Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4000 Series

Release 5.7
NN47205-501
Issue 09.01
November 2013

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

Licence types

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your 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: Introduction

Purpose

This document provides information you need to configure VLANs, Spanning Tree and MultiLink Trunking for the Avaya Ethernet Routing Switch 4000 Series.

Related resources

Documentation

For a list of the documentation for this product, see *Documentation Reference for Avaya Ethernet Routing Switch 4000 Series*, NN47205–101.

Training

Ongoing product training is available. For more information or to register, see http://avaya-learning.com/.

Enter the course code in the **Search** field and click **Go** to search for the course.

Course code	Course title
8D00020E	Stackable ERS and VSP Products Virtual Campus Offering

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Searching a document collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx, for example, ers4000_5.7x.pdx.
3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
   - Whole words only
   - Case-Sensitive
   - Include Bookmarks
   - Include Comments
6. Click **Search**.
   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance ranking.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: New in this release

The following section details what is new in *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4000 Series*, NN47205-501 for Release 5.7.

Features

See the following section for information about feature changes:

ADAC Uplink over SPBM

ADAC Uplink over SPBM adds support for SPBM in ADAC, allowing ADAC to have the uplink over SPBM instead of an uplink port.

With this feature, ADAC can use an I-SID (that you associate with the ADAC Voice-VLAN) instead of a classical uplink-port. In this situation, ADAC can be enabled without the existence of a real uplink-port, and without the need of auto-configuring this uplink-port, therefore without auto-adding it to the Voice-VLAN.

FastEthernet replaced with Ethernet

The “FastEthernet” keyword from all CLI commands containing “FastEthernet” is replaced with the “Ethernet” keyword. For compliance, the old commands containing “FastEthernet” keyword are hidden, and you can configure the previous way too.

Note:

ASCII configurations from a release that has the “FastEthernet replaced with Ethernet” feature activated cannot be used to configure a setup that does not support this feature.

MLT/DMLT/LAG Dynamic VLAN behavior change

A warning message appears when you try to remove all the VLANs on an active MLT/DMLT/LAG. The message does not appear when you try to remove multiple VLANs. Following is the warning message:

```
Warning: you are about to remove all VLANs from the active trunk
group, doing so could cause loss of connectivity to the switch. Are
you sure you want to continue <Y/N>?
```

For more information, see MLT DMLT LAG Dynamic VLAN changes on page 39.

RSPAN VLAN

An RSPAN VLAN is a VLAN dedicated for a Remote Switch Port ANalyzer (RSPAN) session.

For more information, see

- Creating an RSPAN VLAN on page 95
- Deleting an RSPAN VLAN on page 95
- Displaying RSPAN VLAN information: on page 96
- VLAN Configuration using Enterprise Device Manager on page 181
- Creating an RSPAN VLAN using EDM on page 198

Show VLAN interface verbose command

Use the show vlan interface verbose command to display VLAN, PVID, and port information associated with a port.

For more information, see Displaying verbose VLAN interface information on page 89

Static LACP Key to Trunk ID binding

Static LACP Key to Trunk ID binding provides a higher level of control over the management of MLT trunk groups, compared with previous dynamic association of link-aggregated ports with a trunk group ID.

With Static LACP Key to Trunk ID binding, you associate a specific group of link-aggregated ports, identified by a group key, with a specific MLT trunk group ID. The static binding ensures that the switch maintains the LACP Key - MLT ID association until you delete the binding.

For more information, see:

- Static LACP Key to Trunk ID binding on page 81
- Configuring Static LACP Key to Trunk ID binding using ACLI on page 173
- Binding an LACP key to a specific trunk ID on page 173
- Deleting an LACP key binding to a trunk ID on page 174

- Displaying LACP key bindings to trunk IDs on page 174
- Configuring Static LACP Key to Trunk ID binding using EDM on page 292
- Binding an LACP key to a specific trunk ID using EDM on page 293
- Deleting an LACP key binding to a trunk ID using EDM on page 293
- Viewing LACP key bindings to trunk IDs using EDM on page 294

Other changes

See the following section for information about changes that are not feature-related.

New Introduction chapter

The Introduction chapter replaces the Purpose of this document and Customer service chapters.

VLAN Snoop

The VLAN snoop configuration information is documented in this release.

Chapter 3: VLAN Fundamentals

This chapter provides conceptual information relating to VLANs, Spanning Tree, MultiLink Trunks, and associated features and capabilities.

ACLI command modes

ACLI provides the following command modes:

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

Table 1: ACLI command modes

Command mode and sample prompt	Entrance commands	Exit commands

User EXEC
`4548GT-PWR>`
	No entrance command, default mode	`exit`
		or
		`logout`

Privileged EXEC
`4548GT-PWR#`
	`enable`	`exit`
		or
		`logout`

Global Configuration `4548GT-PWR(config)#`	`configure terminal`	mode, enter: `end`

Command mode and sample prompt	Entrance commands	Exit commands

		or
		`exit`
		To exit ACLI completely, enter:
		`logout`

Interface Configuration
`4548GT-PWR(config-if)#`
You can configure the following interfaces:
• Ethernet
• VLAN
	From Global Configuration mode: To configure a port, enter: `interface ethernet <port number>`
	To configure a VLAN, enter: `interface vlan <vlan number>`
		To return to Global Configuration mode, enter:
		`Exit`
		To return to Privileged EXEC mode, enter:
		`end`
		To exit ACLI completely, enter:
		`logout`

Router Configuration `4548GT-(configrouter)#` You can configure the following routers: • RIP • OSPF • VRRP • ISIS	From Global or Interface Configuration mode: To configure RIP, enter `router rip`. To configure OSPF, enter `router ospf`. To configure VRRP, enter `router vrrp`. To configure IS-IS, enter `router isis`.	To return to Global Configuration mode, enter `exit`. To return to Privileged EXEC mode, enter `end`. To exit ACLI completely, enter `logout`.
Application Configuration `4850GT-(config-app)`	From Global, Interface or Router Configuration mode, enter `application`.	To return to Global Configuration mode, enter `exit`. To return to Privileged EXEC mode, enter `end`. To exit ACLI completely, enter `logout`.

Virtual Local Area Networks

The Avaya Ethernet Routing Switch 4000 Series supports up to 1,024 concurrent VLANs.

You can group ports into broadcast domains by assigning them to the same VLAN. Frames received in one VLAN can be forwarded only 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 (refer the following figure). 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.

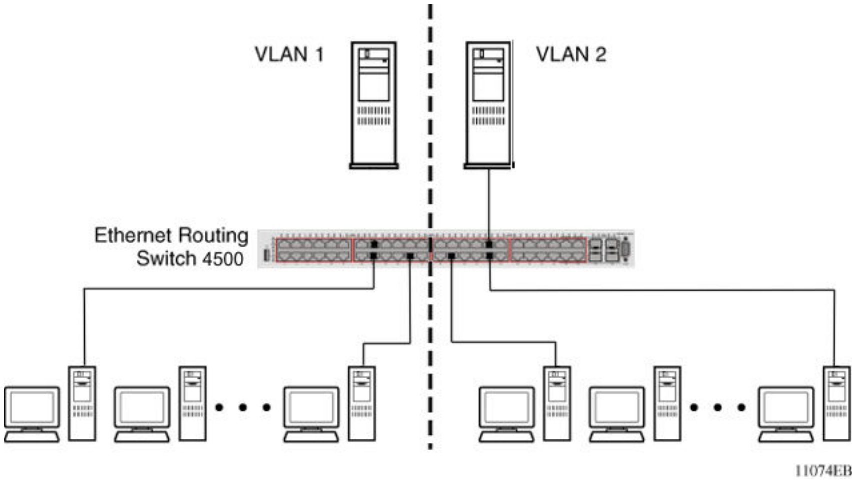


Figure 1: Port-based VLAN

With the Avaya Ethernet Routing Switch 4000 Series , you can assign ports to VLANs using the command line interface (ACLI) or the Enterprise Device Manager (EDM). You can assign different ports (and associated devices) to different broadcast domains to provide network flexibility. You can reassign VLANs to accommodate network moves, additions, and changes, to eliminate the need to change physical cabling.

IEEE 802.1Q Tagging

The Avaya Ethernet Routing Switch 4000 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, the values enabled in the management interfaces can override this default value.
- 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) and identifies the frame as belonging to a specific VLAN.
- Untagged frame: a frame that carries no 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 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 configured as a tagged member of a specific VLAN. When an untagged frame exits the switch through a tagged member port, the frame header changes 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 to 7. The tagged frame uses this field 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 obtain their user priority from the value in the 32-bit 802.1Q frame header.
- Unregistered packet: a tagged frame that contains a VID if the receiving port is not a member of that VLAN.
- Filtering database identifier (FID): the specific filtering and forwarding database within the Avaya Ethernet Routing Switch 4000 Series switch that is assigned to each VLAN. Each VLAN has a 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 4000 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 the following figure, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID =1). Untagged packets enter and leave the switch unchanged.

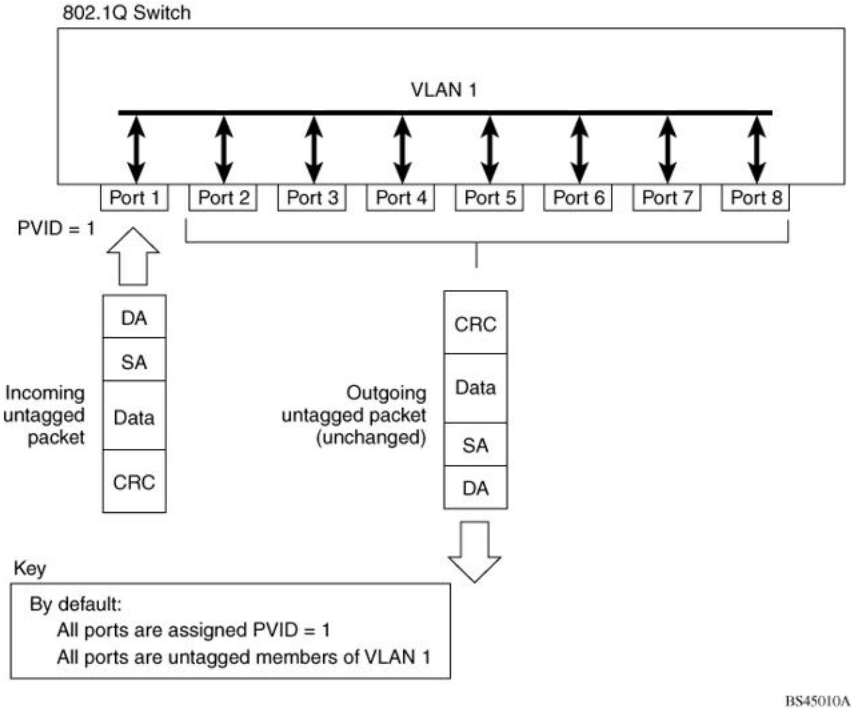


Figure 2: Default VLAN Settings

You can configure switch ports to transmit frames tagged on some VLANs and untagged on other VLANs.

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

In the following figure, untagged incoming packets are assigned directly to VLAN 2 (PVID = 2). Port 5 is as a *tagged* member of VLAN 2, and port 7 is an *untagged* member of VLAN 2.

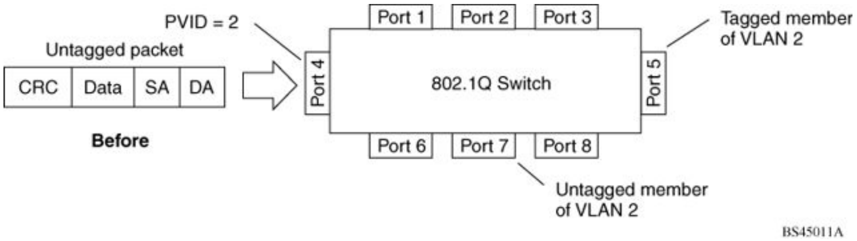


Figure 3: Port-based VLAN assignment

Figure 4: 802.1Q tagging (after port-based VLAN assignment) on page 26 shows the untagged packet is marked (tagged) as it leaves the switch through port 5, which is a tagged member of VLAN 2. The untagged packet remains unchanged as it leaves the switch through port 7, which is an untagged member of VLAN 2.

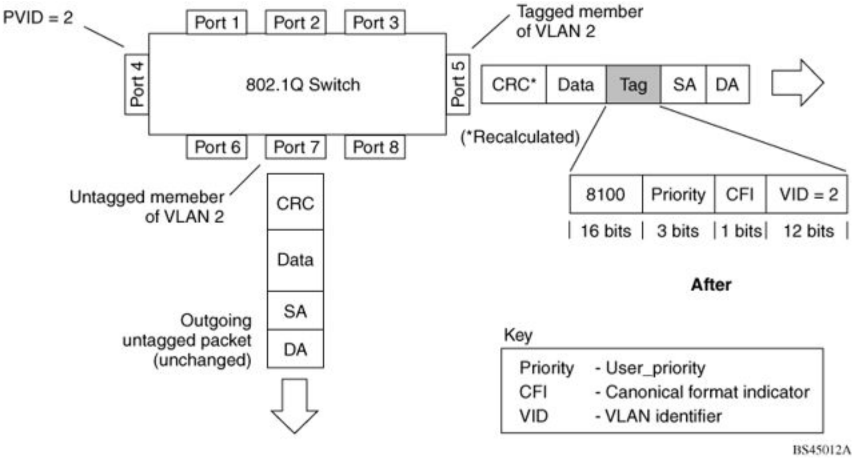


Figure 4: 802.1Q tagging (after port-based VLAN assignment)

In the following figure, untagged incoming packets are assigned to VLAN 3 (policy VLAN = 3, PVID = 2). Port 5 is a tagged member of VLAN 3, and port 7 is an untagged member of VLAN 3.

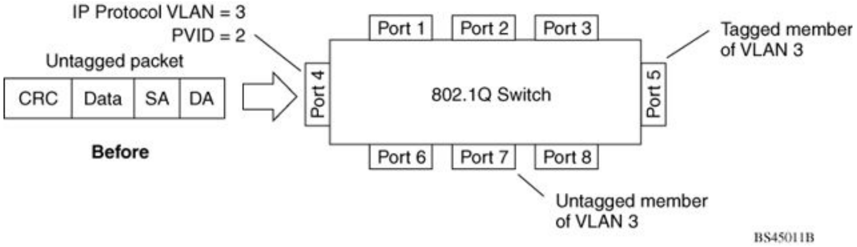


Figure 5: Policy-based VLAN assignment

Figure 6: 802.1Q tagging (after policy-based VLAN assignment) on page 26, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is a tagged member of VLAN 3. The untagged packet remains unchanged as it leaves the switch through port 7, which is an untagged member of VLAN 3.

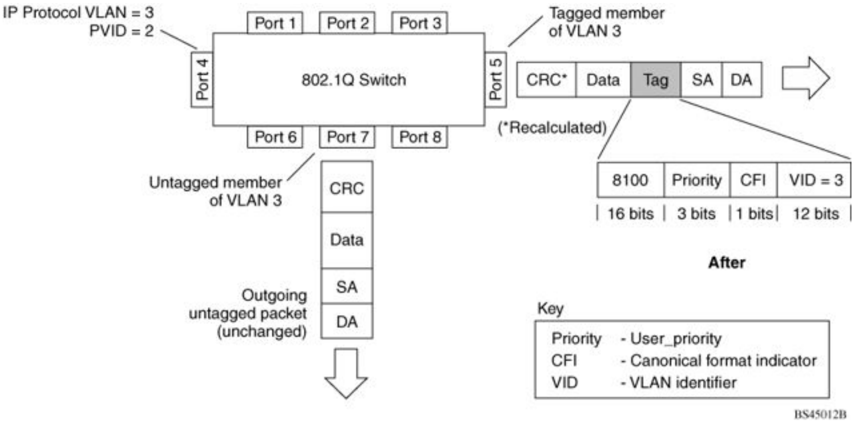


Figure 6: 802.1Q tagging (after policy-based VLAN assignment)

In the following figure, tagged incoming packets are assigned directly to VLAN 2 because of the tag assignment in the packet. Port 5 is a tagged member of VLAN 2, and port 7 is an untagged member of VLAN 2.

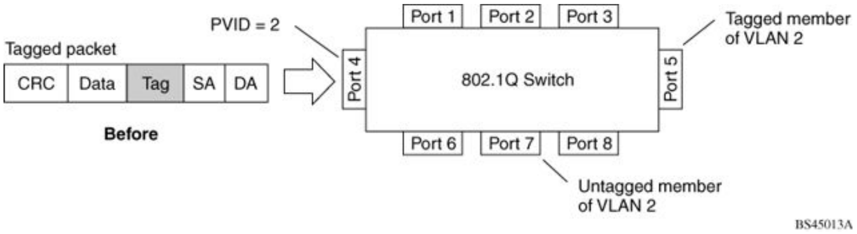


Figure 7: 802.1Q tag assignment

Figure 8: 802.1Q tagging (after 32-bit 802.1Q tag assignment) on page 27 show the tagged packet remains unchanged as it leaves the switch through port 5, which as a tagged member of VLAN 2. However, the tagged packet is stripped (untagged) as it leaves the switch through port 7, which is an untagged member of VLAN 2.

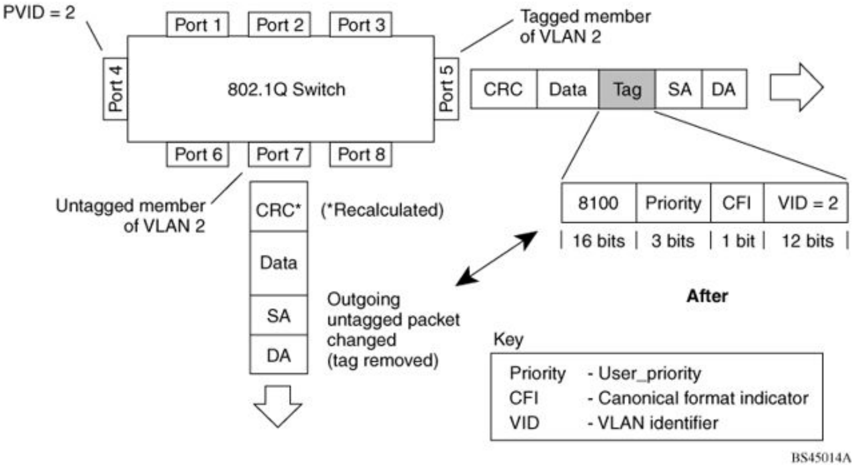


Figure 8: 802.1Q tagging (after 32-bit 802.1Q tag assignment)

In the following figure, untagged incoming packets are assigned directly to a PVID of 2. Port 5 is a tagged member of PVID 2, and port 7 is an untagged member of PVID 2.

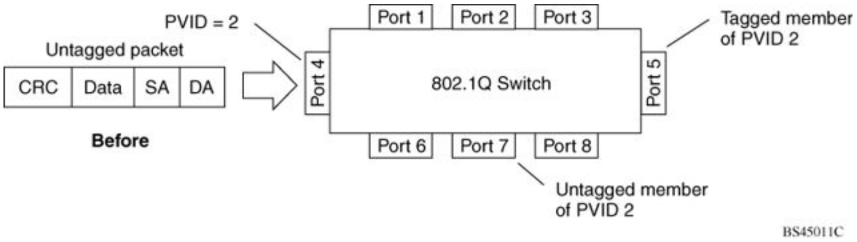


Figure 9: 802.1Q tag assignment

As shown in the following figure, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is a tagged member of PVID 2. The untagged packet remains unchanged as it leaves the switch through port 7, which is an untagged member of PVID 2.

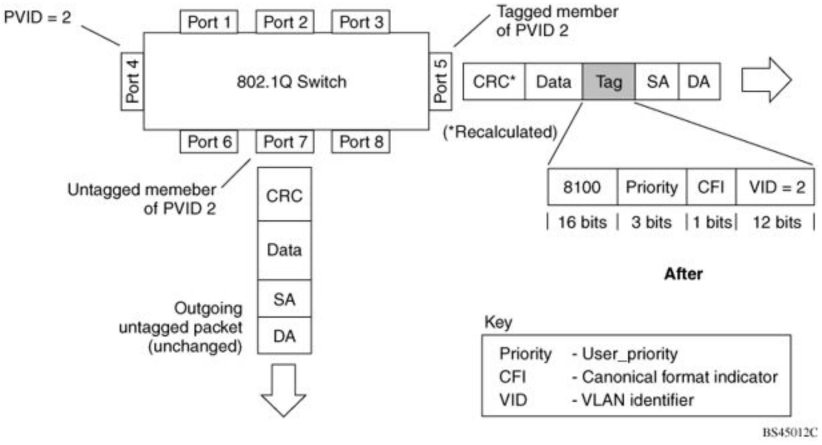


Figure 10: 802.1Q tagging (after 30-bit 802.1Q tag assignment)

VLANs Spanning Multiple Switches

You can use VLANs to segment a network within a switch. For multiple connected switches, 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. You can assign switch ports 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

The following figure shows VLANs spanning two Avaya Ethernet Routing Switch 4000 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.

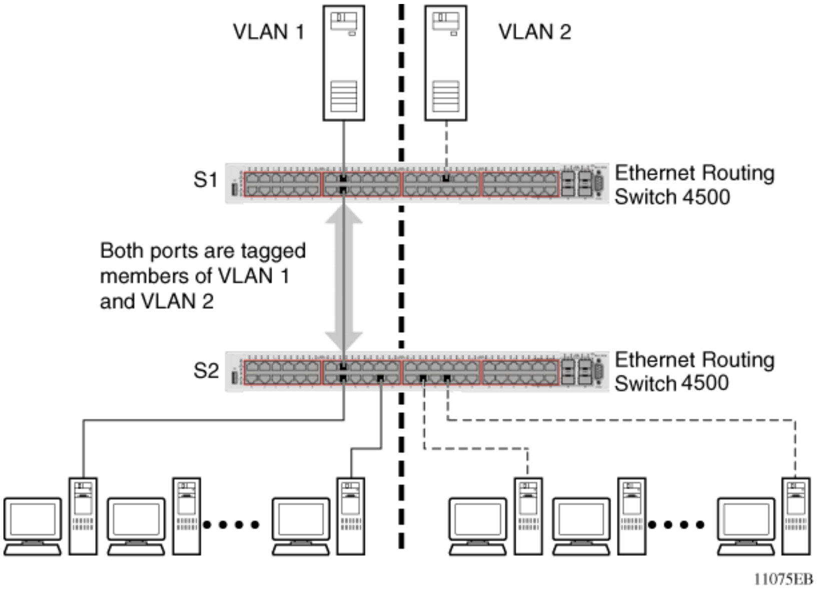

VLAN 1
VLAN 2
S1
Ethernet Routing Switch 4500
Both ports are tagged members of VLAN 1 and VLAN 2
S2
Ethernet Routing Switch 4500
11075EB

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 it treats 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

The following figure 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).

