding State for the specific instance. |
| ReceivedBPDUs | Number of BPDUs received by this port for this spanning tree instance. |
| TransmittedBPDUs | Number of Invalid BPDUs received on this Port for this Spanning Tree instance. |
| InvalidBPDUsRcvd | Number of BPDUs transmitted on this port for this Spanning Tree instance. |

# Chapter 15:  Configuring MLT using Enterprise Device Manager

The Enterprise Device Manager (EDM) screens detailed in the following sections allow for the creation and management of Multi-Link trunks:

## MultiLink Trunks configuration

This section provides information about MultiLink Trunks configuration.

### Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

This section provides information about the following topics:

## Navigation

## Setting up MLTs

### Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to create an MLT:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.

2. From the VLAN tree, double-click **MLT/LACP**.

3. Select the **MultiLink Trunks** tab.

4. In the fields provided on the **Multi-Link Trunks** tab, enter the information necessary to complete the MLT. For a description of adding ports to the MLT (PortMembers field), see Adding MLT Ports on page 265.

5. Click **Apply**.

## Variable definitions

The following table outlines the parameters of the **MultiLink Trunks** tab.

**Table 43: MLT/LACP MultiLink Trunks tab parameters**

| Variable | Value |
|---|---|
| ID | The number of the MLT (assigned consecutively). |
| PortType | The port type:<br>• Access<br>• trunk<br>• UntagPvidOnly<br>• TagPvidOnly |
| Name | The name given to the MLT. |
| PortMembers | The ports that are assigned to the MLT. |
| VlanIds | Specifies the VLAN identifier. |
| Loadbalance(Mode) | Sets the MLT load balancing mode as either basic (MAC-based load balancing) or advanced (IP-based load balancing). |
| Enable | Specifies whether the Multi-Link trunk is active. |
| MltType | Editable field that specifies the type of MLT:<br>• normalMLT<br>• istMLT<br>• splitMLT |
| RunningType | Read-only field the displays the current MLT operational type: |

| Variable | Value |
|---|---|
|  | • normalMLT<br><br>• istMLT<br><br>• splitMLT |
| SmltId | The assigned SMLT ID. Both ends of the SMLT must have the same SMLT ID. The SmltId field is used when the MltType is splitMLT. The SmltId value should be 0 if the MltType is not splitMLT. |

# Filtering the Multi-Link Trunks tab display

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to filter the display of the Multi-Link Trunks tab to display selected types of MLT:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **MLT/LACP**.
3. Select the **MultiLink Trunks** tab.
4. Click **Filter**.

   The MLT_LACP, Multi-Link Trunks - Filter dialog box appears.
5. Set the properties, and click **Filter**.

   The Multi-Link Trunks table displays information based on the specified criteria.

# Adding MLT Ports

The selected ports are now displayed on the MLT_LACP dialog box in the PortMembers field.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to add ports to an MLT:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.

2. From the VLAN tree, double-click **MLT/LACP**.

3. Select the MultiLink Trunks tab.

4. Click **Filter**.

   The MLT_LACP, Multi-Link Trunks - Filter dialog box appears.

5. Set the properties, and click **Filter**.

   The Multi-Link Trunks table displays information based on the specified criteria.

6. Double-click in the **PortMembers** field for the MLT to which ports are to be added. The PortMembers screen appears.

7. Click on the buttons that represent the ports that are to be added to the MLT. For the 5000 Series, up to 8 same-type ports can belong to a single MLT

8. Click **OK**.

9. Click **Apply**.

# Disabling MLT ports on Shutdown

Use this procedure to configure the system to disable MLT ports on shutdown.

1. From the navigation tree, click **VLAN**.

2. From the VLAN tree, click **MLT/LACP**.

3. Select the **Globals** tab.

4. Select the **MltDisablePortsOnShutdown** check box.

5. In the SmltSysId field, enter the LACP system ID for SMLT (MAC address).

6. On the tool bar, click **Apply**.

**Table 44: Variable definitions**

| Variable | Value |
|---|---|
| MltDisablePortsOnShutdown | Specifies whether the function is enabled or disabled. |
| SmltSysId | Specifies the MAC address of the LACP system ID for SMLT. |

# Configuring SMLT

This section describes how to use Enterprise Device Manager (EDM) to configure Split Multi-Link Trunking (SMLT) and includes the following topics:

- Adding an MLT-based SMLT on page 267
- Viewing SLTs configured on your switch on page 268
- Configuring an SLT on page 269
- Deleting an SLT on page 270
- Configuring an IST MLT on page 270
- Removing an IST MLT on page 272
- Viewing IST statistics on page 272

**Note:**

To configure SMLT on the 5000 Series switch, an Advanced License must be purchased that allows this feature to be used.

## Adding an MLT-based SMLT

**Important:**

For SMLT to function properly, you must manually disable STP on all SMLT, IST, and SLT ports in all spanning tree groups or instances to which the ports belong. You must also disable STP on all edge switch MLT ports that are connected to the SMLT or SLT.

You can create an SMLT from the MultiLink Trunks tab by selecting the MLT type as SMLT and then specifying an SMLT ID.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to add an MLT-based SMLT:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **MLT/LACP**.
3. Select the **MultiLink Trunks** tab.

4. From the displayed list of MLTs, choose an available MLT to configure as an SMLT.

5. In the row containing the desired MLT, double-click the **PortMembers** field.

   The PortMembers dialog box appears, displaying the available ports.

6. Click the ports to include in the MLT-based SMLT.

   For the 5000 Series, up to eight same-type ports can belong to a single MLT.

7. Click **OK**.

   The MltPortMembers dialog box closes, and the ports are added to the PortMembers field.

8. Double-click the **MltType** field and choose **splitMLT** from the list.

9. In the **SmltId** field, type an unused SMLT ID (1 - 32).

   > **Note:**
   >
   > The corresponding SMLTs between aggregation switches must have matching SMLT IDs. The same ID number must be used on both sides.

10. Click **Apply**.

# Viewing SLTs configured on your switch

### Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to view the SLTs configured on your switch:

### Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **MLT/LACP**.
3. Select the Single Port SMLT tab.

## Variable definitions

The following table outlines the parameters of the **Single Port SMLT** tab.

**Table 45: MLT/LACP Single Port SMLT tab parameters**

| Variable | Value |
|----------|-------|
| Index | Displays the index number. |

| Variable | Value |
|---|---|
| SmltId | The ID number of the SLT (1 - 512). |
| RunningType | Read only field that displays the current port operational type:<br><br>• normal<br><br>• smlt (single port Split MLT) |

## Configuring an SLT

**Important:**

For SMLT to function properly, you must manually disable STP on all SMLT, IST, and SLT ports in all spanning tree groups or instances to which the ports belong. You must also disable STP on all edge switch MLT ports that are connected to the SMLT or SLT.

Ports that are already configured as MLT or MLT-based SMLT cannot be configured as a single port SLT. You must first remove the split trunk and then reconfigure the ports as an SLT.

**Prerequisites**

• Open one of the supported Web browsers.

• Access the switch.

• Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to configure an SLT:

**Procedure steps**

1. From the Device Physical View, double-click a port.

2. Select the **SMLT** tab.

   **Note:**

   If the MltId field is not zero, this indicates that the port is already configured as an MLT or MLT-based SMLT. If so, you cannot configure an SLT on the port.

3. Click **Insert.**

   The Insert SMLT dialog box appears.

4. In the **SmltId** field, enter an unused SMLT ID number from 1 to 512.

   To view the SMLT IDs that are already in use on your switch, see <u>Viewing SLTs configured on your switch</u> on page 268.

5. Click **Insert**.

   The Insert SMLT dialog box closes, and the ID is entered into the SMLT tab.

## Variable definitions

The following table outlines the parameters of the **Port X/X** tab.

**Table 46: Edit Port X/X tab parameters**

| Variable | Value |
|----------|-------|
| Index | The index number for the port. |
| MltId | Read only field displaying either a value between 1 and 32 indicating that the port is part of an MLT or a value of 0 indicating the port has no MLT assigned and that it can be configured for SLT. |
| SmltId | The Split MLT ID is an integer from 1 to 512. |

# Deleting an SLT

• Open one of the supported Web browsers.

• Access the switch.

• Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete an SLT:

**Procedure steps**

1. From the Device Physical View, double-click a port.
2. Select the **SMLT** tab.
3. Select the Port SLT.
4. Click **Delete** .
5. Click **Close**.

   The SLT configured for this port is deleted.

# Configuring an IST MLT

**Important:**

For SMLT to function properly, you must manually disable STP on all SMLT, IST, and SLT ports in all spanning tree groups or instances to which the ports belong. For Release 6.2 onward, STP is automatically disabled by software on all SMLT ports. You must also disable STP on all edge switch MLT ports that are connected to the SMLT or SLT.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to configure an IST MLT:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **MLT/LACP**.
3. Select the MultiLink Trunks tab.
4. In the row containing the desired MLT, double-click the **PortMembers** field.