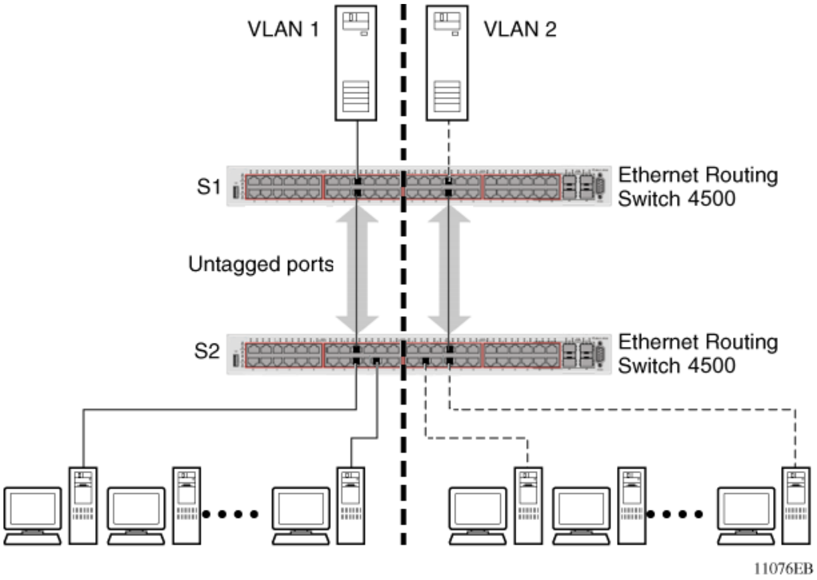


Figure 12: VLANs spanning multiple untagged switches

When you enable the STP 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 you configure 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 30shows possible consequences of enabling the STP when you use VLANs between untagged (non-802.1Q tagged) switches.

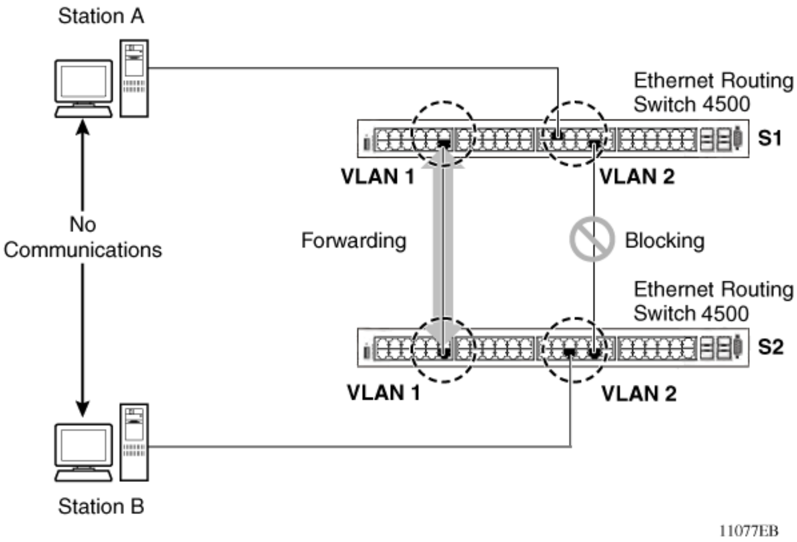


Figure 13: Possible problems with VLANs and Spanning Tree Protocol

As shown in the preceding figure, with STP enabled, only one connection between Switch S1 and Switch S2 forwards traffic at any time. Communication fails between VLAN 2 of S1 and VLAN 2 of S2, blocking communications between Stations A and B.

The STP selects the link that connects VLAN 1 on Switches S1 and S2 as the forwarding link based on port speed, duplex-mode, and port priority. Because the other link that connects 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 forwards traffic.

VLAN Summary

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

Figure 14: VLAN configuration spanning multiple switches on page 32 shows Switch S1 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, you must use a single switch port on each switch for each VLAN (see Figure 12: VLANs spanning multiple untagged switches on page 30).

The connection to S2 requires only one link between the switches because S1 and S2 are both Avaya Ethernet Routing Switch 4000 Series switches that support 32-bit 802.1Q tagging (see VLANs spanning multiple 802.1Q tagged switches on page 28).

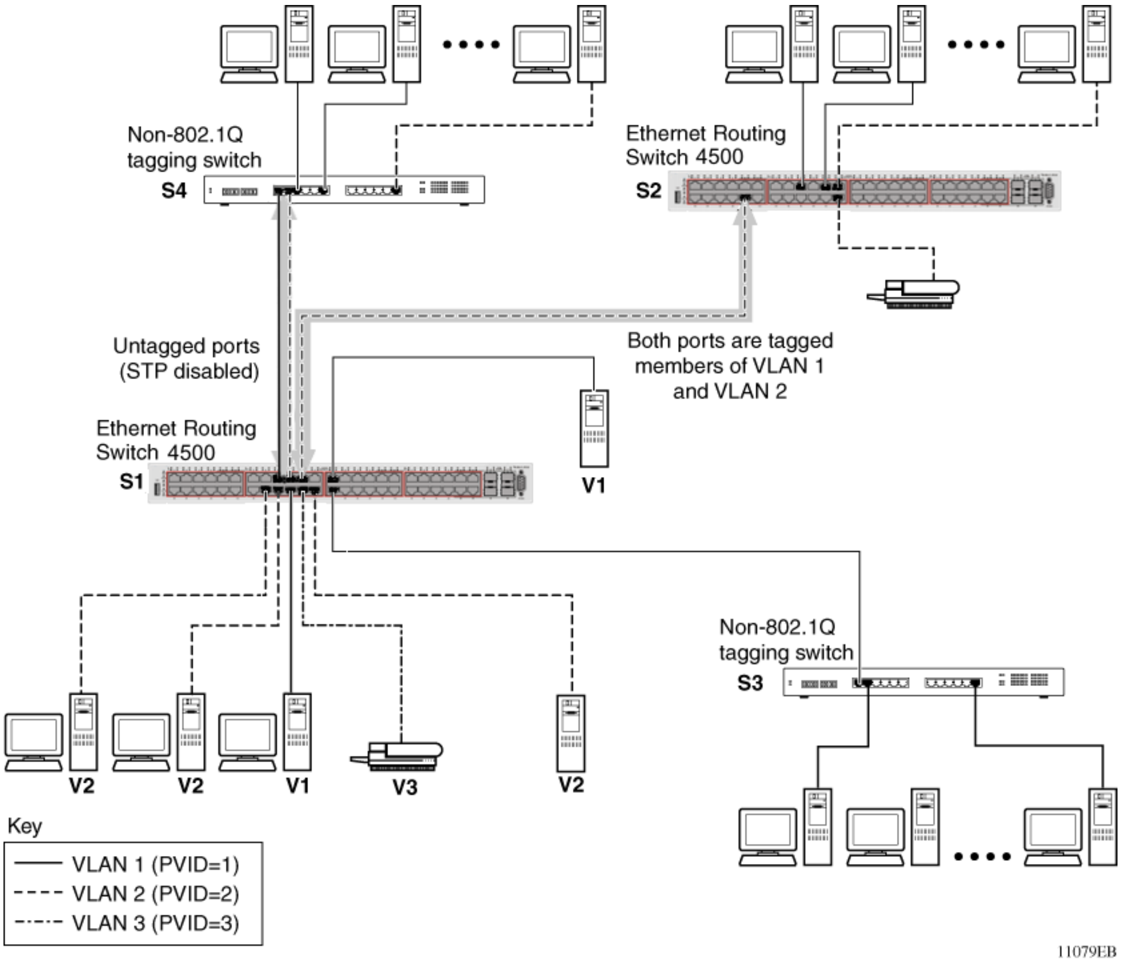


Figure 14: VLAN configuration spanning multiple switches

VLAN Configuration Rules

VLANs operate according to specific configuration rules. When you create 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 to or deleted from the VLAN.
- All ports involved in trunking must have the same VLAN configuration.
- VLANs do not depend on Rate Limiting settings.
- If a port is an Internet Gateway Management Protocol (IGMP) member on any VLAN, and you remove the port from a VLAN, the port IGMP membership is also removed.
- If you add a static router port to a different VLAN, you can configure the port as an IGMP member on that specific VLAN.

Important:

If you tag protocol VLAN client ports, the system cannot assign frames to the protocol VLAN, regardless of the defined ethertype. Frames are not assigned to the protocol VLAN because untagged packets will be assigned to the VLAN identified by the port PVID.

VLAN Configuration Control

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

VLAN Configuration Control offers four options to control VLAN modification:

- **Strict**: Restrict 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.

  Important:

  '**Strict**' is the factory default setting.
- **Automatic**: Automatically add an untagged port to a new VLAN and automatically remove it from any previous VLAN membership. The PVID of the port automatically changes to the VID of the VLAN it joins. Because you first add the port to the new VLAN and then remove it from any previous membership, the Spanning Tree Group participation of the port remains enabled as long as the VLANs involved are in the same Spanning Tree Group.
- **AutoPVID**: This option functions in the same manner as previous AutoPVID functionality. When you add an untagged port to a new VLAN, you add the port to the new VLAN and the PVID assigned to the new VID without removing it from previous VLAN memberships. Using this option, an untagged port can have membership in multiple VLANs.
- **Flexible**: This option functions in a similar manner to disabling AutoPVID functionality. When you use this option, 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 applies only to ports with the tagging modes of **Untag All** and **Tag PVID Only**. VCC does not govern ports with the tagging modes of **Tag All** and **Untag PVID Only**. Ports with the tagging modes of **Tag All** and **Untag PVID Only** can belong to multiple VLANs regardless of VLAN Configuration Control settings and you must manually change their PVID.

Disable MAC Learning

When you use Disable MAC Learning you can disable MAC address learning on specified ports.

Disable MAC Learning is useful in situations where you want to control the Layer 2 Forwarding Database (FDB) entries. For example: when you deploy the switch in metro environments, nodes on the network may flood traffic, and the MAC tables can fill rapidly. Disable MAC Learning gives you control over MAC learning to prevent the MAC tables from filling unnecessarily in a situation like this.

You cannot control the learning behavior for ports per VLAN due to hardware limitations.

You use Disable MAC Learning in combination with the Static MAC FDB Entry feature when you want to add a certain MAC address in the MAC address table, by adding it statically using Static MAC FDB Entry. Disable MAC Learning interacts with Layer 2 applications including MAC Security, NEAP clients authenticated by RADIUS, and ADAC.

Following are examples of feature function if you do not use Static MAC FDB entry with Disable MAC Learning.

For ADAC, when you disable MAC learning, the telephone MAC is not learned and the system does not perform auto configuration.

If you enable auto learning for MAC Security on ports and disable learning with Disable MAC Learning, MAC addresses do not populate the MAC Security address table.

When you use Disable MAC Learning on ports, the system cannot authenticate NEAP clients authenticated by RADIUS that connect through those ports.

If a packet contains the MAC address destination of a device connected to the switch on a port where learning is disabled, the system duplicates the packets on all other ports and ARP continues to function.

However, if you use Static MAC FDB Entry to insert addresses the features function as expected, except for ADAC : when you disable MAC learning on the port in which the telephone is inserted, the system will not perform auto configuration by adding a static MAC address.

You cannot disable learning on a single port that is part of a MLT/DMLT/LAG trunk. You must have MAC learning disabled on all ports in that trunk. For doing this, it is enough to disable MAC learning on a port that is a member of the MLT/DMLT/LAG trunk, and the other ports that are members of the same MLT/DMLT/LAG trunk will instantly have MAC learning disabled on them. You cannot create a trunk that includes only one port with learning disabled.

Static FDB MAC Entry

The forwarding database (FDB) contains information that maps the MAC address of each known device to the switch port where the device address was learned.

When you use the Static FDB MAC Entry feature you can configure static MAC address entries in the FDB (the MAC address table). Once you configure a static MAC address entry in the FDB, the static MAC address does not age out like a dynamically learned address. A static address from the FDB is a unicast address and the system does not erase it after switch resets or when link-down events occur.

You can configure up to 1,024 static MAC addresses in the FDB.

Static FDB MAC Entry works in conjunction with the Disable MAC Learning feature.

Static MAC address entries display the following behavior:

- Remain in NVRAM after switch reset.
- Propagate across the stack during database exchange.
- When you remove a unit from the stack, the static MAC address table entries for the ports belonging to that unit are no longer available for the stack, and the traffic for that static MAC address floods. When the unit rejoins the stack, the system repopulates the MAC address table for the stack and forwards traffic normally.
- When you join two or more units to a stack, if the total number of the static addresses from all the units is greater than the max number, the system retains only the static addresses from the base unit (BU) and removes the addresses from the non-base unit (NBU).
- The static MAC addresses are saved into the ASCII configuration file.
- If the MAC address table is full or the maximum number of static MAC addresses is reached, you cannot insert any more static addresses in the MAC address table until you clear some static addresses.
- If you insert a static MAC address in the MAC address table for a port and the device is not plugged into that port, the switch does not flood the traffic for that MAC address to other ports, and the system drops the packets.
- You cannot delete a VLAN while static addresses for that VLAN remain in the system.
- You cannot remove a port from a VLAN when static addresses exist for the pair (VLAN, port).

You can insert static MAC addresses for both a port and a trunk. However, the following limitations apply when you add static addresses for a trunk:

- You cannot add a static address for a port if the port is part of a trunk.
- You cannot add a port to a trunk if static addresses for that port exist in the MAC address table.
- You cannot erase or disable a trunk if static addresses for that trunk exist in the MAC address table.
- If you insert a static address for a LAG trunk, when the LAG trunk disaggregates, the system erases the address and inserts a system log.
- If you insert a static address for a LAG trunk; the system does not save that static address in the ASCII configuration file.
- If you insert a static address for a LAG trunk, the system does not save the address in NVRAM, and therefore these entries are not restored after a switch reset

Important:

Avaya recommends that you do not use Disable MAC Learning and Static FDB MAC Entry features in conjunction with ADAC, EAP, MAC Security or L3. However, if you choose to use these features together, you are advised to configure the other applications (ADAC, EAP, MAC Security, or L3) prior to the insertion of the static address. If you configure one of these applications (ADAC, EAP, MAC Security, or L3) after you insert the static address, the application will not be informed of the existence of that particular address, so the device with the address will be unknown to the application.

FDB Entry Scenarios

If the system dynamically learns a MAC address on a port or trunk that is a member of a VLAN, and you manually insert that MAC address into the MAC address table, one of the following applies:

- If the existing dynamic entry matches the static information (same port, trunk and VLAN information), the system modifies the entry to a static one.
- If the existing dynamic entry matches the VLAN information with a different port or trunk, the system erases the dynamic entry and inserts the new static one with the changed port or trunk.
- If the existing dynamic entry matches the port or trunk information with a different VLAN, the system maintains the existing entry and inserts a new static entry.
- If the existing dynamic entry differs in VLAN, port, and trunk information, the system maintains the existing entry and inserts a new static entry.

If you insert a static MAC address in the MAC address table on a port or trunk that is a member of a VLAN, and subsequently you insert a static entry for the same MAC address:

- On another port or trunk but on the same VLAN, the system migrates the static address to the new port or trunk.
- On a different VLAN, the system inserts a static entry for the new pair (VLAN, port or trunk).

If you insert a static MAC address in the MAC address table for a port or trunk that is a member of a VLAN, and subsequently the system receives a packet with the same MAC address:

- On another port or trunk but the same VLAN, the system does not dynamically learn the address and drops the packet. The static MAC address has priority over any dynamically learned addresses.
- On another or the same port or trunk but on a different VLAN, the system dynamically inserts an entry for the new pair (VLAN, port or trunk)

MAC Flush

You can use the MAC Flush feature to clear MAC Address entries directly from the MAC Address Table (or Forwarding Data Base). For dynamically learned addresses, if you do not use the MAC Flush feature, you can use the following indirect methods:

- power cycling the switch
- deleting, and then recreating the VLAN
- unplugging, and then replugging the port to flush out all addresses learned on the port

MAC Flush provides the following options to flush out MAC Address entries:

- clear a single MAC Address
- clear all MAC addresses from a port (or list of ports)
- clear all MAC addresses from a trunk (MLT or LAG)
- clear all MAC addresses from a particular VLAN
- clear only dynamic or only static addresses from a port
- clear only dynamic or only static addresses from a VLAN
- clear only dynamic or only static addresses from a trunk
- clear all static addresses
- clear all dynamic addresses
- clear all MAC addresses

MAC Flush clears only dynamically learned or statically entered MAC Addresses. MAC Flush does not delete MAC Addresses created by MAC Security or Port Mirroring because deletion of these MAC Addresses can affect the MAC Security or Port Mirroring function.

MAC Addresses for MAC Security or Port Mirroring have one of the following identifiers:

- AGELOCK
- SECRET
- STATIC

Higher priority tasks can delay MAC Address clearing.

You can configure MAC Flush in ACLI, SNMP, and Enterprise Device Manager.

Voice VLAN Integration

Voice VLAN is enhanced to provide centralized creation and management of Voice VLAN using VLAN-specific commands. The enhancement also includes the option to configure a statically allocated port that you can permanently assign to the Voice VLAN, where that port will still persist after a system boot. Another advantage of a statically allocated port is that it does not have to participate in the ADAC or 802.1AB discovery processes, when this behavior is desired. With Voice VLAN Integration, the switch creates static Voice VLANs and Layer 3 configurations can be applied as per standard operational procedures. Voice VLAN integration is specifically useful when Layer 3 configurations are needed for ADAC Voice VLAN.

When an application such as ADAC, EAP or LLDP requires a Voice VLAN, you need to create the Voice VLAN with the new VLAN commands before configuring this Voice VLAN in the required application. An error message is displayed if the VLAN ID does not exist or is not configured as a Voice VLAN.

When you delete a Voice VLAN, the system ensures it is not used by any of the dependent applications before proceeding with the deletion. An error message is displayed if the Voice VLAN is in use.

Note:

Avaya recommends you do not use the same Voice VLAN for different features.

You can configure up to 6 Voice VLANs.

MLT/DMLT/LAG Dynamic VLAN changes

Enhancements are made to Link Aggregation Groups (LAG) to provide consistent operation of Multi-Link Trunk (MLT), Distributed Multi-Link Trunk (DMLT), and LAGs so that you can make VLAN changes on trunks without disabling the trunk first.

The switch allows you to move a LAG member into a VLAN and all ports that have LACP enabled with the same LACP key will be moved. This behavior is similar to MLT and DMLT.

If you attempt to remove all VLANs from an active MLT/DMLT/LAG, the system outputs a message warning you of possible loss of connectivity to the switch, and requests a confirmation to continue. If you remove all MLT/DMLT/LAG ports from all VLANs, the trunk is disabled. The following warning message appears when you remove all the VLANs from an active MLT/DMLT/LAG:

```
Warning: you are about to remove all VLANs from the active trunk
group, doing so could cause loss of connectivity to the switch. Are
you sure you want to continue <Y/N>?
```

This message does not appear if there is one VLAN and multiple VLANs are removed on the port.

When you add a port to a new STG, you should consider using STG port membership in auto mode, so that STP will be automatically enabled on that port to prevent loops.

IGMP snooping on a VLAN Configuration

If at least one host on a VLAN specifies that it is a member of a group, by default, the Avaya Ethernet Routing Switch 4000 Series forwards to that VLAN all datagrams bearing the multicast address of that group. All ports on the VLAN receive the traffic for that group.

The following figure shows an example of this scenario. Here, the IGMP source provides an IP Multicast stream to a designated router. Because the local network contains receivers, the designated router forwards the IP Multicast stream to the network. Switches without IGMP snoop enabled flood the IP Multicast traffic to all segments on the local subnet. The receivers requesting the traffic receive the desired stream, but so do all other hosts on the network. Although the nonparticipating end stations can filter the IP Multicast traffic, the IP Multicast traffic still exists on the subnet and consumes bandwidth.

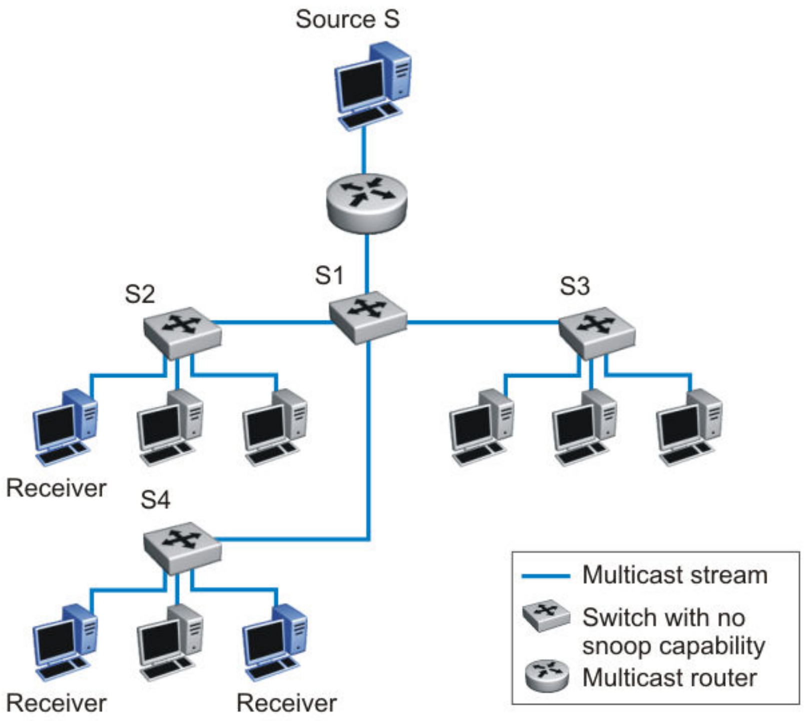


Figure 15: IP multicast propagation on a LAN without IGMP snooping

To prune ports that are not group members from receiving the group data, the Avaya Ethernet Routing Switch 4000 Series supports IGMP snoop for IGMPv1 and IGMPv2. With IGMP snoop enabled on a VLAN, the switch forwards the multicast group data to only those ports that are members of the group. When using IGMP snoop, VLANs can provide the same benefit as IP Multicast routers, but in the local area.

The Avaya Ethernet Routing Switch 4000 identifies multicast group members by listening to IGMP packets (IGMP reports, leaves, and queries) from each port. The switch suppresses the reports by not forwarding them out to other VLAN ports, forcing the members to continuously send their own reports. The switch uses the information gathered from the reports to build a list of group members. After the group members are identified, the switch blocks the IP Multicast stream from exiting any port that does not connect to a group member, thus conserving bandwidth.

As shown in the following figure, after the switches learn which ports are requesting access to the IP Multicast stream, all other ports not responding to the queries are blocked from receiving the IP Multicast data.

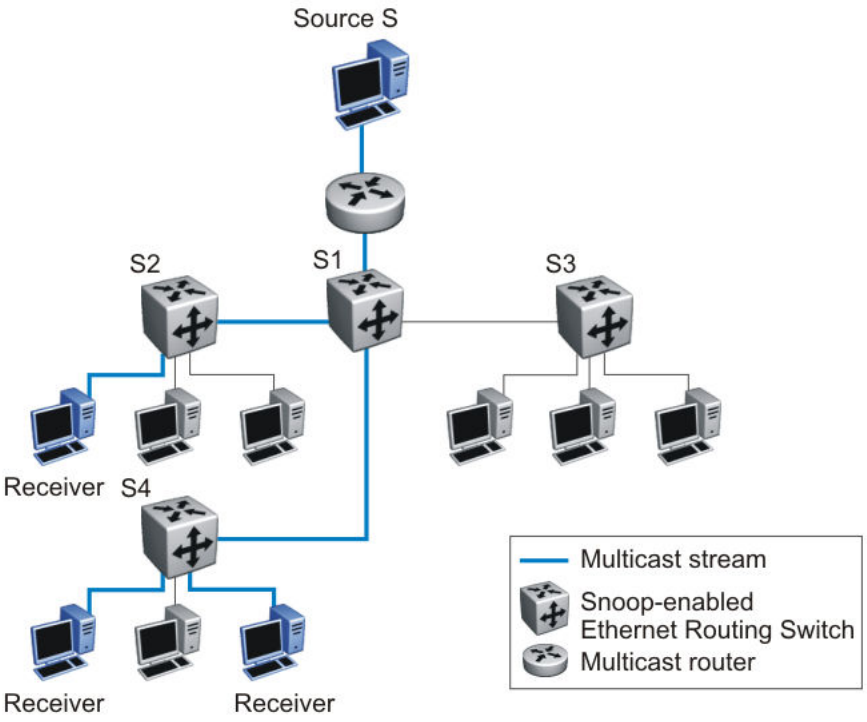


Figure 16: Ethernet Routing Switch running IGMP snooping

The switch continues to forward the IGMP membership reports from the hosts to the multicast routers, and also forwards queries from multicast routers to all port members of the VLAN.

Chapter 4: MLT Fundamentals

MultiLink trunks

With MultiLink trunks, you can group a maximum of 8 switch ports to form a link to another switch or server, thus increasing aggregate throughput of the interconnection between the devices (up to 8 Gigabits if using Gigabit ports or 80 Gigabits if using 10 Gigabit ports). You can configure a maximum of 32 MultiLink trunks. The trunk members can reside on a single unit or on multiple units within the same stack configuration as a distributed trunk. MultiLink Trunking software detects the links that are down or broken and redirects traffic that used to flow on these links to other remaining active links.

You can use the Command Line Interface (ACLI) or Enterprise Device Manager (EDM) to create switch-to-switch and switch-to-server MultiLink trunk links.

Client-server configuration using MultiLink trunks

Figure 17: Client/server configuration example on page 43 shows an example of how you can use MultiLink Trunking 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.

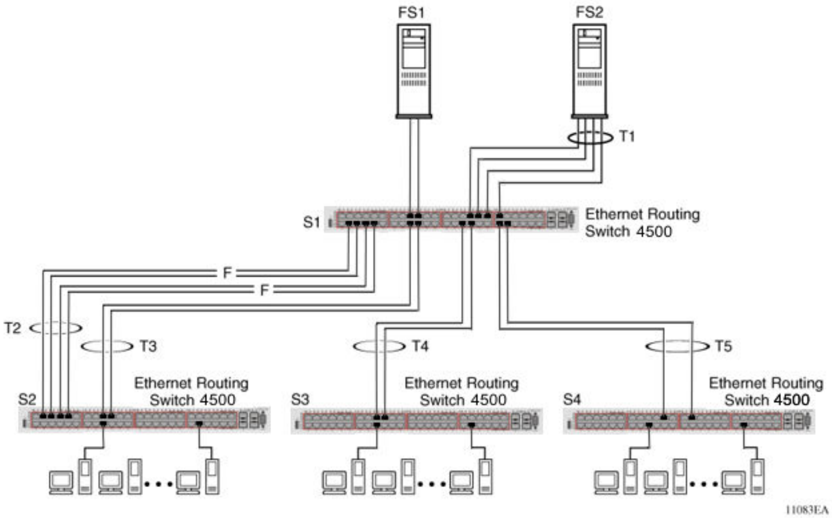

FS1
FS2
T1
S1
Ethernet Routing Switch 4500
F
F
T2
T3
T4
T5
S2
Ethernet Routing Switch 4500
S3
Ethernet Routing Switch 4500
S4
Ethernet Routing Switch 4500
11083EA

Figure 17: Client/server configuration example

Clients who access data from the servers (FS1 and FS2) use maximum bandwidth through trunks T1, T2, T3, T4, and T5. Trunk members (the ports that make up each trunk) need not be consecutive switch ports; ports can be selected randomly, as shown by T5.

With spanning tree enabled, one trunk (T2 or T3) acts as a redundant (backup) trunk to Switch S2. With spanning tree disabled, you must configure trunks T2 and T3 into separate VLANs for this configuration to function properly.

Before Trunks are Configured

When you create and enable a trunk, the trunk members (switch ports) take on certain settings necessary for the correct operation of the MultiLink Trunking feature.

Before you configure a MultiLink trunk, consider the following settings and specific configuration rules:

1. Read the configuration rules provided in the following section.
2. Determine which switch ports (up to eight) are to become trunk members (the specific ports that make up the trunk). Each trunk requires a minimum of two ports.

   ❗ **Important:**

   Disabled ports can belong to MLTs. For traffic to flow to your configured MLT ports, be sure you enable them.
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 you configure any trunks.

   ❗ **Important:**

   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 reacts to the new trunk configuration.

   ❗ **Important:**

   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 the addition of a trunk will affect existing VLANs.

MultiLink Trunking Configuration Rules

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

- Disabled ports can belong to MLTs. For traffic to flow to your configured MLT ports, be sure that you enable them (enable ports using the 'no shutdown' command in ACLI in interface mode).
- All trunk members must have the same VLAN configuration before you enable the trunk using the 'mlt <id> enable' ACLI command.
- When you configure an active port in a trunk, the port becomes a trunk member when the Trunk Status field is Enabled. The spanning tree parameters for the port then change to reflect the new trunk settings.
- If you change the spanning tree participation of any trunk member to Enabled or Disabled, the spanning tree participation of all members of that trunk changes similarly.
- If you change the VLAN settings of any trunk member, the VLAN settings of all members of that trunk change similarly.
- A MLT/DMLT/LAG member can not be configured as a monitor port.
- 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 participate in different STGs. They must have the same spanning tree learning in every group but not necessarily the same learning between different groups to consistently update their state in the port driver.
- Like normal ports, MLT ports can 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

The Avaya Ethernet Routing Switch 4000 supports two modes of MLT load-balancing: Basic for layer 2 operation and Advanced for Layer 3 operation. You can configure this option using the **`mlt <1-32> loadbalance`** ACLI command. You can also use the **`show mlt hash-calc`** ACLI command to display the MLT hashing for a particular MAC source and destination address (loadbalance Basic) or IP source and destination address (loadbalance Advance).

For broadcast and unknown unicast, traffic is forwarded through the DLF (Destination Lookup Failure) link based on the active trunk configuration. The DLF link is the lowest member of an active trunk group.

If the advanced load balancing mode is selected for non-IP packets, load balancing falls back to MAC-Based.

MLT Enable or Disable Whole Trunk

The MLT Enable or Disable Whole Trunk feature is user-configurable switch-wide. The feature is in a disabled state by default. When you enable or disable MLT or DMLT groups, the operational state of the links that make up the bundle are not changed by default. When you disable MLT or DMLT groups, a traffic loop within a network can occur. The Avaya Ethernet Routing Switch 4000 supports the ability to change this operational mode using the MLT Enable or Disable Whole Trunk capability.

If you enable the MLT Enable or Disable Whole Trunk functionality, the underlying state of the port changes to reflect the state of the MLT or DMLT bundle irrespective of their previous status. Similarly, if you disable the MLT or DMLT then all links that are part of the MLT group are disabled except the Destination Lookup Failure (DLF) link. The DLF link is typically the lowest numbered active port of a MLT or DMLT link.

You can enable or disable individual links of a MLT or DMLT when you enable the MLT Enable or Disable Whole Trunk functionality.

❗ **Important:**

For network configuration, Avaya recommends that you set the MLT Enable or Disable Whole Trunk functionality to enabled.

Trunk members behavior when disabling MLT

If you disable any MLT or DMLT trunk member, the member is not removed from the MLT or DMLT group. The port remains a member of the MLT or DMLT group until it is removed from configuration.

Add and delete links from existing MultiLink trunks

You cannot add or remove ports from an Avaya Ethernet Routing Switch 4000 Series switch MLT, unless you first disable MLT. If you have disabled Whole Trunk functionality then you should be aware that disabling MLT does not disable the ports assigned to the MLT. If the MLT is disabled while having Whole Trunk functionality disabled, the ports of the disabled MLT could create a network loop, depending on other network configurations (for example, Spanning-Tree learning is disabled).

How a MultiLink trunk reacts to losing distributed trunk members

A MultiLink trunk (see Figure 18: Loss of distributed trunk member on page 47) 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.

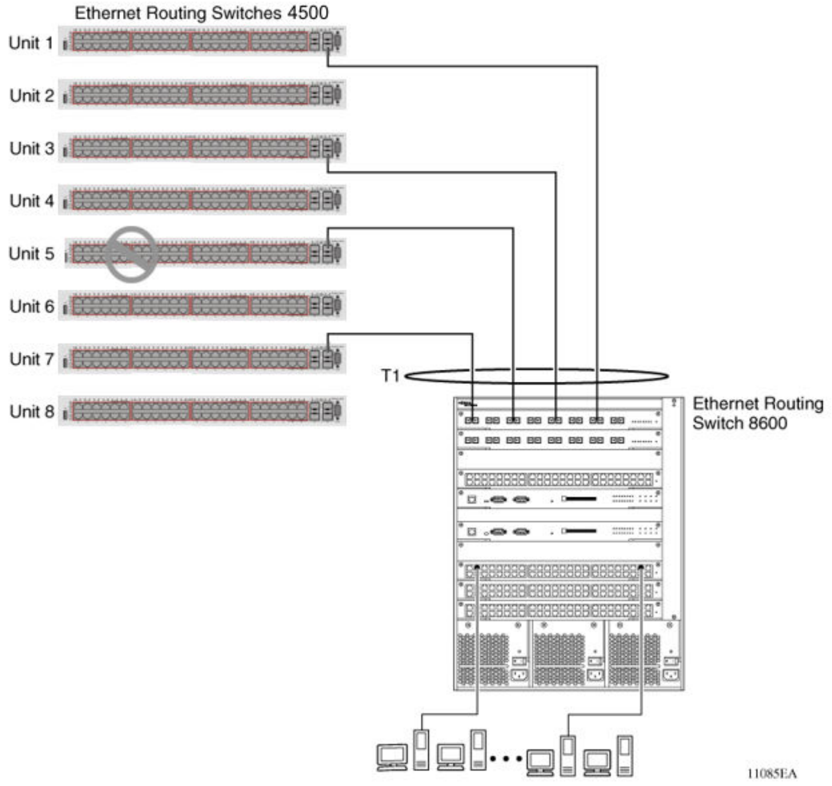


Figure 18: Loss of distributed trunk member

However, until you correct the cause of the failure or change the trunk Status field to Disabled, you cannot modify any of the following parameters for the affected trunk.

- spanning tree configuration
- Port configuration
- IGMP configuration

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

Spanning Tree Considerations for MultiLink trunks

The spanning tree Path Cost parameter is recalculated based on the aggregate bandwidth of the trunk. For example, Figure 19: Path Cost Arbitration on page 48 shows a two-port trunk

(T1) with two port members that operate at an aggregate bandwidth of 2 GB, with a comparable Path Cost of 1. Trunk 2 has two ports at 100 Mb/s with a Path Cost of 5.

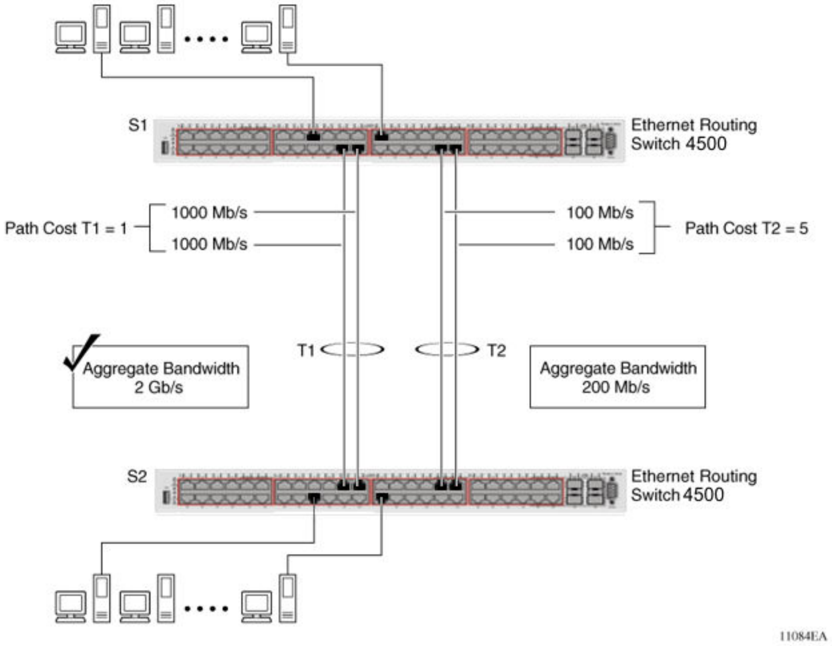

S1
Ethernet Routing Switch 4500
Path Cost T1 = 1
1000 Mb/s
1000 Mb/s
100 Mb/s
100 Mb/s
Path Cost T2 = 5
✓ Aggregate Bandwidth 2 Gb/s
T1
T2
Aggregate Bandwidth 200 Mb/s
S2
Ethernet Routing Switch 4500
11084EA

Figure 19: Path Cost Arbitration

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

Important:

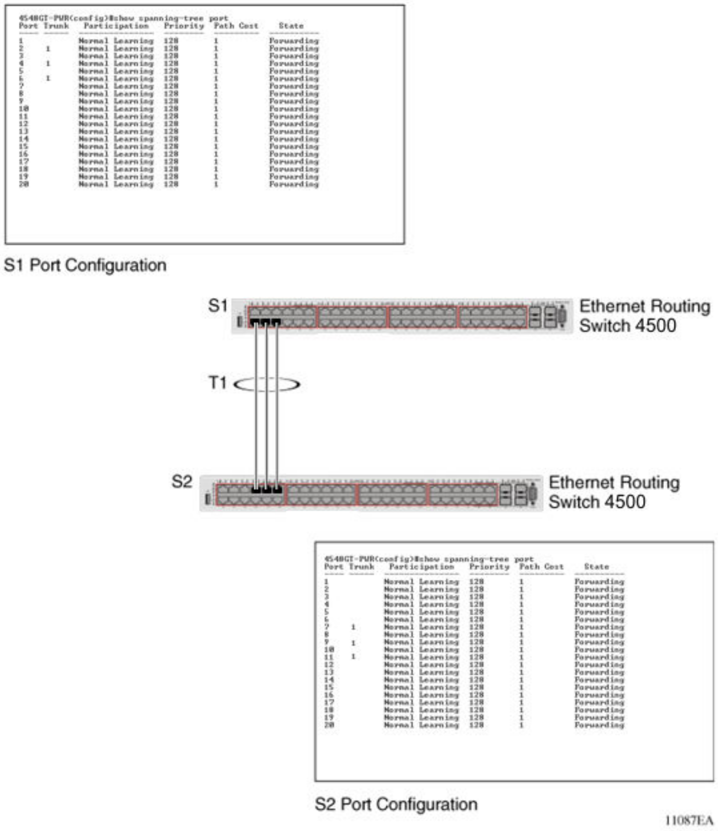
The default spanning tree Path Cost for all gigabit ports is always equal to 1.

When configuring trunks, be aware that when adding a one-gigabit link in front of another trunk, the trunk becomes blocked because both the link and trunks have a Path Cost of 1.

Note:

It is recommended to use 802.1t mode if using 10 Gigabit links and other switches in the network support 802.1t.

The switch can detect trunk member ports that are physically misconfigured. For example, Figure 20: Correctly Configured Trunk on page 49 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 `show spanning-tree port` command output for each switch shows the port state field for each port in the Forwarding state.



```
4548GT-PWR(config)#show spanning-tree port
Port Trunk   Participation    Priority  Path Cost    State
----- -----  ---------------  --------  ---------    ----------
1            Normal Learning  128       1            Forwarding
2     1      Normal Learning  128       1            Forwarding
3            Normal Learning  128       1            Forwarding
4     1      Normal Learning  128       1            Forwarding
5            Normal Learning  128       1            Forwarding
6     1      Normal Learning  128       1            Forwarding
7            Normal Learning  128       1            Forwarding
8            Normal Learning  128       1            Forwarding
9            Normal Learning  128       1            Forwarding
10           Normal Learning  128       1            Forwarding
11           Normal Learning  128       1            Forwarding
12           Normal Learning  128       1            Forwarding
13           Normal Learning  128       1            Forwarding
14           Normal Learning  128       1            Forwarding
15           Normal Learning  128       1            Forwarding
16           Normal Learning  128       1            Forwarding
17           Normal Learning  128       1            Forwarding
18           Normal Learning  128       1            Forwarding
19           Normal Learning  128       1            Forwarding
20           Normal Learning  128       1            Forwarding
```

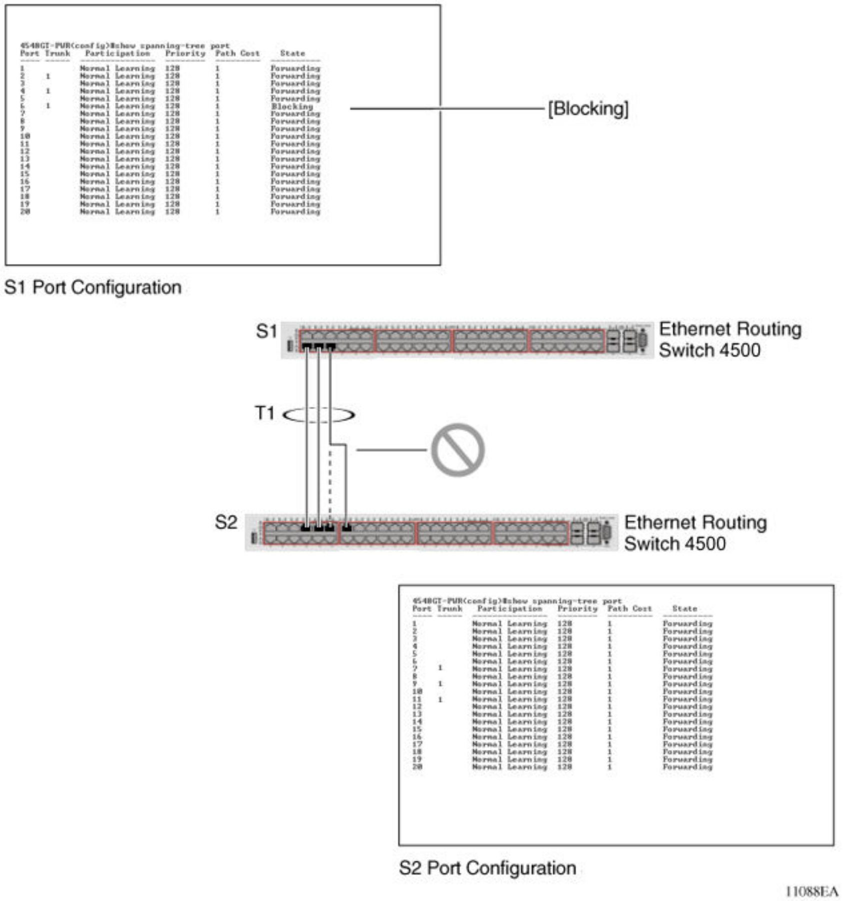
```
4548GT-PWR(config)#show spanning-tree port
Port Trunk   Participation    Priority  Path Cost    State
----- -----  ---------------  --------  ---------    ----------
1            Normal Learning  128       1            Forwarding
2            Normal Learning  128       1            Forwarding
3            Normal Learning  128       1            Forwarding
4            Normal Learning  128       1            Forwarding
5            Normal Learning  128       1            Forwarding
6            Normal Learning  128       1            Forwarding
7     1      Normal Learning  128       1            Forwarding
8            Normal Learning  128       1            Forwarding
9     1      Normal Learning  128       1            Forwarding
10           Normal Learning  128       1            Forwarding
11    1      Normal Learning  128       1            Forwarding
12           Normal Learning  128       1            Forwarding
13           Normal Learning  128       1            Forwarding
14           Normal Learning  128       1            Forwarding
15           Normal Learning  128       1            Forwarding
16           Normal Learning  128       1            Forwarding
17           Normal Learning  128       1            Forwarding
18           Normal Learning  128       1            Forwarding
19           Normal Learning  128       1            Forwarding
20           Normal Learning  128       1            Forwarding
```

Figure 20: Correctly Configured Trunk

Important:

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

If trunk member port 11 of root Switch S2 is physically disconnected and then reconnected to port 13, the **`show spanning-tree port`** command output for Switch S1 changes to show port 6 in the Blocking state, see Figure 21: Detecting a Misconfigured Port on page 50.



```
4548GT-PWR(config)#show spanning-tree port
Port Trunk   Participation    Priority  Path Cost    State
---- -----  ---------------   --------  ---------   ----------
1           Normal Learning   128       1           Forwarding
2     1     Normal Learning   128       1           Forwarding
3           Normal Learning   128       1           Forwarding
4     1     Normal Learning   128       1           Forwarding
5           Normal Learning   128       1           Forwarding
6     1     Normal Learning   128       1           Blocking
7           Normal Learning   128       1           Forwarding
8           Normal Learning   128       1           Forwarding
9           Normal Learning   128       1           Forwarding
10          Normal Learning   128       1           Forwarding
11          Normal Learning   128       1           Forwarding
12          Normal Learning   128       1           Forwarding
13          Normal Learning   128       1           Forwarding
14          Normal Learning   128       1           Forwarding
15          Normal Learning   128       1           Forwarding
16          Normal Learning   128       1           Forwarding
17          Normal Learning   128       1           Forwarding
18          Normal Learning   128       1           Forwarding
19          Normal Learning   128       1           Forwarding
20          Normal Learning   128       1           Forwarding
```

S1 Port Configuration

```
4548GT-PWR(config)#show spanning-tree port
Port Trunk   Participation    Priority  Path Cost    State
---- -----  ---------------   --------  ---------   ----------
1           Normal Learning   128       1           Forwarding
2           Normal Learning   128       1           Forwarding
3           Normal Learning   128       1           Forwarding
4           Normal Learning   128       1           Forwarding
5           Normal Learning   128       1           Forwarding
6           Normal Learning   128       1           Forwarding
7     1     Normal Learning   128       1           Forwarding
8           Normal Learning   128       1           Forwarding
9     1     Normal Learning   128       1           Forwarding
10          Normal Learning   128       1           Forwarding
11    1     Normal Learning   128       1           Forwarding
12          Normal Learning   128       1           Forwarding
13          Normal Learning   128       1           Forwarding
14          Normal Learning   128       1           Forwarding
15          Normal Learning   128       1           Forwarding
16          Normal Learning   128       1           Forwarding
17          Normal Learning   128       1           Forwarding
18          Normal Learning   128       1           Forwarding
19          Normal Learning   128       1           Forwarding
20          Normal Learning   128       1           Forwarding
```

S2 Port Configuration

Figure 21: Detecting a Misconfigured Port

Important:

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

Additional Tips About the MultiLink Trunking Feature

When you create a MultiLink trunk , 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 MultiLink Trunking, you must perform this procedure:

1. Disable the trunk.
2. Make the change.
3. Reenable the trunk.

All configured trunks are indicated with 'show spanning-tree port <port_list>" ACLI command. The Trunk field lists the active trunks that are 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.