   The PortMembers dialog box appears, displaying the available ports.
5. Select the ports to include in the MLT and click **OK**.

   For the 5000 Series, up to eight same-type ports can belong to a single MLT.

   The MltPortMembers dialog box closes, and the ports are added to the PortMembers field.
6. Double-click the **Enable** field and choose **true**.
7. Double-click the **MltType** field and choose **istMLT** from the list.
8. Click **Apply**.
9. Select any field in the IST MLT row and click the **istMlt** button.

   The Ist MLT dialog box appears.
10. In the **PeerIp** field, enter a peer IP address.
11. In the **VlanId** field, enter a VLAN ID.
12. In the **SessionEnable** field, click **enable**.
13. Click **Apply**.

    The IST MLT dialog box closes, and the changes are applied. The IST MLT is now configured.

# Variable definitions

The following table describes the IST MLT parameters .

**Table 47: MLT/LACP IST MLT parameters**

| Variable | Value |
|---|---|
| PeerIp | IST MLT peer IP address. |

| Variable | Value |
|----------|-------|
| VlanId | An IST VLAN ID number from 1 to 4095. |
| SessionEnable | Enable/disable IST functionality. |
| Session Status | Read only: up or down |

# Removing an IST MLT

### Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to remove an existing IST MLT from your switch:

### Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **MLT/LACP**.
3. Select the MultiLink Trunks tab.
4. Change the **MltType** field for the IST from **istMLT** to **normalMLT**.
5. Click **Apply**.

# Viewing IST statistics

### Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to view IST statistics on an interface:

### Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **MLT/LACP**.
3. Select the **Ist/SMLT Stats** tab.

# Variable definitions

The following table outlines the parameters of the **Ist/SMLT Stats** tab.

**Table 48: MLT/LACP Ist/SMLT Stats tab parameters**

| Variable | Value |
| --- | --- |
| SmltIstDownCnt | The number of IST down messages. |
| SmltHelloTxMsgCnt | The number of hello messages transmitted. |
| SmltHelloRxMsgCnt | The number of hello messages received. |
| SmltLearnMacAddrTxMsgCnt | The number of learn MAC address messages transmitted. |
| SmltLearnMacAddrRxMsgCnt | The number of learn MAC address messages received. |
| SmltMacAddrAgeOutTxMsgCnt | The number of MAC address aging out messages transmitted. |
| SmltMacAddrAgeOutRxMsgCnt | The number of MAC address aging out messages received. |
| SmltMacAddrAgeExpTxMsgCnt | The number of MAC address age expired messages transmitted. |
| SmltMacAddrAgeExpRxMsgCnt | The number of MAC address age expired messages received. |
| SmltStgInfoTxMsgCnt | The number of SMLT STG info messages transmitted. |
| SmltStgInfoRxMsgCnt | The number of SMLT STG info messages received. |
| SmltDelMacAddrTxMsgCnt | The number of deleted MAC address messages transmitted. |
| SmltDelMacAddrRxMsgCnt | The number of deleted MAC address messages received. |
| SmltSmltDownTxMsgCnt | The number of SMLT down messages transmitted. |
| SmltSmltDownRxMsgCnt | The number of SMLT down messages received. |
| SmltSmltUpTxMsgCnt | The number of SMLT up messages transmitted. |
| SmltSmltUpRxMsgCnt | The number of SMLT up messages received. |
| SmltSendMacTblTxMsgCnt | The number of send MAC table messages transmitted. |
| SmltSendMacTblRxMsgCnt | The number of send MAC table messages received. |
| SmltIgmpTxMsgCnt | The number of IGMP messages transmitted. |

| Variable | Value |
|---|---|
| SmltIgmpRxMsgCnt | The number of IGMP messages received. |
| SmltPortDownTxMsgCnt | The number of port down messages transmitted. |
| SmltPortDownRxMsgCnt | The number of port down messages received. |
| SmltReqMacTblTxMsgCnt | The number of request MAC table messages transmitted. |
| SmltReqMacTblRxMsgCnt | The number of request MAC table messages received. |
| SmltRxUnknownMsgTypeCnt | The number unknown SMLT messages received. |

# Chapter 16: Configuring LACP and VLACP using Enterprise Device Manager

This section contains information on the following topics:

## Configuring LACP using Enterprise Device Manager

You can configure LACP using the following Enterprise Device Manager tabs:

## Configuring the LACP port compatibility mode

You can use the LACP Global tab to configure the LACP port compatibility mode.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the LACP Global tab:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **MLT/LACP**.
3. Select the **LACP Global** tab.