Management stations view the trunk 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.

SLPP Guard

Because SMLT networks, by design, disable Spanning Tree (STP), Rapid Spanning Tree (RSTP), or Multiple Spanning Tree Protocol (MSTP) for participating ports, you need a method to prevent loops involving these ports.

When you use the ERS4000 in combination with other Avaya switches that support Simple Loop Protection Protocol (SLPP) and Avaya's Switch Clustering (SMLT) - for example, ERS 5000 Series or ERS 8300 - the SLPP Guard feature provides additional network loop protection.

Because the ERS4000 does not support SLPP, the switch does not generate SLPP packets on ports that have SLPP Guard enabled, but when you enable SLPP Guard on switch ports, they can receive SLPP packets. When the system receives the SLPP packet it can generate a local log message, syslog message, and SNMP traps. When you enable SLPP Guard on a switch port and the switch receives an SLPP packet on that port, SLPP Guard can immediately disable the port administratively, for a predetermined interval.

For example: ERS4000 port 1 connects to ERS8300 port 1/1, the links are configured for SMLT, and a loop is created. With SLPP enabled on port 1/1, the ERS8300 transmits SLPP packets from that port. With SLPP Guard enabled on ERS4000 port 1, when ERS 4000 port 1 receives an SLPP packet the system automatically shuts ERS 4000 port 1 down, preventing the possibility of data looping between ERS4000 port 1 and ERS8300 port 1/1. After the predetermined interval expires, SLPP Guard re-enables the port. As an option, you can configure SLPP Guard to administratively disable the port indefinitely.

Note:

You cannot enable SLPP Guard on ports that are members of MLTs, DMLTs, LACPs, or LAGs.

Chapter 5: STP Fundamentals

Spanning Tree Protocol groups

The Avaya Ethernet Routing Switch 4000 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 activate another path, thus sustaining network operations.

The Avaya Ethernet Routing Switch 4000 Series supports multiple spanning tree groups (STG). The Avaya Ethernet Routing Switch 4000 Series supports a maximum of eight STGs, either all in one stand-alone switch or across a stack. Multiple STGs provide multiple data paths, which can be used for load-sharing and redundancy. Enable load sharing 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 you must independently configure each STG.

The STG, or bridge group, forms a loop-free topology that includes one or more virtual LANs (VLAN). The Avaya Ethernet Routing Switch 4000 Series supports multiple instances (eight) of STGs that run simultaneously.

The Avaya Ethernet Routing Switch 4000 Series supports a maximum of 1,024 VLANs. With a maximum of 8 STGs, on average, each STG can have 128 VLANs.

In the default configuration of the Avaya Ethernet Routing Switch 4000 Series, a single STG with the ID of 1 includes all ports on the switch. This STG is the default STG. Although you can add ports or delete ports from the default STG, you cannot delete the default STG (STG1) itself 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 only untagged BPDUs to operate with all devices that support only one instance of STP. (By default, STG2 through STG8 are tagged.) The tagging setting for each STG is user-configurable.

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

You must create all other STGs, except the Default STG. To become active, you must create a non-default STG, add at least one VLAN to this STG, and then enable the STG. Each STG is assigned an ID number from 2 to 8 (the Default STG is assigned the ID number 1). You can assign a management VLAN only to an active STG. A port that is not a member of a VLAN cannot join an STG.

When you create an STG, all ports that belong to any assigned VLAN are automatically added to the STG.

Disable and delete an STG when you no longer need 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.

> **Important:**
>
> When configuring a unique multicast address for an STG, each device in that STG must be configured with the same spanning tree multicast address.

STG Configuration Guidelines

This section provides important information about configuring STGs:

- You must create an STG must by preforming these steps:
  - Create the STG.
  - Add the existing VLAN and port memberships.
  - Enable the STG.
- When you create a VLAN, that VLAN automatically belongs to STG 1, the default STG. If the VLAN is to be in another STG, move the VLAN by assigning it to another STG.
- You must move a newly created VLAN to an existing STG by performing these steps:
  - Create the VLAN.
  - Add the VLAN to an existing STG.
- You cannot move or delete VLAN1 from STG1.
- VLANs must be in 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 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.
- You cannot add a port that is a member of no VLAN to any STG. You must add the port must to a VLAN, and add that VLAN 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
- You can select a VLAN ID 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 you remove a port 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.
- You must disable an STG before you can delete it.
- You can configure a unique multicast address for STGs 1 to 4 only.

Spanning Tree Fast Learning

Spanning Tree Fast Learning is an enhanced port mode supported by the Ethernet Routing Switch 4000 Series. If you enable Spanning Tree Fast Learning on a port with no other bridges, the port starts more quickly after a switch initialization or a spanning tree change. The port passes 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 configured 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.

Important:

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 you enable the port through configuration.

STG port membership mode

The Avaya Ethernet Routing Switch 4000 supports two different STP port membership modes: normal and automatic. In the normal mode, when you assign a port to VLAN X and VLAN X is in STP group Y, the port does not automatically become a member of STP group Y. In automatic mode, when you assign a port to VLAN X and VLAN X is in STP group Y, the port automatically becomes a member of STP group Y.

802.1t path cost calculation

You can configure 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 which provides more bits for spanning tree costs, thus provides a larger range of costs which can better support the higher speed links which can be supported on the Avaya Ethernet Routing Switch 4000. It is recommended to use 802.1t mode if using 10 Gigabit links and other switches in the network support 802.1t. The mode can be changed using the ACLI command, **`spanning-tree cost-calc-mode`**.

802.1D compliancy support

In a complex network environment, STP can cause broadcast storms when a switch port fails and recovers frequently. When you enable 802.1D compliancy support, the system prevents broadcast storms by setting the STP state of a port to disabled when the port link is down.

Rapid Spanning Tree Protocol

The standard Spanning Tree implementation in 4000 Series switches is based on IEEE 802.1D. This implementation results in a slow response 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. RSTP also maintains a backward compatibility with the IEEE 802.1D, which was the Spanning Tree implementation prior to RSTP. In certain configurations, you can reduce the recovery time of RSTP to less than 1 second. Maintain the backward compatibility by configuring a port to be in STP-compatible mode. A port that operates 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.

The 4000 switch uses RSTP and MSTP to achieve the following:

- Reduce converging time from 30 seconds to less than 2 seconds when a topology change occurs in the network (that is, the port goes up or down).
- Eliminate unnecessary flushing of the MAC database and flooding of traffic to the network with a new Topology Change mechanism.
- Obtain backward compatibility with other switches that run legacy 802.1D STP or Avaya MSTG (STP group 1 only).
- Under MSTP mode, simultaneously support 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.
- Run Avaya MSTG, 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 return this port 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 similar parameter sets.

The following figure lists the differences in port roles for STP and RSTP. STP supports two port roles, while RSTP supports four port roles.

Table 2: Differences in port roles for STP and RSTP

Port Role	STP	RSTP	Description
Root	Yes	Yes	This port receives 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 receives 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 receives a better BPDU than its own from another port within the same switch. The Backup port is in Discarding state.

Edged Port

RSTP supports the Edged Port parameter. When a port is connected to a nonswitch device such as a PC or a workstation, you must configure the port as an Edged port for fast convergence. An active Edged port goes directly to Forwarding state with no delay. An Edged port becomes a non-Edged 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. The following figure lists the recommended path cost values.

Table 3: Recommended path cost values

Link speed	Recommended value

Less than or equal to 100 Kb/s
1 Mb/s
10 Mb/s
100 Mb/s
	200 000 000
	20 000 000
	2 000 000
	200 000

1 Gb/s	20 000

Link speed	Recommended value
10 Gb/s 100 Gb/s	2 000 200
1 Tb/s 10 Tb/s	20 2

Rapid convergence

With RSTP and MSTP, the environment root port or the designated port can request permission from a peer to enter the Forwarding State. If the peer grants permission; then the root port moves to the Forwarding State with no delay. This procedure is called the Negotiation Process.

With RSTP and MSTP, information received on a port can be sent immediately if the port malfunctions, 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 full duplex. Port 2 is an Edged port.

Switch B: Ports 1, 2, and 3 are full duplex. Port 2 is an Edged port.

Switch C: Ports 1 and 2 are full duplex. Port 2 is an Edged port.

Switch A is the Root.

Negotiation Process

After ports power up, they ports assume the role of Designated ports. All ports are in the Discarding state, except for Edged ports. Edged ports directly enter the Forwarding state with no delay.

Switch A port 1 and switch B port 1 exchange BPDUs, and switch A is the Root and switch A port 1 is the Designated port. Switch B learns that switch A has high priority. Switch B port 1 becomes the Root port. Both switch A port 1 and switch B port 1 remain in the Discarding state.

Switch A starts negotiating by sending a BPDU with a proposed bit set.

Switch B receives the proposed BPDU and sets its non-Edge ports to the Discarding state. This operation is the synchronization 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 communicate with each other.

- The negotiation process now moves down to switch B port 3 and its partner port.
- PC 3 cannot communicate with either PC 1 or PC 2 until the negotiation process between switch B and switch C is complete.

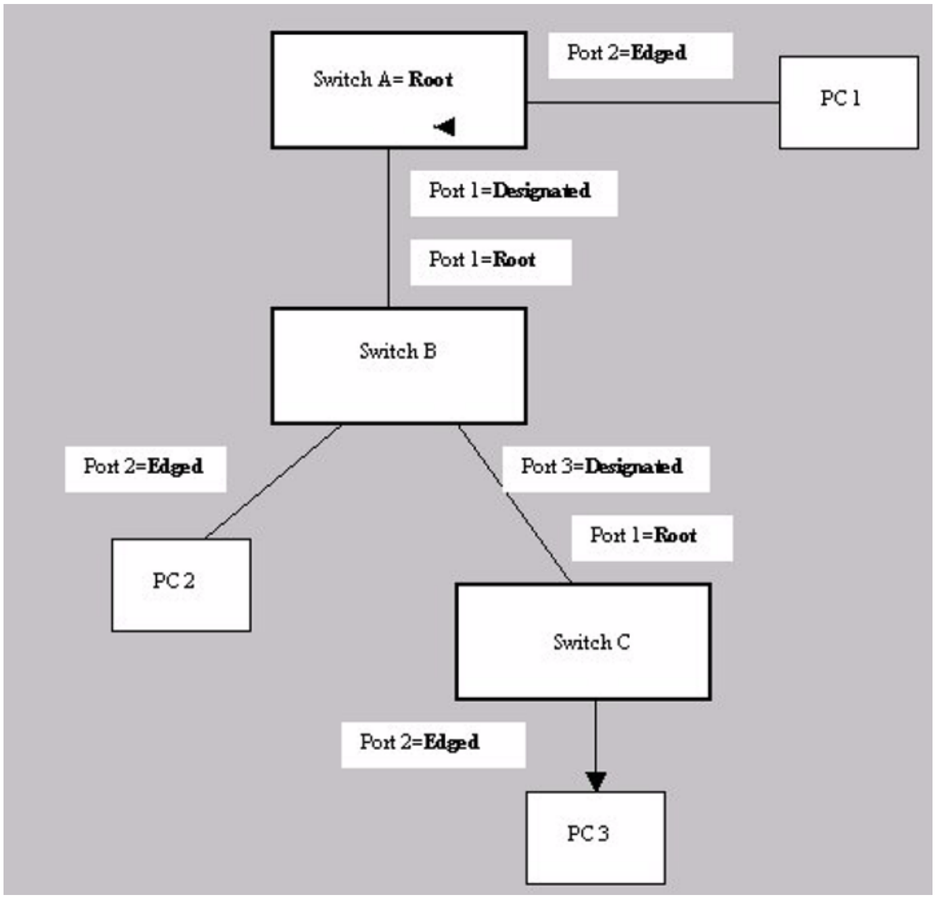


Figure 22: Negotiation process

The RSTP convergent time depends on how quickly the switch can exchange BPDUs during negotiation and the number of switches in the network. For a 4000 Series switch, the convergent time depends on the hardware platform and the number of active applications that run on the switch.

BPDU-Filtering

Ethernet Switches 4000 series support the BPDU-Filtering feature for STG, 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, after 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 after 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.

Important:

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

If 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 65 535 seconds. The port timer is disabled if it is configured as 0.

For details on configuring BPDU Filtering, see Configuring STP BPDU filtering using ACLI on page 125 and Configuring STP BPDU filtering for specific ports using EDM on page 240.

STP BPDU filtering ignore-self

With the STP BPDU filtering *ignore-self* parameter, you can prevent the switch from blocking ports if an IP Phone loops back BPDU packets. If you enable BPDU filtering on a switch port and you turn off an IP Phone connected to the port, the BPDU packet can loop back to the switch. The switch can interpret the looping BPDU packet as an attack and administratively block the port.

Chapter 6: ADAC Fundamentals

Autodetection and Autoconfiguration of IP Phones

Ethernet Switch software supports Autodetection and Autoconfiguration (ADAC) of 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 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 ports) or is indirectly connected to the Call Server using a network uplink (through the Uplink ports).

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 dynamically configures the Call Server or Uplink ports, 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. This mode provides the same configuration as the Untagged-Frames-Advanced mode, but with tagged frames. As with the Untagged-Frames-Advanced mode, ADAC dynamically configures the Call Server or Uplink ports, as applicable, and all telephony ports. While Traffic prioritization is configured automatically, tagging and PVID settings are user configurable.

ADAC operation

The following sections provide detailed explanations of ADAC operation.

Auto-detection of IP Phones

When an 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 in the following instances:

- before enabling auto-detection on the port
- 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 an Avaya IP phone. For more information and the list of defined MAC address ranges, see Auto-Detection by MAC address on page 64.

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 66.

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 an 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 ERS 4000 Series has a default range of MAC addresses configured to be recognized as Avaya IP Phones by ADAC.

The following table shows a list of the default MAC address ranges.

Table 4: 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
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.

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 device.
- Disable on port 5 MAC detection.

```
ERS4500(config)#in fa 5
ERS4500(config-if)#no adac detection mac
ERS4500(config-if)#sho adac detection interface 5
        MAC         LLDP
Port    Detection   Detection
----    ---------   ---------
5       Disabled    Enabled
```

- Enable ADAC on port 5 and globally.

```
ERS4500(config)#adac enable
ERS4500(config)#in fa 5
ERS4500(config-if)#adac enable
```

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

```
ERS4500(config)#vlan create 200 type port voice-vlan
ERS4500(config)#adac voice-vlan 200
ERS4500(config)#adac uplink-port 10
ERS4500(config)#adac op-mode untagged-frames-advanced
```

- Verify that the preceding settings were applied.

```
ERS4500(config)#sho adac
      ADAC Global Configuration
-----------------------------------
ADAC Admin State: Enabled
ADAC Oper State: Enabled
Operating Mode: Untagged Frames Advanced
Voice-VLAN ID: 200
Call Server Port: None
Uplink Port: 10
```