## Variable definitions

The following table outlines the parameters of the **LACP Global** tab.

**Table 49: MLT/LACP LACP Globals tab parameters**

| Variable | Value |
|---|---|
| CompatibilityMode | Specifies the port compatibility mode for LACP:<br><br>• default<br><br>• advanced |

# Configuring Link Aggregation Groups

You can use the LACP tab to configure Link Aggregation Groups.

**Prerequisites**

• Open one of the supported Web browsers.

• Access the switch.

• Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the LACP tab:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.

2. From the VLAN tree, double-click **MLT/LACP**.

3. Select the **LACP** tab.

## Variable definitions

The following table outlines the parameters of the **LACP** tab.

**Table 50: MLT/LACP LACP tab parameters**

| Variable | Value |
|---|---|
| Index | The unique identifier allocated to this Aggregator by the local System. This attribute identifies an Aggregator instance among the subordinate managed objects of the containing object. This value is read-only. |
| MacAddress | The MAC address used by this bridge when it must be referred to in a unique fashion. |

| Variable | Value |
|---|---|
| AggregateOrIndividual | A read-only Boolean value indicating whether the Aggregation Port can Aggregate (TRUE) or can only operate as an Individual link (FALSE). |
| ActorLagID | The combined information of ActorSystemPriority, ActorSystemID, and ActorOperKey in ActorSystemPriority-ActorSystemID-ActorOperKey format. |
| ActorSystemPriority | A 2-octet read-write value indicating the priority value associated with the Actor's System ID. |
| ActorSystemID | A 6-octet read-only MAC address value that defines the value of the System ID for the System that contains this Aggregation Port. |
| ActorOperKey | The current operational value of the Key for the Aggregation Port. This is a 16-bit read-only value. |
| ActorAdminKey | The current administrative value of the Key for the Aggregation Port. This is a 16-bit read-write value. |
| PartnerLagID | The combined information of PartnerSystemPriority, PartnerSystemID, and PartnerOperKey in PartnerSystemPriority-PartnerSystemID-PartnerOper Key format. |
| PartnerSystemPriority | A 2-octet read-only value that indicates the priority value associated with the Partner's System ID. |
| PartnerSystemID | A 6-octet read-only MAC address value consisting of the unique identifier for the current protocol Partner of this Aggregator. A value of zero indicates that no known Partner exists. If the aggregation is manually configured, this System ID value is assigned by the local System. |
| PartnerOperKey | The current operational value of the Key for the Aggregator's current protocol Partner. This is a 16-bit read-only value. |
| CollectorMaxDelay | The value of this 16-bit read-write attribute defines the maximum delay, in tens of microseconds, that can be imposed by the Frame Collector between receiving a frame from an Aggregator Parser, and either delivering the frame to its MAC Client or discarding the frame. |

# Configuring LACP ports

**Prerequisites:**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to view or edit the LACP Ports tab:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **MLT/LACP**.
3. Select the **LACP Ports** tab.

# Variable definitions

The following table outlines the parameters of the **LACP Ports** tab.

**Table 51: MLT/LACP LACP Ports tab parameters**

| Variable | Value |
|---|---|
| Index | The ifIndex of the port |
| AdminEnabled* | The current administrative setting for the port. A value of true means the port is set to participate in LACP. A value of false means the port is set to not participate in LACP. |
| operEnabled | The current operational state for the port. A value of true means the port is participating in LACP. A value of false means the port is not participating in LACP. |
| AggregateOrIndividual | A read-only Boolean value indicating whether the Aggregator represents an Aggregate (true) or an Individual link (false). |
| ActorSystemPriority | A 2-octet read-write value used to define the priority value associated with the Actor's System ID. |
| ActorSystemID | A 6-octet read-only MAC address value that defines the value of the System ID for the system that contains this Port. |
| ActorAdminKey | The current administrative value of the Key for the Aggregation Port. |
| ActorOperKey | The current operational value of the Key for the Aggregation Port. |
| SelectedAggID | The identifier value of the Aggregator that this Aggregation Port has currently selected. Zero indicates that the Aggregation Port has not selected an Aggregator, either because it is in the process of detaching from an Aggregator or because no suitable Aggregator exists for it to select. |
| AttachedAggID | The identifier value of the Aggregator that this Aggregation Port is currently attached to. Zero indicates that the Aggregation Port is not currently attached to an Aggregator. This value is read-only. |