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

```
ERS4500(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 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 following:

- the ID of the VLAN to be used for voice packets
- at least one of the following:
    - Call Server port, if it is connected directly to the switch
    - Uplink port, if used

Important:

You must ensure that you manually create the Voice VLAN prior to enabling its use with ADAC operation.

You must also ensure that voice traffic entering the Uplink port is tagged 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.

Call Server ports must not be:

- a Monitor Port in port mirroring
- a Telephony port
- the Uplink port

Uplink ports must not be:

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

Telephony ports must not be:

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

Operating modes

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

- QoS Settings
- Untagged-Frames-Basic operating mode
- Untagged-Frames-Advanced operating mode
- Tagged-Frames operating mode

QoS Settings

ADAC QoS configuration is applied to:

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

Untagged-Frames-Basic operating mode

In the Untagged-Frames-Basic operating mode, the Call Server and Uplink ports are not used, and therefore 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.)
- Ensure that the Filter Unregistered Frames option is set to disabled on the ADAC-enabled ports (or that the ports belong to at least one VLAN).

Untagged-Frames-Basic QoS configuration

In this operating mode, QoS settings are applied only for traffic coming from the IP Phones. The Call Server and Uplink ports are not used.

Autoconfiguration performs the following:

- creates an Unrestricted Interface with all Telephony ports (each time a new Telephony port is detected, it will be added to this interface)
- creates an IP Filter (all fields set to Ignore) and an IP Filter Group
- uses Premium Service (transmit frame, update DSCP to 0x2E, Drop Precedence to Loss Sensitive, Update Priority to 6)

  DSCP to 0x2E is the default for ADAC.
- creates a policy containing the preceding functions

Untagged-Frames-Basic VLAN configuration

In the Untagged-Frames-Basic operating mode, Autoconfiguration 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.)
- Ensure that Filter Unregistered Frames option is set to disabled on the ADAC-enabled ports (or that the ports belong to at least one VLAN).
- 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.

Untagged-Frames-Advanced QoS configuration

In the Untagged-Frames-Advanced mode, Autoconfiguration performs the following QoS configuration for each port:

Table 5: Untagged-Frames-Advanced QoS configuration

For traffic coming from:	Autoconfiguration does the following:
Telephony ports	• creates an Unrestricted Interface with all Telephony ports (each time a new Telephony port is detected, it will be added to this interface) • creates an IP Filter (all fields set to Ignore) and an IP Filter Group • uses Premium Service (transmit frame, update DSCP to 0x2E, Drop Precedence to Loss Sensitive, Update Priority to 6) DSCP to 0x2E is the default for ADAC. • creates a policy containing the preceding functions
Call Server ports	• adds the Call Server port to the interface group created for Telephony ports
Uplink ports	• creates an Unrestricted Interface containing the Uplink port • creates a Layer 2 Filter, with EtherType IP, VLAN set to ID of the Voice-VLAN and Tagged (all other fields set to Ignore) • uses Premium Service • creates a policy containing the preceding functions

Untagged-Frames-Advanced VLAN configuration

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

Table 6: Untagged-Frames-Advanced VLAN configuration

Port type	Membership	Tagging	PVID
Telephony port	added to Voice-VLAN; removed from other VLANs (The port does not need to be a member of other VLANs)	Untagged	Voice-VLAN
Call Server port (if any)	added to Voice-VLAN; not removed from other VLANs	Untagged	Voice-VLAN
Uplink port (if any)	added to Voice-VLAN; not removed from other VLANs	Tagged	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.

Tagged-Frames QoS configuration

In the Tagged-Frames operating mode, Autoconfiguration performs the following QoS configuration:

Table 7: Tagged-Frames QoS configuration

For traffic coming from:	Autoconfiguration does the following:
Telephony ports	• creates an Unrestricted Interface (Call Server interface ID will be a member of this interface group) • creates an IP Filter (all fields set to Ignore) and an IP Filter Group • uses Premium Service • creates a policy containing all of the above
IP Phones and Uplink ports	• create an Unrestricted Interface containing all Telephony ports and Uplink ports • create a Layer 2 Filter, with EtherType IP, VLAN set to ID of the Voice-VLAN and Tagged (all other fields set to Ignore) • use Premium Service • create a policy containing all of the above

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

Tagged-Frames VLAN configuration

In the Tagged-Frames operating mode, Autoconfiguration also performs the following VLAN configurations:

Table 8: Tagged-Frames VLAN configuration

Port type	Membership	Tagging	PVID
Telephony port	added to Voice-VLAN; not removed from other VLANs	User-configurable (default is UntagPVIDOnly)	User-configurable [1] (default value is Default VLAN [1])
Call Server ports (if any)	added to Voice-VLAN; not removed from other VLANs	Untagged	Voice-VLAN
Uplink ports (if any)	added to Voice-VLAN; not removed from other VLANs	Tagged	no change (All VLAN changes made by ADAC are as if VCC=flexible, so the Auto-PVID setting is ignored.)

[1] If the PVID is set to a VLAN which does not exist when ADAC is applied, the PVID is set to Default VLAN (1).

Dynamic VLAN Autoconfiguration

Important:

Dynamic configurations are switch configurations that are not saved to NVRAM. Therefore, dynamic configurations are not restored following a switch reboot.

The following describes the details of the ADAC VLAN configuration:

- The Voice VLAN to be used by ADAC is created manually prior to configuration for ADAC.
- All ADAC ports membership to the ADAC Voice VLAN is dynamic.
- From the moment ADAC is enabled on a telephony port or Call Server port, all VLAN configuration is dynamic (including user configuration). After the ADAC configuration is removed from these ports, the pre-ADAC configuration from NVRAM is restored.
- For telephony ports, the NVRAM VLAN configuration is restored in two cases: after the ADAC configuration is removed due to the removal of the IP Phone, or after ADAC is disabled for that port.
- Any VLAN configuration that is made to an Uplink port is always saved to NVRAM (even when ADAC is enabled).
- The VLAN Configuration Control (VCC) rules, other than those for the Flexible mode, are skipped internally by ADAC when 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 manually make on ADAC ports follow the current VCC mode, similar to a non-ADAC port.

ADAC and stacking

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

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

If two or more units each have configured Call Server ports in stand-alone mode and are then joined together in a stack, the Call Server ports with the lowest interface number in the stack are elected the stack Call Server ports, until all the Call Server ports are elected or until all the Call Server slots are used.

This same scenario also occurs for the Uplink port.

Lost Call Server Port or Uplink Port

Beginning with release 5.4, the Avaya Ethernet Routing Switch 4000 maintains ADAC operation if the designated call server or uplink ports become unreachable. This allows the switch to maintain any current communications between end devices located on the switch.

ADAC Uplink port as part of trunk

When a port that is a member of an already active MLT, DMLT, or LAG is selected as the ADAC Uplink port; then the entire trunk is set as the Uplink connection. This means that the ADAC configuration (VLAN and QoS) is applied for all the members of the trunk. ADAC does not interfere in the way traffic is forwarded in the trunk.

Uplink port as part of MLT in a stack

The Uplink port can be part of an MLT. 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 stack, the lowest Uplink port is elected as the stack's Uplink port.

ADAC and LACP enabled on an Uplink port

To set an Uplink port as LACP-enabled, you must first configure and enable Link Aggregation Control Protocol (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 Link Aggregation Group (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.

Disabling LACP on an 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.

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.

ADAC Uplink over SPBM

ADAC Uplink over SPBM adds support for SPBM in ADAC, allowing ADAC to have the uplink over SPBM instead of an uplink port.

With this feature, ADAC can use an I-SID (that you associate with the ADAC Voice-VLAN) instead of a classical uplink-port. In this situation, ADAC can be enabled without the existence of a real uplink-port, and without the need of auto-configuring this uplink-port, therefore without auto-adding it to the Voice-VLAN.

> **Note:**
>
> You must correctly configure SPBM and the association between the I-SID and the ADAC Voice-VLAN to prevent a misconfiguration. Otherwise, the IP Phones are not able to reach the call-server device located on the other side of the SPBM cloud.

ADAC and EAP configuration

ADAC and Extensible Authentication Protocol (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, you must perform the following:

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

1. EAP: While ADAC is enabled, cannot disable per-port EAP Multihost or EAP setting:
    - Cannot disable Multihost on port if EAP is enabled per port and ADAC Detection is enabled per port
    - Cannot enable EAP per port if Multihost is disabled per port and ADAC Detection is enabled per port
2. ADAC: The detection can be enabled (for example, set ADAC enable per port) only if:
    - EAP is disabled per port

or

- EAP is enabled per port and Multihost is enabled per port

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

ADAC User Restrictions

After ADAC is enabled, you cannot:

- erase the Voice-VLAN
- remove auto-configured ports from Voice-VLAN
- remove any QoS setting made by ADAC (auto-configured settings)
- use the filter groups created by ADAC when setting policies
- disable the policies created by ADAC
- modify Call Server and Uplink port configuration

You can:

- add/remove the non-ADAC ports to the Voice-VLAN (configuration is static)
- add/remove the ADAC ports to VLANs (configuration is static)
- change the tagging and PVID of all ADAC ports (except for the Uplink ports, configuration is dynamic)
- add interfaces to and remove interfaces from ADAC interface groups
- use the filters created by ADAC when setting filter groups. (This means that when disabling the feature or when changing operating mode, if the filter is used by filter groups other than the ADAC filter group, the filter is not deleted.)
- use the interface groups created by ADAC when setting policies. (This means that when disabling the feature or when changing operating mode, if the interface group is used by a policy other than the ADAC policy, the interface group is not deleted.)

Adding the Voice-VLAN to another STG

In Untagged-Frames-Advanced or Tagged-Frames modes, ADAC sets tagging for the Call Server port to UntaggedAll. However, STP configuration rules do not allow an untagged port to span multiple STGs. As a result, you cannot add the Voice-VLAN to an STG as long as the Call Server is a member of another VLAN that belongs to another STG.

To successfully add the Voice-VLAN to a different STG using the same Call Server port, you must first remove the Call Server port from all other VLANs.

Disabling ADAC

Disabling the ADAC feature means the deletion of all configurations (except as noted in ADAC User Restrictions on page 77), including the following:

- All ADAC-involved ports are removed from the Voice-VLAN.
- PVID is set to the Management VLAN ID. The Uplink port is not changed if it has a value other than the Voice-VLAN ID (that is, if you have explicitly changed it after Autoconfiguration).

ADAC management

For more details on network configurations required to support IP Phones, see *Data Networking for Voice over IP,* (553-3001-160).

Chapter 7: LACP and VLACP Fundamentals

IEEE 802.3ad Link Aggregation

With IEEE 802.3ad-based link aggregation, you can aggregate one or more links 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 providing link redundancy.

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

With Link Aggregation Control Protocol (LACP), as defined by the IEEE 802.3ad standard, a switch can 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 for each port. 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 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 distributes frame transmissions from the MAC client to the various ports. The Aggregator also collects received frames from the ports and transparently passes them to the MAC client.
- A system can contain multiple Aggregators that serve multiple MAC clients. A given port binds to (at most) a single Aggregator at any time. At any one time, only one Aggregator serves a MAC client.
- The binding of ports to Aggregators within a system is managed by the Link Aggregation Control feature. The Link Aggregation Control feature determines which links can be aggregated, aggregates them, binds the ports within the system to an appropriate Aggregator, and monitors conditions to determine when a change in aggregation is needed.

  The network manager can control the determination and binding directly by manipulating the state variables of Link Aggregation (for example, Keys). In addition, automatic determination, configuration, binding, and monitoring can occur by using 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 to continuously provide the maximum level of aggregation between a pair of systems.

- Each port has a unique, globally administered MAC address.

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

- 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 4000 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 connect to the same far-end system.
- All ports in a link aggregation group must operate in full-duplex mode.
- You must configure all ports in a link aggregation group 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 groups 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 are supported for each LAG (for example, if a switch or stack has one LAG, you can configure all non active LAG link ports as standby ports for that LAG).
- The MLT/LAG is a logical port. The STP protocol is computing the topology using this logical port, not on individual MLT/LAG member ports. The logical port is represented by the first MLT/LAG port. The STP events related to MLT/LAG are logged using the first MLT/LAG port.

The maximum number of LAGs is 32, and the maximum number of active links for each group is 8. With Link Aggregation, you can configure more than 8 links 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 an active links goes down, the standby link becomes active and is added to the trunk group. For more information, see LACP and VLACP configuration using ACLI on page 167 and LACP and VLACP configuration using Enterprise Device Manager on page 287.

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.

A temporary delay in traffic flow can occur due to links switching. 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.

Static LACP Key to Trunk ID binding

Static LACP Key to Trunk ID binding provides a higher level of control over the management of MLT trunk groups, compared with previous dynamic association of link-aggregated ports with a trunk group.

With dynamic association, when you configure a group of link-aggregated ports (LAG), you have no control choosing which particular trunk is associated with the LAG. The trunk association with an aggregator depends on the state of the system. The LAG is automatically associated with the trunk group with the greatest ID, from the available trunks. After system state changes, as turning off/on the ports lacp mode or rebooting the switch, this association can be made differently, resulting in undesired effects for the trunk group and LACP ports.

For example, if you configure two LACP trunks, the MLT IDs are assigned to each trunk in the order of trunk creation. When the switch is rebooted, the order in which each LAG receives a trunk may invert. Settings kept strictly on a trunk group basis, as STP learning, are linked only with that specific trunk group, regardless of it being configured as a Dynamic LACP or a static MLT. If LACP ports aggregate in a different trunk group than the trunk group with the appropriate STP learning, traffic flooding may occur.

With Static LACP Key to Trunk ID binding, you associate a specific group of link-aggregated ports with a specific MLT trunk group. The static binding ensures that the switch maintains the LACP Key - MLT ID association until you delete the binding

Note:

Avaya recommends using Static LACP Key to Trunk ID binding instead of dynamic trunk group assignation for LACP ports.

After upgrading the switch to release 5.7, Static LACP key to trunk ID binding is enabled by default on the switch. When configured, Static LACP key - MLT ID binding overrides the dynamic association. If no binding settings are made, the dynamic behavior applies.

To configure static LACP key to trunk id binding, follow these generic steps:

- Bind each LACP key to be used to the required MLT ID.
- Assign LACP keys to the ports to be used. If no key is specified, all ports have the default value of 1.
- Configure LACP mode for the used ports. The LACP mode of the links must be either active or passive. If the chosen mode is passive, the mode of the partner at the other end of the links must be active in order for the LACP ports to aggregate in the same LAG.
- Enable LACP aggregation on the ports.

If the LACP ports having assigned a key cannot be all assigned to the same aggregator (because of different settings, such as port speed), only one of the aggregators will occupy the specified trunk group. The other LAGs are dynamically bound to other MLT trunks.

If the user specifies an MLT trunk ID for a key set on ports already associated with an up-and-running LACP trunk, the aggregator frees the previously used trunk and uses the newly specified one. Reciprocally, if the user deletes a key binding with an LACP trunk, the aggregator frees this LACP trunk and is dynamically assigned a new MLT trunk.

Note:

Because the maximum number of key to trunk ID associations is bound to the maximum number of MLT trunks that can be configured on the device, you can assign trunk IDs between 1 and 32.

If an MLT ID is bound to a key, its corresponding trunk entry cannot be used anymore for configuring other MLT/LACP trunks. Binding multiple different keys to different trunks may easily lead to the use of all available MLT IDs. If all available MLT IDs are used, the configuration of a new LACP trunk is not possible, even if all the other required conditions for trunk formation are accomplished. To fix this problem, a trunk ID must be freed. You can use the **`show lacp key`** and **`show mlt`** commands to check the LACP key bindings.

Usually, any problems caused by the limited number of MLT IDs can be avoided if the bindings are made carefully and kept track of.

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 is 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 23: Problem description (1 of 2) on page 83 and Figure 24: Problem description (2 of 2) on page 84 provides 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 the following figure, the MLT (between Enterprise switches S1 and S2) extends through the service provider (SP) network.

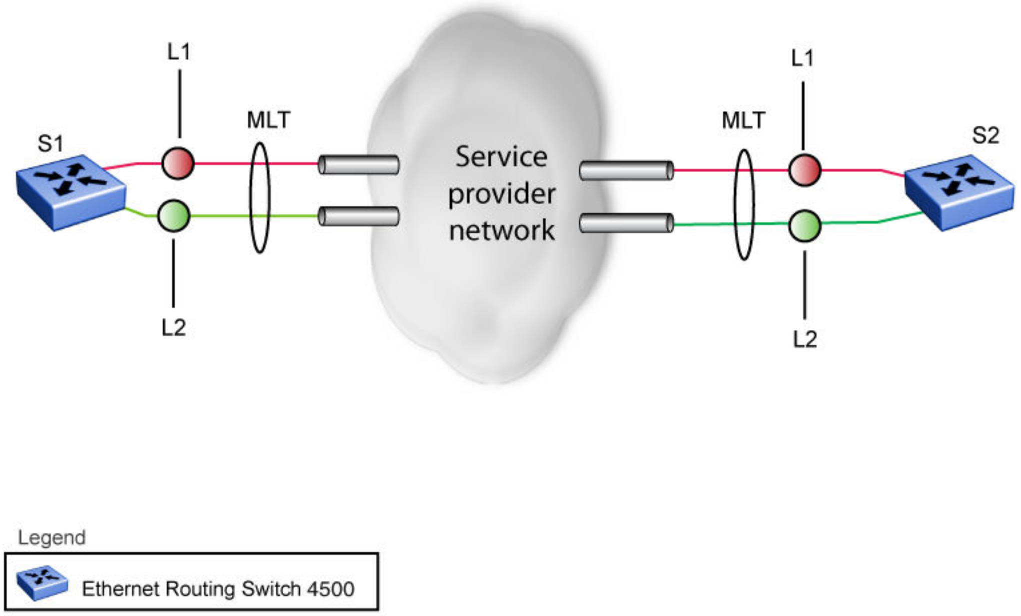


Figure 23: Problem description (1 of 2)

As shown in Figure 24: Problem description (2 of 2) on page 84 , 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.

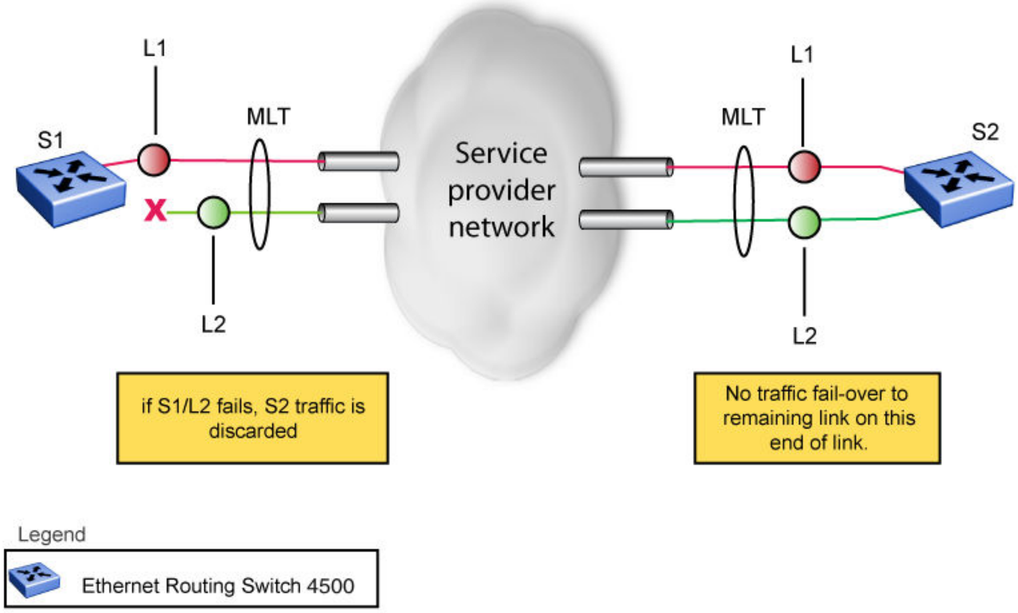

L1
S1
MLT
X
L2
Service provider network
MLT
L1
S2
L2
if S1/L2 fails, S2 traffic is discarded
No traffic fail-over to remaining link on this end of link.
Legend
Ethernet Routing Switch 4500

Figure 24: 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 preceding figure.

Prior to Release 5.6, when you used VLACP, the switch could not detect certain types unidirectional communication outage. With the addition to the software of two new VLACP Protocol Data Unit (PDU) subtypes, DOWN and HOLD, the switch manages certain operational situations better. For example:

- When a VLACP partner stops receiving PDUs from the other end (often due to certain types of unidirectional communication failures) the partner transmits a VLACP PDU that contains the DOWN subtype. The DOWN subtype informs the other end that the partner is no longer receiving VLACP PDUs and has declared the link down. The partner declares the link down and maintains this state until it receives a TXOK message.
- When ports are being initialised, if a port immediately transitions to active, in some cases the switch can temporarily forward traffic to a black hole. With the VLACP HOLD enhancement, a core switch running SMLT can transmit a VLACP PDU with the HOLD subtype when ports are not ready to forward traffic. The VLACP PDU HOLD subtype informs the partner that even though the link is up, the partner should not use the link until it receives an appropriate VLACP TXOK message.

VLACP features

This section provides a summary of some of the key features of VLACP:

- 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.

Avaya recommends you to set VLACP enabled ports with the following values to provide a higher resiliency.

- the timeout scale to five
- the timeout type to short
- the fast periodic time to 500ms

When you set the timeout scale to lower values in heavily loaded networks, it causes undesired behavior for VLACP enabled ports.

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 8: VLAN Configuration using ACLI

The ACLI commands described in this section help you to create and manage VLANs. Depending on the VLAN type, the command mode needed to execute these commands can differ.

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.

Prerequisites

Use this command in the Privileged EXEC mode.

Procedure steps

Enter the following command:

```
show vlan [id <VID_list>] [type {port | protocol decEther2 |
protocol-ipEther2 | protocol-ipv6Ether2 | protocol ipx802.2 |
protocol-ipx802.3 | protocol-ipxEther2 | protocol ipxSnap |
protocol-Netbios | protocol-RarpEther2 | protocol sna802.2 |
protocol-snaEther2 | protocol-vinesEther2 | protocol-xnsEther2
| protocol-Userdef {<4096-65534> | ether | llc | snap } | voice-
vlan | spbm-bvlan | spbm-switchedUni }] | voice-vlan | remote-
span
```

Variable Definitions

Variable	Value
id <VID_list>	Enter as an individual VLAN ID to display a single VLAN or enter as a range of VLAN IDs to create multiple VLANs simultaneously. A VLAN ID can range from 1 to 4094.
type	Enter the type of VLAN to display:

Variable	Value
	• port - port-based • protocol - protocol-based (see following list) • spbm-bvlan • spbm-switchedUni
voice-vlan	Displays voice VLAN information.
remote-span	Displays RSPAN VLAN information.
spbm-bvlan	Displays SPBM B-VLAN information.
spbm-switchedUni	Displays SPBM Switched Uni VLAN information.
Protocol parameter	**Description**
protocol-ipEther2	Specify an ipEther2 protocol-based VLAN.
protocol-ipx802.3	Specify an ipx802.3 protocol-based VLAN.
protocol-ipx802.2	Specify an ipx802.2 protocol-based VLAN.
protocol-ipxSnap	Specify an ipxSnap protocol-based VLAN.
protocol-ipxEther2	Specify an ipxEther2 protocol-based VLAN.
protocol-decEther2	Specify a decEther2 protocol-based VLAN.
protocol-snaEther2	Specify an snaEther2 protocol-based VLAN.
protocol-Netbios	Specify a NetBIOS protocol-based VLAN.
protocol-xnsEther2	Specify an xnsEther2 protocol-based VLAN.
protocol-vinesEther2	Specify a vinesEther2 protocol-based VLAN.
protocol-ipv6Ether2	Specify an ipv6Ether2 protocol-based VLAN.
protocol-Userdef	Specify a user-defined protocol-based VLAN. Enter optional parameters. • all – display all Userdef VLANs • ether – display Ethernet II Userdef VLANs • llc – display LLC Userdef VLANs
protocol-RarpEther2	Specify a RarpEther2 protocol-based VLAN.
protocol-sna802.2	Specify a sna802.2 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 settings, use the following command in Privileged EXEC mode:

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

Displaying verbose VLAN interface information

Use the following procedure to display VLAN, PVID, and port information associated with a port.

Procedure

1. Enter Privileged EXEC mode.
2. Use the following command to display verbose VLAN information:

   ```
   show vlan interface verbose <LINE>
   ```

   - where *<LINE>* is the list of ports for which you are setting the maximum number of clients. You can enter a single port, a range of ports, several ranges, or all ports.

Displaying port membership in VLANs

Use the following procedure to display port membership in VLANs.

Procedure steps

To display port membership in VLANs, use the following command in Privileged EXEC mode:

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

Displaying the management VLAN

Use the following procedure to display the management VLAN.

Procedure steps

To display the management VLAN, use the following command in Privileged EXEC mode:

```
show vlan mgmt
```

Displaying Voice VLAN information

Use the following procedure to display voice VLAN information.

Prerequisites

Use this command in the Privilege Exec mode.

Procedure steps

Enter the following command:

```
show vlan voice-vlan
```

Configuring the management VLAN

Use the following procedure to configure the management VLAN.

Procedure steps

To configure the management VLAN, use the following command from Global Configuration mode:

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

Deleting the management VLAN IP address

Use the following procedure to delete the management VLAN IP address.

Procedure steps

To delete the management VLAN IP address, use the following command from Global Configuration mode:

```
default ip address
```

Note:

This command will delete the management VLAN IP address from any mode.

Resetting the management VLAN

Use the following procedure to reset the management VLAN.

Procedure steps

To reset the management VLAN, use the following command in Global Configuration mode:

```
default vlan mgmt
```

Creating VLANs

Use the following procedure to create an individual VLAN or a range of VLANs.

Prerequisites

Use this command in the Global Configuration mode.

Procedure steps

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

```
vlan create <VID_list> [name <LINE>] type { port { voice-vlan |
remote-span | [<1-8>] { voice-vlan | remote-span } } | protocol
decEther2 | protocol-ipEther2 | protocol-ipv6Ether2 | protocol
ipx802.2 | protocol-ipx802.3 | protocol-ipxEther2 | protocol
ipxSnap | protocol-Netbios | protocol-RarpEther2 | protocol
sna802.2 | protocol-snaEther2 | protocol-vinesEther2 |
protocol-xnsEther2 | protocol-Userdef { <4096-65534> | ether |
llc | snap } | voice-vlan | spbm-bvlan | spbm-switchedUni
[<1-8>] } | [voice-vlan]
```

Important:

If you tag protocol VLAN client ports, the system cannot assign frames to the protocol VLAN, regardless of the defined ethertype. Frames are not assigned to the protocol VLAN because untagged packets will be assigned to the VLAN identified by the port PVID.

Example

```
vlan create 2-25,80,101-256 type port
```

Variable Definitions

Variable	Value
<VID_list>	Enter as an individual VLAN ID to create a single VLAN or enter as a range of VLAN IDs to create multiple VLANs simultaneously. A VLAN ID can range from 1 to 4094.

Variable	Value
	Note: VLAN ID values 4001 through 4008 are reserved and cannot be used.
name <line>	Specifies a unique alphanumeric name for an individual VLAN. **Note:** Do not enter a value for this parameter when you are creating multiple VLANs simultaneously.
type	Enter the type of VLAN to create: • port - port-based • protocol - protocol-based (see following list)
remote-span	Specify as RSPAN VLAN.
protocol-decEther2	Specify a decEther2 protocol-based VLAN.
protocol-ipEther2	Specify an ipEther2 protocol-based VLAN.
protocol-ipv6Ether2	Specify an ipv6Ether2 protocol-based VLAN.
protocol-ipx802.2	Specify an ipx802.2 protocol-based VLAN.
protocol-ipx802.3	Specify an ipx802.3 protocol-based VLAN.
protocol-ipxEther2	Specify an ipxEther2 protocol-based VLAN.
protocol-ipxSnap	Specify an ipxSnap protocol-based VLAN.
protocol-Netbios	Specify a NetBIOS protocol-based VLAN.
protocol-RarpEther2	Specify a RarpEther2 protocol-based VLAN.
protocol-sna802.2	Specify an sna802.2 protocol-based VLAN.
protocol-snaEther2	Specify an snaEther2 protocol-based VLAN.
protocol-Userdef	Specify a user-defined protocol-based VLAN. Enter • `<4094 - 65534 > {<1-8> | voice-vlan}` - Ethernet II Userdef VLAN with this Protocol ID, where <1-8> is Spanning Tree Group ID • `ether <4096 - 65534>` –Ethernet II Userdef VLAN with this Protocol ID • `llc <1-65534>` –LLC Userdef VLAN with this Protocol ID • `snap <1-65534>` – SNAP Userdef VLAN with this Protocol ID

Variable	Value
protocol-xnsEther2	Specify an xnsEther2 protocol-based VLAN.
protocol-vinesEther2	Specify a vinesEther2 protocol-based VLAN.
<1-8>	Specifies the Spanning Tree Group ID.
spbm-bvlan	Specify as SPBM B-VLAN.
spbm-switchedUni	Specify as SPBM switched UNI.
voice-vlan	Specify as Voice VLAN.

Deleting a VLAN

Use the following procedure to delete a VLAN or a range of VLANs.

Prerequisites

Use this command in the Global Configuration mode

Procedure steps

Enter the following command:

```
vlan delete <VID_list>
```

Important:

VLAN 1 cannot be deleted.

Example

```
vlan delete 2-25,80,101-256
```

Variable Definitions

Variable	Value
<VID_list>	Enter as an individual VLAN ID to delete a single VLAN or enter as a range of VLAN IDs to delete multiple VLANs simultaneously. A VLAN ID can range from 1 to 4094.

Creating an RSPAN VLAN

Use this procedure to create an RSPAN VLAN.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Use the following command to create an RSPAN VLAN:

   ```
   vlan create <VID> type port [<1–8>] remote-span
   ```

Variable definitions

The following table describes the parameters for the **`vlan create remote-span`** command.

Variable	Value
<VID>	Specifies the RSPAN VLAN ID.
[<1–8>]	Specifies the Spanning Tree Group ID.

Deleting an RSPAN VLAN

Use this procedure to delete an RSPAN VLAN.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Use the following command to delete an RSPAN VLAN:

   ```
   no vlan <VID> remote-span
   ```

   - where <*VID*> specifies the RSPAN VLAN ID.

Note:

An RSPAN VLAN cannot be deleted if it is used in a port-mirroring RSPAN instance. The RSPAN instance must be deleted first.

Displaying RSPAN VLAN information:

Use this procedure to display RSPAN VLAN information.

Procedure

1. Enter Privileged EXEC mode.
2. Use the following command to display RSPAN VLAN information:

   ```
   show vlan remote-span
   ```

Disabling a voice VLAN

Use the following procedure to disable a VLAN or a list of VLANs as a voice VLAN.

Prerequisites

Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

```
no vlan <LINE> voice-vlan
```

Variable definition

Variable	Value
<LINE>	Enter as an individual VLAN ID to disable a single VLAN or enter as a range of VLAN IDs

Variable	Value
	to disable multiple VLANs simultaneously. A VLAN ID can range from 1 to 4094.

Removing a MAC address from allowed flooding

Use the following procedure to remove a MAC address from the list of addresses for which flooding is allowed.

Procedure steps

To remove a MAC address, use the following command from Global Configuration mode:

```
no vlan [igmp unknown-mcast-allow-flood <mac_address>]
```

Configuring VLAN name

Use the following procedure to configure or change a VLAN name.

Procedure steps

To change the VLAN name, use the following command from Global Configuration mode:

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

Configuring automatic PVID

Use the following procedure to enable automatic PVID.

Procedure steps

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

```
auto-pvid
```

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

Configuring IGMP snooping on a VLAN

Enable IGMP snooping on a VLAN to forward the multicast data to only those ports that are members of the group.

IGMP snooping is disabled by default.

Procedure steps

1. Log on to VLAN Interface Configuration command mode in ACLI.
2. Enable IGMP snooping:

```
[default] [no] ip igmp snooping
```

OR

1. Log on to Global Configuration command mode in ACLI:
2. Enable IGMP snooping:

```
[default] vlan igmp <vid> [snooping {enable | disable}]
```

Variable definitions

The following table describes the command variables.

Variable	Value
default	Disables IGMP snooping on the selected VLAN.
no	Disables IGMP snooping on the selected VLAN.
enable	Enables IGMP snooping on the selected VLAN.
disable	Disables IGMP snooping on the selected VLAN.

Configuring port VLAN settings

Use the following procedure to configure port VLAN settings.

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.
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. **Important:** This option can only be used if a single port is specified in the <portlist>.

Configuring VLAN member ports

Use the following procedure to add or remove VLAN member ports from a VLAN or a range of VLANs

Prerequisites

- Use this command in the Global Configuration mode
- The VLAN configuration control setting must be set to flexible

Procedure steps

Enter the following command:

```
vlan configcontrol flexible
```

```
vlan members [ add | remove ] <VID_list> <portlist>
```

Example

```
vlan configcontrol flexible
```

```
vlan members add 2-25,80,101-256 25-30
```

Variable Definitions

Variable	Value
add | *remove*	Adds a port to or removes a port from a VLAN. ❗ **Important:** 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.
<VID_list>	Enter as an individual VLAN ID or enter as a range of VLAN IDs to add/remove members to multiple VLANs simultaneously. A VLAN ID can range from 1 to 4094.
portlist	Enter the list of ports to be added, removed, or assigned to the VLAN or list of VLAN IDs.

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

Important:

Strict is the factory default setting.

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

To configure VCC using ACLI, see the following commands:

Displaying VLAN Configuration Control settings

Use the following procedure to display VLAN Configuration Control settings.

Procedure steps

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

```
show vlan configcontrol
```

Modifying VLAN Configuration Control

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 the current VLAN Configuration Control setting, use the following command from Global Configuration mode:

```
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: • automatic: Changes the VCC option to Automatic. • autopvid: Changes the VCC option to AutoPVID. • flexible: Changes the VCC option to Flexible. • strict: Changes the VCC option to Strict. This is the default VCC value.

Managing MAC address forwarding database table

✱ **Note:**

In certain situations, due to the hash algorithm used by switch to store MAC addresses into memory, some MAC addresses may not be learned.

This section shows you how to view the contents of the MAC address forwarding database table, setting the age-out time for the addresses, and clearing The MAC address table.

Displaying the MAC address forwarding table

Use the following procedure to display the current contents of the MAC address forwarding database table. The MAC address table can store up to 8192 addresses.

Procedure steps

To display 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>] [dynamic ] [static] [spbm {i-sid <1-
16777215>}] [mlt <1–32>]
```

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	Display the time in seconds after which an unused entry is removed from the forwarding database.
address <H.H.H>	Display a specific MAC address if it exists in the database. Enter the MAC address you want displayed.
port <portlist>	Specify ports.
dynamic	Display only dynamically learned addresses.
static	Display only statically inserted addresses.
spbm *i-sid* <1–6777215>	Displays SPBM MAC address entries. You can enter also display MAC address entries for a specific i-sid.
mlt <1–32>	Displays the MAC addresses for the specified Trunk.

Enabling MAC address learning using ACLI

If you disabled MAC address learning, use this procedure to enable MAC address learning.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

```
[ default ] mac-address-table learning [<portList>]
```

Variable definitions

Variable	Value
default	Default is learning enabled.
portList	Specifies a list of ports to be enabled. If you do not specify a port list, the system enables learning on all ports.

Disabling MAC address learning using ACLI

Use this procedure to disable MAC address learning.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

```
no mac-address-table learning [<portList>]
```

Variable definitions

Variable	Value
portList	Specifies a list of ports on which you want to disable MAC address learning. If you do not specify a port list, the system disables learning for all ports.

Configuring aging time for unseen MAC addresses

Use the following procedure to configure the time during which the switch retains unseen MAC addresses.

Procedure steps

To configure aging time, use the following command from Global Configuration mode:

```
mac-address-table aging-time <10-1 000 000>
```

Note:

The aging-time value defines the minimum time during which an unused MAC entry remains in the MAC address table. The maximum time is twice the value of aging-time. So, an unused MAC address expires in the interval between the value of aging-time and twice the value of aging-time.

Variable Definitions

Variable	Value
aging-time <10-1 000 000>	Enter the aging time in seconds that you want for MAC addresses before they expire.

Setting aging time for unseen MAC addresses to default

Use the following procedure to set the aging time for MAC addresses to 300 seconds.

Procedure steps

To set again time to default (300 seconds), use the following command from Global Configuration mode:

```
default mac-address-table aging-time
```

Adding a static address in the MAC address table using ACLI

Use this procedure to add a static address in the MAC address table.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

```
mac-address-table static <H.H.H.> <vid> interface <interface-
type> <interface-id>
```

Variable definitions

Variable	Value
H.H.H	Static address to be added in the MAC address table, range from 0:0:0:0:0 to FE:FF:FF:FF:FF:FF. Address can only be a unicast address.
vid	VLAN ID range from 1 - 4094.
interface-type	Enter the type of interface • Ethernet – add MAC address on a port • mlt – add MAC address on a trunk
interface-id	Number of port or trunk, for mlt, range is 1-32, for Ethernet, range is from 1/1 to x/y (max of x is 8 and max of y is 50).

Clearing the MAC address table

Use the following procedure to clear the MAC address table.

Prerequisites

- Log on to the Privileged EXEC mode.

Procedure steps

To flush the MAC address table, use the following command:

```
clear mac-address-table
```

Clearing the MAC address table on a VLAN

Perform this procedure to flush the MAC addresses for a specific VLAN.

Prerequisites

- Log on to the Privileged EXEC mode.

Procedure steps

To flush the MAC address table for a specific VLAN, use the following command:

```
clear mac-address-table interface vlan <1-4094>
```

Variable definition

Variable	Value
1-4094	Specify the VLAN for which you want to be flush the MAC addresses.

Clearing the MAC address table on an Ethernet interface

Perform this procedure to flush the MAC addresses for the specified ports. This command does not flush the addresses learned on the trunk.

Prerequisites

- Log on to the Privileged EXEC mode.

Procedure steps

To clear the MAC address table on an Ethernet interface, use the following command.

```
clear mac-address-table interface Ethernet <LINE>
```

Variable definition

Variable	Value
LINE	Specifies the list of ports for which you want to flush the MAC addresses.

Clearing the MAC address table on a trunk

Perform this procedure to flush the MAC addresses for the specified trunk. This command flushes only addresses that are learned on the trunk.

Prerequisites

- Log on to the Privileged EXEC mode.

Procedure steps

To clear the MAC address table on a trunk, use the following command:

```
clear mac-address-table interface mlt <1-32>
```

Variable definition

Variable	Value
1-32	Specifies the Trunk for which you want to flushed the MAC addresses.

Removing a single address from the MAC address table

Perform this procedure to flush one MAC address from the MAC address table.

Prerequisites

- Log on to the Privileged EXEC mode.

Procedure steps

To flush a single MAC address, use the following command:

```
clear mac-address-table address <H.H.H>
```

Variable definition

Variable	Value
H.H.H	Specify the address you want to flush out.

Removing a static address for a VLAN in the MAC address table

Use this procedure to clear a static address for a VLAN in the MAC address table

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

```
no mac-address-table static <address:H.H.H> <vid> interface
<interface-type> <interface-id>
```

OR

```
default mac-address-table static <address:H.H.H> <vid>
interface <interface-type> <interface-id>
```

Variable definitions

Variable	Value
H.H.H	Static address to be cleared from the MAC address table, range from 0:0:0:0:0 to FE:FF:FF:FF:FF:FF. Address can only be a unicast address.

Variable	Value
vid	VLAN ID range is 1 - 4094.
interface-type	Enter the type of interface. • Ethernet – add MAC address on a port • mlt – add MAC address on a trunk • vlan – add MAC address in a VLAN
interface-id	Number of port or trunk, for mlt, range is 1-32, for Ethernet, range is from 1/1 to x/y (max of x is 8 and max of y is 50), for vlan, range is 1-4094.

Removing static addresses from the MAC address table using ACLI

Use this procedure to flush static MAC addresses from the MAC address table.

Prerequisites

- Use this command in the Privileged EXEC mode.

Procedure steps

Enter the following command:

```
clear mac-address-table static [ interface <interface-type>
<interface-id>]
```

Variable definitions

Variable	Value
interface-type	Enter the type of interface. • Ethernet – flush MAC addresses on a port, or a list of ports • mlt – flush all MAC addresses on a trunk • vlan – flush all MAC addresses in a VLAN

Variable	Value
interface-id	• mlt, enter the trunk number, range is 1-32, • for Ethernet, enter a list of ports to be flushed out, range is from 1/1 to x/y (max of x is 8 and max of y is 50) • for vlan, enter the VLAN ID, range is 1-4094

Removing dynamic addresses from the MAC address table using ACLI

Use this procedure to flush dynamic MAC addresses from the MAC address table.

Prerequisites

- Use this command in the Privileged EXEC mode.

Procedure steps

Enter the following command:

```
clear mac-address-table dynamic [ interface <interface-type>
<interface-id> ]
```

Variable definitions

Variable	Value
interface-type	Enter the type of interface • Ethernet – flush MAC addresses on a port, or a list of ports • mlt – flush all MAC addresses on a trunk • vlan – flush all MAC addresses in a VLAN
interface-id	• mlt, enter the trunk number, range is 1-32 • for Ethernet, enter a list of ports to be flushed out, range is from 1/1 to x/y (max of x is 8 and max of y is 50) • For vlan, enter the VLAN ID, range is 1-4094

Chapter 9: MultiLink Trunk Configuration using ACLI

Use the ACLI commands described in this section to create and manage MultiLink trunks. Depending on the type of MultiLink trunk being created or managed, the command mode needed to execute these commands can differ.

Configuring a Multi Link Trunk using ACLI

Use the following procedure to configure a MLT.

Procedure steps

To configure a MLT, 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 <advance|basic>
```

Use the **no** form of this command to disable a MLT.

Variable Definitions

Variable	Value
id	Enter the trunk ID; the range is 1–32.
name <trunkname>	Specify a text name for the trunk; enter up to 16 alphanumeric characters.
enable | disable	Enable or disable the trunk.
member <portlist>	Enter the ports that are members of the trunk.
learning <disable | fast | normal>	Set STP learning mode.
bpdu {all-ports | single-port}	Set trunk to send and receive BPDUs on either all ports or a single port.

Variable	Value
loadbalance	Specifies the type of MLT load balancing. • advance—performs hashing based on layer2 criteria • basic—performs hashing based on layer3 criteria

Displaying MLT configuration using ACLI

Use the following procedure to display 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>
```

Viewing IP address-based MLT hashing information using ACLI

Use the following procedure to display MLT hashing information for specific source and destination IP addresses.

Procedure steps

To display IP address-based MLT hashing, use the following command from Privileged EXEC mode:

```
show mlt hash-calc <1-32> dest-ip <ip-add> src-ip <ip-add>
[tcp-udp-dport <0-65535>] [tcp-udp-sport <0-65535>]
```

Variable definitions

Variable	Value
`<1-32>`	Specifies the MLT ID.
`dest-ip <ip-add>`	Specifies the destination IP address.
`src-ip <ip-add>`	Specifies the source IP address.
`tcp-udp-dport <0-65535>`	Specifies the destination TCP or UDP port number.
`tcp-udp-sport <0-65535>`	Specifies the source TCP or UDP port number.

Job aid: IP address-based show mlt hash-calc command output

The following example displays sample output for the **`show mlt hash-calc <1-32> dest-ip <ip-add> src-ip <ip-add>`** command when MLT is not enabled.

```
ERS4000#show mlt hash-calc 1 dest-ip 172.16.2.1 src-ip
172.16.2.5 tcp-udp-dport 2 tcp-udp-sport 7
% MLT trunk is disabled.
```

The following example displays sample output for the **`show mlt hash-calc <1-32> dest-ip <ip-add> src-ip <ip-add>`** command when MLT links are down.

```
ERS4000#show mlt hash-calc 1 dest-ip 172.16.2.1 src-ip
172.16.2.5 tcp-udp-dport 2 tcp-udp-sport 7
% MLT links are all down.
```

The following example displays sample output for the **`show mlt hash-calc <1-32> dest-ip <ip-add> src-ip <ip-add>`** command with a hash calculation.

```
ERS4000#show mlt hash-calc 1 dest-ip 172.16.2.1 src-ip
172.16.2.5 tcp-udp-dport 2 tcp-udp-sport 7
Hash Calc:  1/24
```

Viewing MAC address-based MLT hashing using ACLI

Use the following procedure to display MLT hashing information for specific source and destination devices.

Procedure steps

To display MAC address-based MLT hashing information, use the following command from Privileged EXEC mode:

```
show mlt hash-calc <1-32> dest-mac <h:h:h> src-mac <h:h:h>
[vlan <vlan-id> | ethertype <ether_type>] | src-port
<unit_port>]
```

Variable definitions

Variable	Value
<1-32>	Specifies the MLT ID.
dest-mac <h:h:h>	Specifies the destination MAC address.
src-mac <h:h:h>	Specifies the source MAC address.
vlan <vlan-id>	Specifies the destination TCP or UDP port number.
ethertype <ether_type>	Specifies the Ethernet type.
src-port <unit_port>	Specifies the source port number.

Job aid: MAC address-based show mlt hash-calc command output

The following example displays sample output for the **show mlt hash-calc <1-32> dest-mac <h:h:h> src-mac <h:h:h>** command when MLT is not enabled.

```
ERS4000#show mlt hash-calc 1 dest-mac 00-13-49-4b-04-74 src-
mac 00-1D-42-36-EC-40 vlan 3 ethertype 0x001D src-port 1/24
% MLT trunk is disabled.
```

The following example displays sample output for the **`show mlt hash-calc <1-32> dest-mac <h:h:h> src-mac <h:h:h>`** command when MLT links are down.

```
ERS4000#show mlt hash-calc 1 dest-mac 00-13-49-4b-04-74 src-
mac 00-1D-42-36-EC-40 vlan 3 ethertype 0x001D src-port 1/24
% MLT links are all down.
```

The following example displays sample output for the **`show mlt hash-calc <1-32> dest-mac <h:h:h> src-mac <h:h:h>`** command when the load balancing mode selected for the MLT algorithm is **advanced**.

```
ERS4000#show mlt hash-calc 1 dest-mac 00-13-49-4b-04-74 src-
mac 00-1D-42-36-EC-40 vlan 3 ethertype 0x001D src-port 1/24
% You must use dest-ip and src-ip when MLT load-balancing
mode is advanced.
```

The following example displays sample output for the **`show mlt hash-calc <1-32> dest-mac <h:h:h> src-mac <h:h:h>`** command when the load balancing mode selected for the MLT algorithm is **basic**.

```
ERS4000#show mlt hash-calc 1 dest-mac 00-13-49-4b-04-74 src-
mac 00-1D-42-36-EC-40 vlan 3 ethertype 0x001D src-port 1/24
% Hash Calc: 2/23
```

Displaying STG MLT properties using ACLI

Use the following procedure to display the properties of MultiLink trunks (MLT) participating in Spanning Tree Groups (STG).

Procedure steps

To display the properties of MLTs participating in Spanning Tree Groups, use the following command in Global Configuration mode:

```
show mlt spanning-tree <1-32>
```

Configuring STP participation for MLTs using ACLI

Use the following procedure to set Spanning Tree Protocol (STP) participation for Multi Link Trunks (MLT).

Procedure steps

To set 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>	Specify the ID of the MLT to associate with the STG.
stp <1 - 8 | all >	Specify the spanning tree group.
learning {disable | normal | fast}	Specify the STP learning mode: • disable: disables learning • normal: sets the learning mode to normal • fast: sets the learning mode to fast

Enabling all ports shutdown in the MLT using ACLI

Perform this procedure to enable the shutdown of all ports in the MLT if the MLT is disabled.

Prerequisites

- Log on to the Global Configuration mode.

Procedure steps

To enable the shutdown of all ports in the MLT if MLT is disabled, use the following command:

```
mlt shutdown-ports-on-disable enable
```

Disabling MLT Enable or Disable Whole Trunk feature using ACLI

Perform this procedure to disable the MLT Enable or Disable Whole Trunk feature, and restore MLTs to the default operational mode.

Prequisites

- Log on to the Global Configuration mode.

Procedure steps

To disable the MLT Enable or Disable Whole Trunk feature and restore MLTs to the default operational mode use the following command:

```
no mlt shutdown-ports-on-disable enable
```

Displaying the current MLT Enable or Disable Whole Trunk mode of operation using ACLI

Perform this procedure to display the status of the MLT Enable or Disable Whole Trunk feature.

Prerequisites

- Log on to the Privileged EXEC mode.

Procedure steps

To see current MLT mode of operation use the following command:

```
show mlt shutdown-ports-on-disable
```

Job aid

The following displays sample output for the **show mlt shutdown-ports-on-disable** command:

```
show mlt shutdown-ports-on-disable
Trunk loop prevention is enabled.
```

Selecting an SLPP Guard Ethernet type using ACLI

Use this procedure to select an SLPP Guard Ethernet type for the switch.

Important:

You must configure Ethertype to match the SLPP Ethernet type on the adjacent core or distribution switches that have SLPP enabled.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. Select an SLPP Guard ethernet type by using the following command:

   ```
   slpp-guard ethertype <0x0600-0xffff>
   ```

2. Set the SLPP Guard ethernet type to the default value by using the following command:

   ```
   default slpp-guard ethertype
   ```

Variable definitions

Variable	Value
<0x0600-0xffff>	Specifies a hexadecimal value ranging from 0x0600 to 0xffff. Use the prefix 0x to type the hexadecimal value.

Configuring SLPP Guard using ACLI

Use this procedure to configure SLPP Guard for switch ports.

Prerequisites

- Log on to the Ethernet Interface Configuration mode in ACLI.

Note:

SLPP packets are generated only on switches that are configured with SLPP - for example ERS 5000 Series or ERS 8300. The ERS 4000 switches do not support SLPP. When you enable SLPP Guard on an ERS 4000, the switch must be connected to another Avaya switch that supports SLPP and SLPP must be enabled on that switch.

Procedure steps

Configure SLPP Guard for switch ports by using the following command:

```
[default][no] slpp-guard [port <portlist>][enable][timeout {0|
<10-65535>}]
```

Variable definitions

Variable	Value
[default]	Sets SLPP Guard parameters to default values for a port or list of ports.
[enable]	Enables SLPP Guard parameters for a port or list of ports.
[no]	Disables SLPP Guard parameters for a port or list of ports.
[port <portlist>]	Specifies the port or list of ports on which the specified SLPP Guard parameter or parameters are configured.
[timeout {0|<10-65535>}]	Specifies the time period, in seconds, for which SLPP Guard disables the port. After the timeout period expires, the switch re-

Variable	Value
	enables the port. The timeout value can be 0 or a value ranging from 10 to 65535. With a value of 0, the port remains disabled until it is manually re-enabled. The default timeout value is 60 seconds.

Viewing the SLPP Guard status using ACLI

Use this procedure to display the SLPP Guard configuration status for the switch or a specific list of ports.

Prerequisites

- Log on to the User EXEC mode in ACLI.

Procedure steps

Display the SLPP Guard configuration status by using the following command:

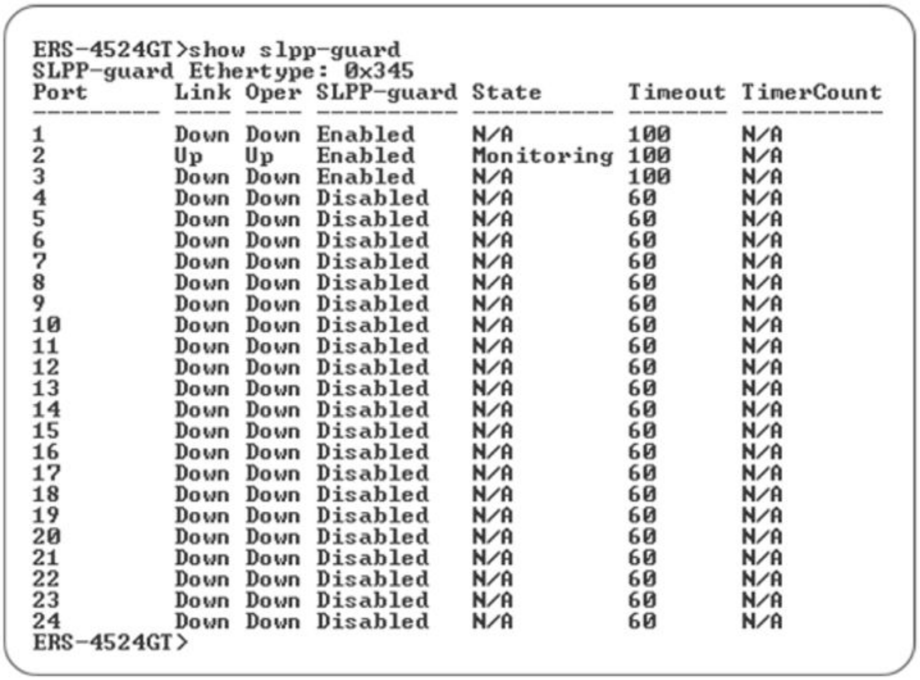
```
show slpp-guard [<portlist>]
```

Variable definitions

Variable	Value
<portlist>	Specifies a list of ports for which to display the SLPP Guard configuration status.

Job aid: show eapol multihost command output

The following figure displays sample output for the show slpp-guard command.