| Variable | Value |
|---|---|
| ActorPort | The port number locally assigned to the Aggregation Port. The port number is communicated in LACPDUs as the Actor_Port. This value is read-only |
| ActorPortPriority | The priority value assigned to this Aggregation Port. This 16-bit value is read-write. |
| ActorAdminState* | A string of 8 bits, corresponding to the administrative values of Actor_State as transmitted by the Actor in LACPDUs. |
| ActorOperState | A string of 8 bits, corresponding to the current operational values of Actor_State as transmitted by the Actor in LACPDUs. |
| PartnerOperPort | The operational port number assigned by the port's protocol partner. This value is read-only. |

*To set the LACP modes using DM, you must ensure that the LACP port properties are set according to the desired mode, as follows:

- LACP mode Off = **AdminEnabled** field cleared (disabled)

- LACP mode Passive = **AdminEnabled** field selected (enabled)

- LACP mode Active = **AdminEnabled** field selected (enabled) and **ActorAdminState** options **lacpActive** and **aggregation** selected

# Mapping the LACP key mapping

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the LACP key mapping tab:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **MLT/LACP**.
3. Select the **LACP key mapping** tab.

## Variable definitions

The following table outlines the parameters of the **LACP key mapping** tab.

**Table 52: MLT/LACP LACP key mapping tab parameters**

| Variable | Value |
|---|---|
| LacpKeyValue | Specifies the value of the LACP administration key. |
| MltId | Specifies the ID of the MLT. |
| SmltId | Specifies the ID of the SMLT. |

# Configuring VLACP using Enterprise Device Manager

You can configure VLACP using the following Enterprise Device Manager tabs:

## Viewing VLACP Global information

VLACP is an extension to LACP used to detect end-to-end failure.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to view VLACP information for the switch:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **MLT/LACP**.
3. Select the **VLACP Global** tab.

## Variable definitions

The following table outlines the parameters of the **VLACP Global** tab.

**Table 53: MLT/LACP VLACP Global tab parameters**

| Variable | Value |
|---|---|
| Enable | Enables or disables VLACP on the switch. |

| Variable | Value |
|---|---|
| MulticastMACAddress | Identifies a multicast MAC address used exclusively for VLACPDUs. Default is 01:80:c2:00:11:00. |

# VLACP tab for ports

Use the following procedure to view the VLACP tab for ports:

## Procedure steps

1. In the Device Physical View, double-click a Port.

   The Port X/X dialog box appears with the Interface tab displayed.

2. Select the VLACP tab.

If you want to configure multiple ports, you can access the VLACP tab on the MLT/LACP tab.

## Variable definitions

The following table outlines the parameters of the **VLACP** tab.

**Table 54: Port X/X VLACP tab parameters**

| Variable | Value |
|---|---|
| AdminEnable | Enables or disables VLACP on a port. The default value is False. |
| OperEnable | Indicates whether VLACP is operationally enabled or disabled. This is a read-only field. |
| FastPeriodicTimer | Specifies the number of milliseconds between periodic transmissions using short timeouts. Valid values range from 400-20000 with a default of 500. |
| SlowPeriodicTimer | Specifies the number of milliseconds between periodic transmissions using long timeouts. Valid values range from 10000-30000 with a default of 30000. |
| Timeout | Specifies whether the timeout control value is a short or long timeout. |
| TimeoutScale | Sets a timeout scale for the port, where timeout = (periodic time) * (timeout scale).<br>The range is 1-10. Default is 3. |

| Variable | Value |
|---|---|
| | Note: With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. However, if the timeout-scale is set to less than 3, the port timeout value does not take into account the normal travel time of the VLACPDU. The port expects to receive a VLACPDU at the same moment the partner port sends it. Therefore, the delayed VLACPDU results in the link being blocked, and then enabled again when the packet arrives. To prevent this scenario from happening, set the timeout-scale to a value larger than 3. If a VLACP partner does not receive a VLACPDU during (periodic time)*(timeout scale) the system sets the link as VLACP down. |
| EtherType | Specifies VLACP protocol identification. The ID value is a 4-digit Hex number, with a default of 8103. |
| EtherMacAddress | The default value is 00:00:00:00:00:00 and it can be configured with the MAC address of the switch or stack to which this port is sending VLACPDUs. It cannot be configured as a multicast MAC.<br>Note: VLACP has only one multicast MAC address, configured using the MulticastMACAddress field in the VLACP Global tab, which is the Layer 2 destination address used for the VLACPDUs. The port-specific EtherMACAddresss parameter does not specify a multicast MAC address, but instead specifies the MAC address of the switch or stack to which this port is sending VLACPDUs. You are not always required to configure EtherMACAddresss. If not configured, the first VLACP-enabled switch that receives the PDUs from a unit assumes that it is the intended recipient and processes the PDUs accordingly.<br>If you want an intermediate switch to drop VLACP packets, configure the EtherMACAddresss field with the desired destination MAC address. With EtherMACAddresss configured, the intermediate switches do not misinterpret the VLACP packets. |
| PortState | Identifies whether the VLACP port state is up or down. This is a read-only field. |

# Chapter 17: Configuring SLPP using Enterprise Device Manager

This chapter provides procedures used to configure Simple Loop Prevention Protocol (SLPP) using Device Manager.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the SLPP dialog box:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **SLPP**.

This section contains information about the following topics:

## Configuring SLPP transmitting list

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to add a VLAN to the SLPP transmitting list:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **SLPP**.
3. Select the **VLANs** tab.
4. Under the **SlppEnable** heading, select the VLAN you want to add.
5. Double click to select True (enabled) or False (disabled).
6. Click **Apply**.
7. Click **Close**.

# Enabling SLPP

**Prerequisites**

• Open one of the supported Web browsers.

• Access the switch.

• Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to globally enable SLPP:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **SLPP**.
3. Select the **Globals** tab.
4. Select the **GlobalEnable** checkbox.
5. Click **Apply**.
6. Click **Close**.

# Configuring SLPP PDU transmit interval

The default SLPP PDU trasmit interval setting is 500 ms.

**Prerequisites**

• Open one of the supported Web browsers.

• Access the switch.

• Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to configure the SLPP PDU transmit interval in milliseconds:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **SLPP**.
3. Select the **Globals** tab.
4. In the **TransmissionInterval** text box, enter the value, in milliseconds, for the transmit interval in the range 500 to 5000. The default is 500.
5. Click **Apply**.
6. Click **Close**.

# Configuring SLPP PDU ether type

The default SLPP PDU ether type value is 0x8102.

> **Note:**
> Values 0x0000 and 0x8100 are disallowed.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to configures the SLPP PDU ether type value:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **SLPP**.
3. Select the **Globals** tab.
4. In the **EtherType** text box, enter the value for ether type.
5. Click **Apply**.
6. Click **Close**.

# Configuring SLPP port auto enable

If the timeout value is 0 (not active), the port will remain disabled until manually enabled by the user. The default value is 0 (disabled).

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to configure the auto enable timer for ports shut down by SLPP:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **SLPP**.
3. Select the **Globals** tab.
4. In the **PortsReEnableTimeout** text box, enter the value, in seconds, for the timeout in the range 0 to 65535.
5. Click **Apply**.
6. Click **Close**.

# Enabling SLPP PDU received function per port

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to enable the SLPP PDU received function on a port:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **SLPP**.
3. Select the **Ports** tab.
4. Under the **SlppEnable** heading, select the port you want to enable.
5. Double click to select True (enabled) or False (disabled).
6. Click **Apply**.
7. Click **Close**.

# Configuring the SLPP PDU receipt threshold

This procedure describes the steps necessary to configure the number of SLPP PDUs, in the range 1 to 500, that must be received prior to shutting down a port as a result of looping. The default threshold is 5.

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to enable the SLPP PDU received function on a port:

**Procedure steps**

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **SLPP**.
3. Select the **Ports** tab.
4. Under the **PktRxThreshold** heading, select the port you want to modify.
5. Double click and enter the value for the threshold in the range 1 to 500.
6. Click **Apply**.
7. Click **Close**.

# Chapter 18: Configuring ADAC using Enterprise Device Manager

You can configure ADAC-related settings using Enterprise Device Manager.

## Configuring ADAC settings

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to configure the global ADAC settings:

**Procedure steps**

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **ADAC**.
4. Select the **ADAC** tab.
5. Select the **AdminEnable** field to enable ADAC.
6. Choose the Operating Mode.
7. In the **NotificationControlEnable** field, enable or disable trap notifications.
8. Enter the Voice VLAN ID, Call Server port, and Uplink port.
9. Click **Apply**.

## Variable definitions

The following table outlines the parameters of the **ADAC** tab.