```
ERS-4524GT>show slpp-guard
SLPP-guard Ethertype: 0x345
Port       Link Oper SLPP-guard State      Timeout TimerCount
---------- ---- ---- ---------- ---------- ------- ----------
1          Down Down Enabled    N/A        100     N/A
2          Up   Up   Enabled    Monitoring 100     N/A
3          Down Down Enabled    N/A        100     N/A
4          Down Down Disabled   N/A        60      N/A
5          Down Down Disabled   N/A        60      N/A
6          Down Down Disabled   N/A        60      N/A
7          Down Down Disabled   N/A        60      N/A
8          Down Down Disabled   N/A        60      N/A
9          Down Down Disabled   N/A        60      N/A
10         Down Down Disabled   N/A        60      N/A
11         Down Down Disabled   N/A        60      N/A
12         Down Down Disabled   N/A        60      N/A
13         Down Down Disabled   N/A        60      N/A
14         Down Down Disabled   N/A        60      N/A
15         Down Down Disabled   N/A        60      N/A
16         Down Down Disabled   N/A        60      N/A
17         Down Down Disabled   N/A        60      N/A
18         Down Down Disabled   N/A        60      N/A
19         Down Down Disabled   N/A        60      N/A
20         Down Down Disabled   N/A        60      N/A
21         Down Down Disabled   N/A        60      N/A
22         Down Down Disabled   N/A        60      N/A
23         Down Down Disabled   N/A        60      N/A
24         Down Down Disabled   N/A        60      N/A
ERS-4524GT>
```

Note:

The TimerCount column in the preceding figure indicates the time, in seconds, that elapses after SLPP Guard disables a port. When the value TimerCount value equals the Timeout value, the switch re-enables the port.

Chapter 10: Spanning Tree Protocol configuration using ACLI

Use the ACLI commands described in this section to configure and manage Spanning Tree Protocol (STP).

Configuring STP operation mode using 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 MST (802.1s Multiple Spanning Tree Protocol).

Prerequisites

Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

```
spanning-tree mode {mst | rstp | stpg}
```

Configuring STP BPDU filtering using ACLI

Use the following procedure to configure STP BPDU filtering on a port. This command is available in all STP modes (STG, RSTP, and MSTP).

Procedure steps

To configure STP BPDU filtering, use the following command in Interface Configuration mode:

```
spanning-tree bpdu-filtering [port <portlist>] [enable]
[timeout <10-65535 | 0> ]
```

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.

Configuring STP BPDU filtering ignore-self using ACLI

Use this procedure to prevent the switch from blocking ports if an IP Phone loops back BPDU packets

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Configure STP BPDU Filtering ignore self by using the following command:

```
[no] [default] spanning-tree bpdu-filtering ignore-self
```

Variable definitions

Variable	Value
[default] [no]	Disables STP BPDU Filtering ignore self.

Viewing the STP BPDU Filtering ignore-self status using ACLI

Use this procedure to display the configuration status for STP BPDU Filtering ignore-self.

Prerequisites

- Log on to the Privileged EXEC mode in ACLI.

Procedure steps

Display the configuration status for STP BPDU Filtering ignore self by using the following command:

```
show spanning-tree bpdu-filtering ignore-self
```

Creating and Managing STGs using ACLI

To create and manage Spanning Tree Groups, see 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 ACLI, see the following:

Configuring path cost calculation using ACLI

Use the following procedure to set the path cost calculation mode for all Spanning Tree Groups on the switch.

Procedure steps

1. To set path cost calculation, use the following command from Global Configuration mode:

   ```
   spanning-tree cost-calc-mode {dot1d | dot1t}
   ```

2. To set the cost-calc-mode to its default value (dot1d), use the following command:

```
default spanning-tree cost-calc-mode
```

Configuring STG port membership using ACLI

Use the following procedure to set the STG port membership mode for all Spanning Tree Groups on the switch.

Procedure steps

To set STG membership mode, use the following command from Global Configuration mode:

```
spanning-tree port-mode {auto | normal}
```

Displaying spanning tree configuration information using ACLI

Use the following procedure to display spanning tree configuration information that is specific to either the Spanning Tree Group or to the port.

Prerequisites

Use this command in the Privileged EXEC mode.

Procedure steps

Enter the following command:

```
show spanning-tree [stp <1-8>] {config | port| vlans} {cost-
calc-mode | mode | port-mode}
```

Variable Definitions

Variable	Value
stp <1-8>	Display specified Spanning Tree Group configuration; enter the number of the group to be displayed.
config | port | vlans	Display spanning tree configuration for

Variable	Value
	• config: the specified (or default) Spanning Tree Group • port: the ports within the Spanning Tree Group • vlans: the VLANs that are members of the specified Spanning Tree Group
cost-calc-mode	Display pathcost type.
mode	Display the STP operational mode (STG, RSTP, or MST).
port-mode	Display the STG port membership mode.

Creating a spanning tree group using ACLI

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 using ACLI

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 using ACLI

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 using ACLI

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 by STG using ACLI

Use the following procedure to configure STP values by STG.

Prerequisites

Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

```
spanning-tree [stp <1-8>] [forward-time <4-30>] [hello-time
<1-10>] [max-age <6-40>] [priority {0000 | 1000| 2000 | 3000
| ... | E000 | F000}] [tagged-bpdu {enable | disable}] [tagged-
bpdu-vid <1-4094>] [multicast-address <H.H.H>] [add-vlan
<1-4094>] [remove-vlan <1-4094>]
```

Variable Definitions

Variable	Value
stp <1-8>	Specify the Spanning Tree Group; enter the STG ID. DEFAULT: ?
forward-time <4-30>	Enter the forward time of the STG in seconds; the range is from 4–30. DEFAULT: 15 seconds.
hello-time <1-10>	Enter the hello time of the STG in seconds; the range is from 1–10. DEFAULT: 2 seconds.
max-age <6-40>	Enter the max-age of the STG in seconds; the range is from 6–40. DEFAULT: 20 seconds.
priority {0000 | 1000 | 2000 | 3000 | .... | E000 | F000}	Set the spanning tree priority (in Hex); if 802.1T compliant, this value must be a multiple of 1000.
tagged-bpdu {enable | disable}	Set the BPDU as tagged or untagged. DEFAULT: For STG 1 (default group) is untagged; for all other groups is tagged.
tagged-bpdu-vid <1-4094>	Set the VLAN ID for the tagged BPDU. DEFAULT: 4001 to 4008 for STG 1 to 8, respectively.
multicast-address <H.H.H>	Set the spanning tree multicast address.
add-vlan <1-4094>	Add a VLAN to the Spanning Tree Group.
remove-vlan <1-4094>	Remove a VLAN from the Spanning Tree Group.

Restoring default spanning tree value for a STG using ACLI

Use the following procedure to restore default spanning tree values for a Spanning Tree Group.

Procedure steps

To restore default values, 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>	Disable the Spanning Tree Group; enter the STG ID.
forward-time	Set the forward time to the default value of 15 seconds.
hello-time	Set the hello time to the default value of 2 seconds.
max-age	Set the maximum age time to the default value of 20 seconds.
priority	Set spanning tree priority (in Hex); if 802.1T compliant, this value must be a multiple of 0x1000.
tagged-bpdu	Set 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	Set the spanning tree multicast MAC address to the default.

Setting STP and STG participation using ACLI

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 set participation, use the following command from Interface Configuration mode:

```
spanning-tree [port <portlist>] [stp <1-8>] [learning {disable
| normal | fast}] [cost <1-65535>] [priority {00 | 10 | < | F0}
```

Variable Definitions

Variable	Value
port <portlist>	Enable the spanning tree for the specified port or ports; enter port or ports you want enabled for the spanning tree. **Important:** 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>	Specify the spanning tree group; enter the STG ID.
learning {disable|normal|fast}	Specify the STP learning mode: • disable: disables FastLearn mode • normal: changes to normal learning mode • fast: enables FastLearn mode
cost <1-65535>	Enter the path cost of the spanning tree; range is from 1–65535.
[priority {00 | 10 | < | F0}	Set the spanning tree priority for a port as a hexadecimal value.

Setting default spanning tree values for ports using ACLI

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 set default values, 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>	Enable spanning tree for the specified port or ports; enter port or ports to be set to factory spanning tree default values. **Important:** 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>	Specify 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	Set the spanning tree learning mode to the factory default value. The default value for learning is Normal mode.
cost	Set the path cost to the factory default value. The default value for path cost depends on the type of port.
priority	Set the priority to the factory default value. The default value for the priority is 0x8000.

Disable spanning tree for a port using ACLI

Use the following procedure to disable spanning tree for a port in a specific Spanning Tree Group.

Procedure steps

To disable, use the following command from Interface Configuration mode:

```
no spanning-tree [port <portlist>] [stp <1-8>]
```

Variable Definitions

Variable	Value
port <portlist>	Disable spanning tree for the specified port or ports; enter port or ports you want disabled for STP. **Important:** If this parameter is omitted, the system uses the port number specified when the interface command was used to enter the Interface Configuration mode.
stp <1-8>	Disable the port in the specified Spanning Tree Group; enter the STG ID.

STP 802.1D compliancy support configuration using ACLI

Use the information in this section to enable or disable STP 802.1D compliancy support on the switch, and to display the STP 802.1D compliancy support configuration status.

Enabling STP 802.1D compliancy support using ACLI

Use the following procedure to enable STP 802.1D compliancy support for the switch.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enable STP 802.1D compliancy support by using the following command:

```
spanning-tree 802dot1d-port-compliance enable
```

Disabling STP 802.1D compliancy support using ACLI

Use the following procedure to disable STP 802.1D compliancy support as required.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Disable STP 802.1D compliancy support by using one of the following commands:

```
no spanning-tree 802dot1d-port-compliance enable
```

```
default spanning-tree 802dot1d-port-compliance enable
```

Viewing STP 802.1D compliancy support status using ACLI

Prerequisites

Use the following procedure to display the administrative and operational status of STP 802.1D compliancy support.

- Log on to the User EXEC mode in ACLI.

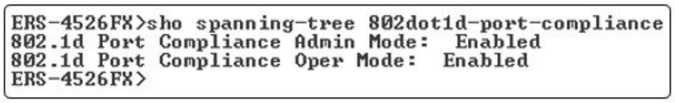
Procedure steps

View STP 802.1D compliancy support by using one of the following commands:

```
show spanning-tree 802dot1d-port-compliance
```

Job aid

The following figure shows sample output for the **`show spanning-tree 802dot1d-port-compliance`** command.



```
ERS-4526FX>sho spanning-tree 802dot1d-port-compliance
802.1d Port Compliance Admin Mode:  Enabled
802.1d Port Compliance Oper Mode:  Enabled
ERS-4526FX>
```

Figure 25: show spanning-tree 802dot1d-port-compliance command output

STP 802.1t cost calculation support configuration using ACLI

Use the information in this section to enable, disable, and display the STP 802.1t cost calculation support configuration status.

Enabling STP 802.1t cost calculation support using ACLI

Use the following procedure to enable STP 802.1t cost calculation support for the switch.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enable STP 802.1t cost calculation support by using the following command:

```
spanning-tree cost-calc-mode dot1t
```

Disabling STP 802.1t cost calculation support using ACLI

Use the following procedure to disable STP 802.1t cost calculation support for the switch.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Disable STP 802.1t cost calculation support by using the following command:

```
default spanning-tree cost-calc-mode
```

Viewing STP 802.1t cost calculation status using ACLI

Use the following procedure to display the administrative and operational status of STP 802.1t cost calculation support.

Prerequisites

- Log on to the Privileged EXEC mode in ACLI.

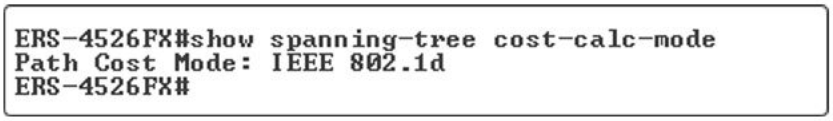
Procedure steps

View STP 802.1t cost calculation support by using the following command:

```
show spanning-tree cost-calc-mode
```

Job aid

The following figure displays sample output for the **show spanning-tree cost-calc-mode** command.



```
ERS-4526FX#show spanning-tree cost-calc-mode
Path Cost Mode: IEEE 802.1d
ERS-4526FX#
```

Managing RSTP using ACLI

This section contains the following procedures:

Configuring RSTP parameters using ACLI

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 in 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>	Set the RSTP forward delay for the bridge in seconds; the default is 15.
hello-time <1- 10>	Set the RSTP hello time delay for the bridge in seconds; the default is 2.
max-age <6 - 40>	Set the RSTP maximum age time for the bridge in seconds; the default is 20.
pathcost-type {bits16 | bits32}	Set the RSTP default path cost version; the default is bits32.
priority {0000 | 1000 | ... | F000}	Set the RSTP bridge priority (in hex); the default is 8000.
tx-hold count	Set the RSTP Transmit Hold Count; the default is 3.
version {stp-compatible | rstp}	Set the RSTP version; the default is rstp.

Configuring RSTP parameters per port using ACLI

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 parameters, 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>	Set the RSTP path cost on the single or multiple ports; the default is 200000.
edge-port {false | true}	Indicate 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}	Enable or disable RSTP on the single or multiple ports; the default is enable.
p2p {auto | force-false | force-true}	Indicate 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}	Set the RSTP port priority on the single or multiple ports; the default is 80.
protocol-migration {false | true}	Force the single or multiple port to transmit RSTP BPDUs when set to true, while operating in RSTP mode; the default is false.

Displaying RSTP bridge-level configuration details using ACLI

Use the following procedure to display the Rapid Spanning Tree Protocol (RSTP) related bridge-level configuration details.

Procedure steps

To display configuration details, use the following command from Privileged EXEC mode:

```
show spanning-tree rstp {config | status | statistics }
```

Variable Definitions

Variable	Value
config	Display RSTP bridge-level configuration.
status	Display RSTP bridge-level role information.
statistics	Display RSTP bridge-level statistics.

Displaying RSTP port-level configuration details using ACLI

Use the following procedure to display the Rapid Spanning Tree Protocol (RSTP) related port-level configuration details.

Procedure steps

To display configuration details, use the following command from Privileged EXEC mode:

```
show spanning-tree rstp port {config | status | statistics |
role} [<portlist>]
```

Variable Definitions

Variable	Value
config	Display RSTP port-level configuration.
status	Display RSTP port-level role information.
statistics	Display RSTP port-level statistics.
role	Display RSTP port-level status.

Configuring RSTP SNMP traps using ACLI

RSTP SNMP traps feature provides the ability to receive SNMP notification about RSTP protocol. These events are also logged to syslog.

The following events are generated:

- **nnRstNewRoot**—a notification that is generated whenever a new root bridge is selected in the topology.
- **nnRstTopologyChange**—a notification that is generated whenever a topology change is detected.
- **nnRstProtocolMigration**—a notification that is generated whenever a protocol migration appears on the port. There are two types of protocol migration: STP BPDU or RSTP BPDU.

Use the following procedures to configure RSTP SNMP Traps when in RSTP operating mode.

Enable RSTP SNMP traps using ACLI

Use the following procedure to enable RSTP SNMP traps.

Procedure steps

To enable RSTP SNMP Traps, use the following command from Global Configuration mode:

```
[no]spanning-tree rstp traps
```

Use the `no` form of this command to disable RSTP SNMP traps.

Reset RSTP SNMP traps settings to default using ACLI

Use the following procedure to reset RSTP SNMP traps settings to default.

Procedure steps

To restore RSTP SNMP traps settings to default, use the following command from Global Configuration mode:

```
default spanning-tree rstp traps
```

Settings are returned to default values.

Verifying RSTP SNMP traps settings using ACLI

Use the following procedure to verify RSTP SNMP traps settings.

Procedure steps

To verify RSTP SNMP Traps settings, use the following command from Privileged EXEC mode:

```
show spanning-tree rstp config
```

Job aid: Verifying RSTP SNMP traps output

```
#show spanning-tree rstp config
Stp Priority (hex):         8000
Stp Version:                Rstp Mode
Bridge Max Age Time:        20 seconds
Bridge Hello Time:          2 seconds
Bridge Forward Delay Time: 15 seconds
Tx Hold Count:              3
Path Cost Default Type:     32-bit
STP Traps:                  Enabled
```

Managing MSTP using ACLI

This section contains the following procedures:

Configuring MSTP parameters for CIST Bridge using ACLI

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 <100 - 4000>][forward-time <4 -
30>][max-age <6 - 40>][pathcost-type {bits16 | bits32}]
[priority {0000 | 1000 | 2000 | ... | F000}] [tx-holdcount <1 -
10>] [version {stp-compatible | rstp| MSTP}] [add-vlan <1 -
4094>] [remove-vlan <1 - 4094>]
```

Variable Definitions

Variable	Value
max-hop <100 - 4000>	Set the MSTP maximum hop count for the CIST bridge; the default is 2000.
forward-time <4 - 30>	Set the MSTP forward delay for the CIST bridge in seconds; the default is 15.
max-age <6 - 40>	Set the MSTP maximum age time for the CIST bridge in seconds; the default is 20.
pathcost-type {bits16 | bits32}	Set the MSTP default path cost version; the default is bits32.
priority {0000 | 1000| 2000 ... | F000}	Set the MSTP bridge priority for the CIST Bridge; the default is 8000.
tx-holdcount<1 - 10>	Set the MSTP Transmit Hold Count; the default is 3.
version {stp-compatible | rstp | MSTP}	Set the MSTP version for the CIST Bridge; the default is MSTP.
add-vlan <1 - 4094>	Add a VLAN to the CIST bridge.
remove-vlan <1 - 4094>	Remove the specified VLAN from the CIST bridge.