**Table 55: ADAC tab parameters**

| Variable | Value |
| --- | --- |
| AdminEnable | Enables and disables ADAC. |

| Variable | Value |
|---|---|
| OperEnable | Indicates ADAC operational state: true is enabled and false is disabled.<br><br>**Note:**<br>If AdminEnable is True and OperEnable is False, this indicates an error condition such as missing Uplink and Call Server ports. |
| OperatingMode | Sets the ADAC operation mode:<br><br>• untaggedFramesBasic: IP Phones send untagged frames, and the Voice VLAN is not created.<br><br>• untaggedFramesAdvanced: IP Phones send untagged frames, and the Voice VLAN is created.<br><br>• taggedFrames: IP Phones send tagged frames. |
| NotificationControlEnable | Enables and disables ADAC trap notifications. |
| VoiceVLAN | Sets the Voice VLAN ID. |
| CallServerPort | Sets the Call Server port. The Ethernet Routing Switch 5000 Series supports up to 8 Call Server ports. |
| UplinkPort | Sets the Uplink port. The Ethernet Routing Switch 5000 Series supports up to 8 Uplink ports. |
| MacAddrRangeControl | Provides two options for configuring the MAC address range table:<br><br>• clearTable: clears the MAC address range table.<br><br>• defaultTable: sets the MAC address range table to its default values. |

# Configuring ADAC MAC address ranges using EDM

**Prerequisites**

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to add MAC address ranges to the ADAC MAC address range table:

**Procedure steps**

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **ADAC**.
3. Select the **ADAC MAC Ranges** tab.
4. Click **Insert**.
5. In the **MacAddrRangeLowEndIndex** field, enter the low-end of the MAC address range to add.
6. In the **MacAddrRangeHighEndIndex** field, enter the high-end of the MAC address range to add.
7. Click **Insert**.

# Deleting MAC address ranges using Device Manager

**Prerequisites**

• Open one of the supported Web browsers.
• Access the switch.
• Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete MAC address ranges from the ADAC MAC address range table:

**Procedure steps**

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **ADAC**.
3. Select the **ADAC MAC Ranges** tab.
4. Select the desired range to delete.
5. Click **Delete**.

# Configuring ADAC settings on a port

**Prerequisites**

• Open one of the supported Web browsers.
• Access the switch.
• Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to configure ADAC settings on a port:

### Procedure steps

1. From the navigation tree, double-click **Edit**.

2. From the Edit tree, double-click **ADAC**.

3. Select the **ADAC** tab.

4. To enable ADAC for the port, select the **AdminEnable** check box. To disable ADAC for the port, clear the **AdminEnable** check box.

5. Select the **ADAC Ports** tab.

6. In the **TaggedFramesPvid** box, type a number between 0 and 4094, where 0 means "no change."

7. Click on the **TaggedFramesTagging** setting required.

8. Select **MacDetectionEnable** or **LldpDetectionEnable** or select them both to enable the detection methods on the port.

9. Click **Apply**.

## Variable definitions

The following table outlines the parameters of the **ADAC Ports** tab.

**Table 56: ADAC Ports tab parameters**

| Variable | Value |
|----------|-------|
| AdminEnable | Enables or disables ADAC for the port. |
| OperEnable | Indicates ADAC operational state: true is enabled and false is disabled.<br><br>**Note:**<br>If OperEnable is False and AdminEnable is True, then Auto-Detection/Auto-Configuration is disabled. This can occur due to a condition such as reaching the maximum number of devices supported per port. |
| ConfigStatus | (Read only) Describes the ADAC status for the port:<br>• configApplied means that the ADAC configuration is applied to this port.<br>• configNotApplied means that the ADAC configuration is not applied to this port. |
| TaggedFramesPVID | Unique PVID between 1 and 4094. A value of 0 indicates that Auto-Configuration cannot change the PVID for the respective port. |
| TaggedFramesTagging | Choose |

| Variable | Value |
|---|---|
|  | • tagAll to tag all frames |
|  | • tagPvidOnly to tag frames by the unique PVID |
|  | • untagPvidOnly to untag frames by the unique PVID |
|  | • noChange to accept frames without change |
| AdacPortType | Describes how ADAC classifies the port:<br><br>• telephony (when Auto-Detection is enabled for the port)<br><br>• callServer<br><br>• uplink<br><br>• none |
| MacDetectionEnable | True indicates that Auto-Detection of Avaya IP Phones, based on MAC address, is enabled on the interface. False indicates that Auto-Detection of Avaya IP Phones, based on MAC address, is disabled on the interface. NOTE: MacDetectionEnable cannot be set to false if no other supported detection mechanism is enabled on the port. |
| LldpDetectionEnable | True indicates that Auto-Detection of Avaya IP Phones, based on 802.1ab is enabled on the interface. False indicates that Auto-Detection of Avaya IP Phones, based on 802.1ab, is disabled on the interface. NOTE: LldpDetectionEnable cannot be set to False if no other supported detection mechanism is enabled on the port. |

*Comments? infodev@avaya.com*

# Appendix A: LACP over SMLT configuration example

This appendix shows you how to configure LACP over SMLT.

## LACP over SMLT configuration example

The following configuration example shows you how to configure LASP over SMLT.

The configuration is a triangle SMLT in which A and B are SMLT aggregation switches and C is the edge switch. The MAC address for switch A is 00:aa:aa:aa:aa:00; for switch B, 00:bb:bb:bb:bb:00: and C, 00:cc:cc:cc:cc:00.

### Prerequisites

- Ports 3 and 4 of switches A and B are SMLT ports.
- LACP is enabled on ports 1–4 of edge switch C, ports 3 and 4 of switch A, and ports 3 and 4 of switch B, .
- The switches are all in Global Configuration mode.

## Switch A configuration

Use the following procedure to configure switch A.

### Procedure steps

1. Prevent loops by configuring the switch in advance mode:

   ```
   lacp port-mode advance
   ```

2. Select switch A base MAC (00:aa:aa:aa:aa:00) as the system MAC and configure the LAC system MAC for SMLT:

```
lacp smlt sys-id 00:aa:aa:aa:aa:00
```

3. Place switch A in interface mode:

```
interface fastethernet 3,4
```

4. Assign key 2 to ports 3 and 4

```
lacp key 2
```

5. Enable LACP on ports 3 and 4:

```
lacp mode active
```

6. Return switch A to Global Configuration mode:

```
exit
```

7. Bind MLT 30 to key 2. This command tells MLT application to reserve MLT 30 for LACP key 2. Otherwise MLT will dynamically allocate an unused MLT # for LACP. Populate SMLT ID to the reserved trunk to make it SMLT enabled.

```
lacp key 2 mlt 30 smlt 2
```

8. Enable MLT1 with ports 1 and 2.

```
mlt 1 en mem 1-2
```

9. Set MLT 1 as the IST trunk.

```
int mlt 1
```

10. Set the IST VLAN ID as 10 and the IST peer IP address as 10.30.20.101.

```
ist enable peer-ip 10.30.20.101 vlan 10
```

11. Return switch A to the Global Configuration mode:

```
exit
```

# Switch B configuration

Use the following procedure to configure switch B.

## Procedure steps

1. Prevent loops by configuring the switch in advance mode:

```
lacp port-mode advance
```

2. Select switch A base MAC (00:aa:aa:aa:aa:00) as the system MAC and configure the LAC system MAC for SMLT:

```
lacp smlt sys-id 00:aa:aa:aa:aa:00
```

3. Place switch A in interface mode:

```
interface fastethernet 5
```

4. Assign key 2 to ports 3 and 4:

```
lacp key 2
```

5. Enable LACP on ports 3 and 4:

```
lacp mode active
```

6. Return switch B to the Global Configuration mode:

```
exit
```

7. Bind MLT 30 to key 2. This command instructs the MLT application to reserve MLT 30 for LACP key 2. Otherwise MLT will dynamically allocate an unused MLT number for LACP. Populate SMLT ID to the reserved trunk to make it SMLT-enabled.

```
lacp key 2 mlt 30 smlt 2
```

8. Enable MLT1 with ports 1 and 2.

```
mlt 1 en mem 1-2
```

9. Set MLT 1 as the IST trunk.

```
int mlt 1
```

10. Set the IST VLAN ID as 10 and the IST peer IP address as 10.30.20.101.

```
ist enable peer-ip 10.30.20.100 vlan 10
```

11. Return switch B to the Global Configuration mode:

```
exit
```

# Switch C configuration

Use the following procedure to configure switch C.

## Procedure steps

1. Prevent loops by configuring the switch in advance mode:

```
lacp port-mode advance
```

2. Place switch C in interface mode:

```
interface fastethernet 1-4
```

3. Enable LACP on ports 1–4:

```
lacp mode active
```

4. Return switch C to the Global Configuration mode:

```
exit
```

# Index

## U

## V