Configuring MSTP parameters for Common Spanning Tree using ACLI

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 parameters, 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}][instance-specific <1-7>]
```

Variable Definitions

Variable	Value
port <portlist>	Enter a list or range of port numbers.
cost <1 - 200000000>	Set the MSTP path cost on the single or multiple ports for the CIST; the default is 200000.
hello-time <1 - 10>	Set the MSTP hello time on the single or multiple ports for the CIST; the default is 2.
edge-port {false | true}	Indicate 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}	Enable or disable MSTP on the single or multiple ports; the default is enable.
p2p {auto | force-false | force-true}	Indicate 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}	Set the MSTP port priority on the single or multiple ports; the default is 80.
protocol-migration {false | true}	Force the single or multiple ports to transmit MSTP BPDUs when set to true, while operating in MSTP mode; the default is false.
instance-specific <1-7>	Set the MSTP instance-specific configuration in a range from 1–7 (filter on the MSTP instance).

Configuring MSTP region parameters using ACLI

Use the following procedure to set the MSTP parameters, which include config ID selector, region name, and region version.

Procedure steps

To configure MSTP 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>]	Set the MSTP config ID selector; the default is 0.
[region-name <1 - 32 chars>]	Set the MSTP region name; the default is the bridge MAC address.
[region-version <0 - 65535>]	Set the MSTP region version; the default is 0.

Configuring MSTP parameters for bridge instance using ACLI

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}	Set the MSTP priority for the bridge instance; the default is 8000.
add-vlan <1 - 4094>	Map the specified Vlan and MSTP bridge instance.
remove-vlan <1 - 4094>	Unmap the specified Vlan and MSTP bridge instance.
enable	Enable the MSTP bridge instances.

Disabling a MSTP bridge instance using ACLI

Use the following procedure to disable a MSTP bridge instance.

Procedure steps

To disable, use the following command from Global Configuration mode:

```
no spanning-tree MSTP MSTI <1 - 7> enable
```

Deleting a MSTP bridge instance using ACLI

Use the following procedure to delete a MSTP bridge instance.

Procedure steps

To delete, use the following command from Global Configuration mode:

```
no spanning-tree MSTP MSTI <1 - 7>
```

Displaying MSTP status by selected bridge using ACLI

Use the following procedure to display Multi Spanning Tree Protocol (MSTP) related status information known by the selected bridge.

Procedure steps

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

```
show spanning-tree MSTP {config | status | statistics}
```

Variable Definitions

Variable	Value
config	Display the MSTP-related bridge-level VLAN and region information.

Variable	Value
status	Display the MSTP-related bridge-level status information known by the selected bridge.
statistics	Display the MSTP-related bridge-level statistics.

Displaying MSTP CIST port information using ACLI

Use the following procedure to display the Multi Spanning Tree Protocol (MSTP) CIST Port information maintained by every port of the Common Spanning Tree.

Procedure steps

To display, 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	Display the MSTP CIST port information maintained by every port of the Common Spanning Tree.
role	Display MSTP CIST related port role information maintained by every port.
statistics	Display the MSTP CIST Port statistics maintained by every port.

Displaying MSTP MSTI settings using ACLI

Use the following procedure to display MSTP MSTI settings.

Procedure steps

To display 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	Display the MSTP instance-specific configuration and the VLAN mapping port.
statistics	Display MSTP instance-specific statistics.
port {config | role | statistics}	Display MSTP instance-specific port information: • config: Display MSTI port configuration • role: Display MSTI port role information • statistics: Display MSTI port statistics
<1 - 7>	Specify the MSTI instance for which to display the statistics.

Chapter 11: ADAC configuration using ACLI

You can configure ADAC-related settings using ACLI.

Configuring ADAC globally using ACLI

Use the following procedure to configure ADAC for a switch.

Procedure steps

To configure settings, use the following command from Global Configuration mode:

```
adac [enable] [op-mode <untagged-frames-basic | untagged-
frames-advanced| tagged-frames>] [traps enable] [voice-vlan
<1-4094>] [uplink-port {<portlist> | spbm}][call-server-port
<portlist>]
```

Variable Definitions

Variable	Value
`enable`	Enables ADAC on the switch.
`op-mode <untagged-frames-basic| untagged-frames-advanced | tagged-frames >`	Sets the ADAC operation mode to one of the following: • untagged-frames-basic: IP Phones send untagged frames, and the Voice VLAN is not created. • untagged-frames-advanced: IP Phones send untagged frames, and the Voice VLAN is created. • tagged-frames: IP Phones send tagged frames.

Variable	Value
`traps enable`	Enables ADAC trap notifications.
`voice-vlan <1-4094>`	Sets the Voice VLAN ID. The assigned VLAN ID must first be created.
`uplink-port <portlist>`	Configures a maximum of 8 ports as Uplink ports.
`spbm`	Sets the Uplink over SPBM.
`call-server-port <portlist>`	Configures a maximum of 8 ports as Call Server ports.

Disabling ADAC globally using ACLI

Use the following procedure to disable ADAC for a switch.

Procedure steps

To disable or clear settings, use the following command from Global Configuration mode:

```
no adac [enable] [traps enable] [voice-vlan] [uplink-port]
[call-server-port]
```

Variable Definitions

Variable	Value
`enable`	Disables ADAC on the switch.
`traps enable`	Disables ADAC trap notifications.
`voice-vlan`	Clears the Voice VLAN ID.
`uplink-port`	Clears the Uplink ports.
`call-server-port`	Clears Call Server ports.

Restoring default ADAC settings using ACLI

Use the following procedure to restore default ADAC settings on a device.

Procedure steps

To restore default settings, use the following command from Global Configuration mode:

```
default adac [enable] [op-mode] [traps enable] [voice-vlan]
[uplink-port] [call-server-port]
```

If you do not specify any of the following parameters in the **default adac** command, the command restores the default settings for all of these parameters.

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 per port ADAC settings using ACLI

Use the following procedure to configure per port ADAC for a device.

Procedure steps

To configure ADAC settings, use the following command from Interface Configuration mode:

```
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.
`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 • tagAll • tagPvidOnly • untagPvidOnly Use no-change to keep the current setting.

Disable ADAC settings per port using ACLI

Use the following procedure to disable ADAC settings per port.

Procedure steps

To disable ADAC settings, use the following command from Interface Configuration mode:

```
no adac [port <portlist>] [enable]
```

Variable Definitions

Variable	Value
`port <portlist>`	Ports for which to disable ADAC.
`enable`	Disables ADAC on the port or ports listed.

Configuring per port ADAC defaults for a specified port using ACLI

Use the following procedure to configure per port ADAC defaults for a specified port.

Procedure steps

To configure defaults, 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 the autodetection method using ACLI

Use the following procedure to configure the autodetection 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:

```
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.

Disabling autodetection using ACLI

Use the following procedure to turn off the autodetection method for either MAC address or LLDP.

Procedure steps

To disable 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 disable the detection mode.
mac	Disables the MAC address detection mode.
lldp	Disables the LLDP detection mode.

Setting autodetection method to default using ACLI

Use the following procedure to return the autodetection method to its defaults. The default is to have both MAC and LLDP enabled.

Procedure steps

To return 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.
lldp	LLDP is enabled by default.

Configuring autodetection for a specified port using ACLI

Use the following procedure to enable autodetection on specified ports.

Procedure steps

To enable autodetection, use the following command from Interface Configuration mode:

```
adac port <port-list> enable
```

Disabling autodetection on specified ports using ACLI

Use the following procedure to disable autodetection on the specified port(s).

Procedure steps

To disable autodetection, use the following command from Interface Configuration mode:

```
no adac port <port-list> enable
```

Restoring default ADAC setting for ports using ACLI

Use the following procedure to restore the default ADAC setting (disabled) for the specified ports.

Procedure steps

To restore the default setting (disabled), use the following command from Global Configuration mode:

```
default adac [port <port-list>] enable
```

Adding a range of MAC addresses for autodetection using ACLI

Use the following procedure to add a specified range to the table of MAC addresses recognized as Avaya IP Phones by the autodetection process.

Procedure steps

To add a range of addresses, use the following command on Global Configuration mode:

```
adac mac-range-table low-end <MACaddress> high-end <MACaddress>
```

Deleting a range of MAC addresses used by autodetection using ACLI

Use the following procedure to delete an existing MAC address range used by the autodetection process. If the low-end and high-end MAC address values are not provided, the switch deletes all existing MAC address ranges from the switch.

Procedure steps

To delete a range of addresses, use the following command from Global Configuration mode:

```
no adac mac-range-table low-end <MACaddress> high-end
<MACaddress>
```

Resetting supported MAC address ranges using ACLI

Use the following procedure to restore all supported MAC address ranges on the switch to their default values.

Procedure steps

To reset to default values, use the following command from Global Configuration mode:

```
default adac mac-range-table
```

Displaying global ADAC settings for a device using ACLI

Use the following procedure to display global ADAC settings for a device.

Procedure steps

To display settings, use the following command in Privileged EXEC mode:

```
show adac
```

Displaying ADAC settings per port using ACLI

Use the following procedure to display ADAC settings per port.

Procedure steps

To display ADAC settings, use the following command from Privileged EXEC mode:

```
show adac interface <interface-type> <slot/port>
```

Displaying configured ADAC MAC ranges using ACLI

Use the following procedure to display the ADAC MAC ranges configured on the switch.

Procedure steps

To display ranges, use the following command from Privileged EXEC mode:

```
show adac mac-range-table
```

Displaying detection mechanism configured per port using ACLI

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>]
```

Enabling ADAC uplink over SPBM

Use this procedure to enable ADAC uplink over SPBM.

Procedure

1. Enter Global Configuration Mode:

   ```
   enable
   configure terminal
   ```

2. To enable ADAC uplink over SPBM, enter the following command at the command prompt:

   ```
   adac uplink-port spbm
   ```

ADAC UFA configuration example

The following figure is 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 4000 series switch.)

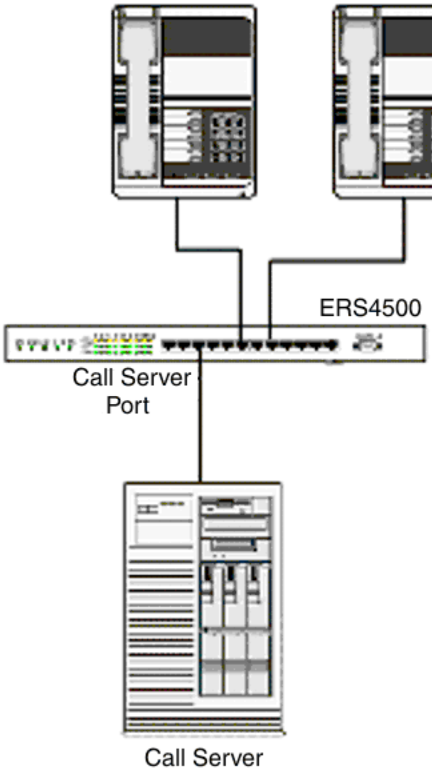


Figure 26: ADAC UFA configuration example

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. (Autodetection 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 the preceding figure, 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.

ADAC ACLI configuration commands

The following section describes the detailed ACLI commands required to carry out the configuration shown in Figure 26: ADAC UFA configuration example on page 162.

```
(config)#vlan create 2 type port voice-vlan
(config)#adac  call-server-port  7
(config)#adac  voice-vlan  2
(config)#adac  enable  op-mode  untagged-frames-advanced
(config)#interface  Ethernet  all
(config-if)#interface  Ethernet  16,24
(config-if)#adac enable
```

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
```

```
(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

```
ERS4000#show running-config module adac

! Embedded ASCII Configuration Generator Script
! Base model = Ethernet Routing Switch 4524GT
! Base Software version = v5.4.0.074
! Stack info:
!Unit# Switch Model     Pluggable Pluggable Pluggable Pluggable SW Version
!                         Port      Port      Port      Port
!----- ---------------- --------- --------- --------- --------- ----------
!1     4524GT           (21) None (22) None (23) None (24) None v5.4.0.074
!2     4526GTX          (21) None (22) None (23) None (24) None v5.4.0.074
!                       (25) None (26) None
!
! Displaying only parameters different to default
!================================================
enable
configure terminal
!
! *** ADAC ***
!
adac voice-vlan 101
adac uplink-port 2/25,2/26
adac op-mode tagged-frames
adac enable
```

```
ERS4000#show running-config verbose module adac

! Embedded ASCII Configuration Generator Script
! Base model = Ethernet Routing Switch 4524GT
! Base Software version = v5.4.0.074
! Stack info:
!Unit# Switch Model     Pluggable Pluggable Pluggable Pluggable SW Version
!                         Port      Port      Port      Port
!----- ---------------- --------- --------- --------- --------- ----------
!1     4524GT           (21) None (22) None (23) None (24) None v5.4.0.074
!2     4526GTX          (21) None (22) None (23) None (24) None v5.4.0.074
!                       (25) None (26) None
!
! Displaying all switch parameters
!================================================
enable
configure terminal
!
! *** ADAC ***
!
no adac enable
no adac mac-range-table
interface Ethernet ALL
adac detection port 1/1-24,2/1-26 mac
adac detection port 1/1-24,2/1-26 lldp
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 mac-range-table low-end 00-13-65-FE-F3-2C high-end 00-13-65-FF-ED-2B
adac mac-range-table low-end 00-15-9B-FE-A4-66 high-end 00-15-9B-FF-24-B5
adac mac-range-table low-end 00-16-CA-00-00-00 high-end 00-16-CA-01-FF-FF
adac mac-range-table low-end 00-16-CA-F2-74-20 high-end 00-16-CA-F4-BE-0F
adac mac-range-table low-end 00-17-65-F6-94-C0 high-end 00-17-65-F7-38-CF
adac mac-range-table low-end 00-17-65-FD-00-00 high-end 00-17-65-FF-FF-FF
adac mac-range-table low-end 00-18-B0-33-90-00 high-end 00-18-B0-35-DF-FF
adac mac-range-table low-end 00-19-69-83-25-40 high-end 00-19-69-85-5F-FF
adac voice-vlan 101
no adac call-server-port
adac uplink-port 2/25,2/26
adac op-mode tagged-frames
adac enable
```

Chapter 12: LACP and VLACP configuration using ACLI

The ACLI commands in this section help you to create and manage Link Aggregation Control Protocol (LACP) and Virtual LACP (VLACP).

Configuring LACP using ACLI

This section describes the procedures necessary to configure and manage Link Aggregation using the Command Line Interface (ACLI).

Displaying LACP settings using ACLI

Use the following procedure to display system-wide LACP settings.

Procedure steps

To display settings, use the following command from Privileged EXEC mode:

```
show lacp system
```

Displaying per port LACP configuration information using ACLI

Use the following procedure to display per port LACP configuration information.

Procedure steps

To display configuration information, 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 statistics using ACLI

Use the following procedure to display LACP port statistics.

Procedure steps

To display 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 using ACLI

Use the following procedure to clear LACP port statistics.

Procedure steps

To clear statistics, use the following command from Interface Configuration mode:

```
lacp clear-stats <portList>
```

Displaying port debug information using ACLI

Use the following procedure to display port debug information.

Procedure steps

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

```
show lacp debug member [<portList>]
```

Displaying LACP aggregators or LACP trunks using ACLI

Use the following procedure to display LACP aggregators or LACP trunks.

Procedure steps

To display LACP aggregators or trunks, use the following command from Privileged EXEC mode:

```
show lacp aggr <1-65535>
```

Configuring LACP system priority using ACLI

Use the following procedure to set the system-wide LACP priority. The factory default priority value is 32768.

Procedure steps

1. To set the priority, use the following command from Global Configuration mode:

   ```
   lacp system-priority <0-65535>
   ```

2. To reset the priority level to default, use the following command from Global Configuration mode:

   ```
   default lacp system-priority
   ```

Enabling port aggregation mode using ACLI

Use the following procedure to enable the port aggregation mode.

Procedure steps

1. To enable the aggregation mode, use the following command from Interface Configuration mode:

   ```
   lacp aggregation [port <portList>] enable
   ```

2. To reset the aggregation mode to default, use the following command from Interface Configuration mode:

   ```
   default lacp aggregation
   ```

Disabling port aggregation mode using ACLI

Use the following procedure to disable the port aggregation mode.

Procedure steps

To disable, use the following command from Interface Configuration mode:

```
no lacp aggregation [port <portList>] enable
```

Configuring administrative LACP key using ACLI

Use the following procedure to configure the administrative LACP key for a set of ports.

Procedure steps

1. To configure the administrative LACP key, use the following command from Interface Configuration mode:

   ```
   lacp key [port <portList>] <1-4095>
   ```

2. To reset the LACP key value to default, use the following command from Interface Configuration mode:

   ```
   default lacp key
   ```

Variable Definitions

Variable	Value
port <portList>	The ports to configure the LACP key for.
<1-4095>	The LACP key to use.

Configuring LACP mode of operation using ACLI

Use the following procedure to configure the LACP mode of operations for a set of ports.

Procedure steps

1. To configure the mode, use the following command from Interface Configuration mode:

   ```
   lacp mode [port <portList>] {active | passive | off}
   ```

2. To reset the mode to default value, use the following command from Interface Configuration mode:

   ```
   default lacp mode [port <portList>]
   ```

Variable Definitions

Variable	Value
port <portList>	The ports for which the LACP mode is to be set.
{active | passive | off}	The type of LACP mode to set for the port. The LACP modes are: • 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. • 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. • off — The port does not participate in Link Aggregation. LACP requires at least one end of each link to be in active mode.

Configuring per port LACP priority using ACLI

Use the following procedure to configure the per-port LACP priority for a set of ports.

Procedure steps

1. To configure the priority, use the following command from Interface Configuration mode:

   ```
   lacp priority [port <portList>] <0-65535>
   ```

2. To reset the priority to default, use the following command from Interface Configuration mode:

   ```
   default lacp priority [port <portList>]
   ```

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 using ACLI

Use the following procedure to configure the LACP periodic transmission timeout interval for a set of ports.

Procedure steps

1. To configure the timeout, use the following command from Interface Configuration mode:

   ```
   lacp timeout-time [port <portList>] {long | short}
   ```

2. To reset the timeout value to default, use the following command from Interface Configuration mode:

   ```
   default lacp timeout-time [port <portList>]
   ```

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 Static LACP Key to Trunk ID binding

Use the following procedures to configure and manage Static LACP Key to Trunk ID binding using ACLI.

Note:

Partner configuration is also required. The local ports do not aggregate if the remote ends of the links are not part of a similar configuration.

Binding an LACP key to a specific trunk ID

Use this procedure to bind an LACP key to a specific MLT ID.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   lacp key <1-4095> mlt-id <1-32>
   ```

Example

The following is an example of key binding using ACLI interface:

```
UNIT>enable
UNIT#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
UNIT(config)#lacp key 11 mlt-id 11
```

Variable Definitions

Variable	Value
<1-4095>	The LACP key to use.
<1-32>	The MLT ID.

Deleting an LACP key binding to a trunk ID

Use this procedure to delete an LACP key binding to a trunk ID.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   default lacp key <1-4095>
   ```

   Note:

   The MLT ID for the defaulted LACP key becomes 0.

Variable Definitions

Variable	Value
<1-4095>	The LACP key to use.

Displaying LACP key bindings to trunk IDs

Use this procedure to display LACP key bindings to trunk IDs.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Use the following command to display all LACP key bindings:

```
show lacp key
```

3. Use the following command to display a specific LACP binding:

```
show lacp key <1-4095>
```

Variable Definitions

Variable	Value
<1-4095>	The LACP key to use.

Configuring VLACP using ACLI

To configure VLACP using ACLI, see the following procedures:

ⓘ **Important:**

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

Enabling VLACP using ACLI

Use the following procedure to globally enable VLACP for a device.

Procedure steps

To enable VLACP, use the following command from Global Configuration mode:

```
vlacp enable
```

Configuring multicast MAC address for VLACP using ACLI

Use the following procedure to set the multicast MAC address used by the device for VLACPDUs.

Procedure steps

To configure the address, use the following command from Global Configuration mode:

```
vlacp macaddress <macaddress>
```

Configuring VLACP parameters per port using ACLI

Use the following procedure to configure VLACP parameters per port.

Procedure steps

To configure VLACP parameters, use the following command in Interface Configuration mode:

```
vlacp port <slot/port> [enable] [timeout <long/short>] [fast-
periodic-time <integer>] [slow-periodic-time <integer>]
[timeout-scale <integer>] [funcmac-addr <mac>] [ethertype
<hex>]
```

Variable Definitions

Variable	Value
`<slot/port>`	Specifies the slot and port number.
`enable`	Enables VLACP.
`timeout <long/short>`	Specifies whether the timeout control value for the port is a long or short timeout. • long— sets the port timeout value to: (timeout-scale value) × (slow-periodic-time value). • short— sets the port's timeout value to: (timeout-scale value) × (fast-periodic-time value). For example, if the timeout is set to short while the timeout-scale value is 5 and the fast-periodic-time value is 500 ms, the timer expires after 2500 ms. Default is long.

Variable	Value
`fast-periodic-time <integer>`	Specifies the number of milliseconds between periodic VLACPDU transmissions using short timeouts. 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. 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). The range is 1-10. Default is 3. ✱ **Note:** When you use fast-timers, you do not use a timeout-scale of 1, because this breaks the link continuity from service due to the time taken to transmit VLACPDU and for the partner to provide a corresponding response. Avaya recommends that you set the minimum timeout-scale to 3. Avaya also recommends that you use the minimum setting of 5 for the timeout-scale when using the fast-periodic-timer of 500 ms.
`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. ✱ **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.

Variable	Value
	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.

Disabling VLACP using ACLI

Use the following procedure to disable VLACP for a device.

Procedure steps

To disable VLACP, use the following command from Global Configuration mode:

```
no vlacp enable
```

Resetting multicast MAC address for VLACP to default using ACLI

Use the following procedure to reset the multicast MAC address used by the device for VLACPDUs to the default value (01:80:c2:00:11:00).

Procedure steps

To reset the address to default, use the following procedure from Global Configuration mode:

```
no vlacp macaddress
```

Disabling VLACP on a port using ACLI

Use the following procedure to disable VLACP on a port.

Procedure steps

To disable VLACP, use the following command from Global Configuration mode:

```
no vlacp <slot/port> [enable] [funcmac-addr]
```

Variable Definitions

Variable	Value
`<slot/port>`	Specifies the slot and port number.
`enable`	Disables VLACP on the specified port.
`funcmac-addr`	Sets the funcmac-addr parameter to the default value.

Displaying VLACP status using ACLI

Use the following procedure to display the status of VLACP on a switch.

Procedure steps

To display the status, use the following command from Privileged EXEC mode:

```
show vlacp
```

Displaying VLACP configuration details for ports using ACLI

Use the following procedure to display the VLACP configuration details for a port or list of ports.

Procedure steps

To display configuration details, use the following command from Privileged EXEC mode:

```
show vlacp interface <slot/port>
```

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 and OPER ENABLED are true;then that port did not yet receive any VLACPDUs.

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.

The **show vlacp interface** command is in the privExec command mode.

As long as the VLACP functional address for a specifc interface is not changed when using the (config-if)# **vlacp port x funcmac-addr H.H.H** command, the MAC address is displayed as 00:00:00:00:00:00. The MAC address used for sending VLACP PDUs for an interface is the global VLACP MAC address (01:80:c2:00:11:00). The VLACP global destination MAC can be specifed by the user. Setting a func-mac-addr on an interface displays that address in the show vlacp interface instead of 00:00:00:00:00:00.

Chapter 13: VLAN Configuration using Enterprise Device Manager

This chapter describes how to create and manage a VLAN using Enterprise Device Manager (EDM).

VLAN management using EDM

Use the information in this section to view, create, and manage VLAN configurations for a switch or stack.

Viewing VLAN information using EDM

Use this procedure to display VLAN configuration information for a switch or stack.

Procedure steps

1. From the navigation tree, choose **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.

Variable definitions

Use the data in this table to help you understand the VLAN display.

Variable	Value
Id	Indicates the VLAN ID for the VLAN.
Name	Indicates the name of the VLAN.
IfIndex	Indicates the interface index.
Type	Indicates the VLAN type as defined by the policy used to define the VLAN port membership. Values include: • byPort—VLAN by Port • byProtocolId—VLAN by Protocol ID • spbm-bvlan — SPBM B-VLAN • spbm-switchedUni — SPBM switched UNI VLAN

Variable	Value
VoiceEnabled	Indicates whether VLAN is a voice VLAN (true) or not (false).
RspanEnabled	Indicates whether VLAN is an RSPAN VLAN (true) or not (false).
I-sid	Indicates the VLAN I-SID ID.
PortMembers	Indicates the ports that are members of the VLAN.
ActiveMembers	Indicates the 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	Indicates the STG to which the selected VLAN belongs. **Important:** This column is available only when the switch is operating in the STG mode. Avaya Ethernet Routing Switch 4000 Series does not support multiple STGs when operating in the STG mode.
MstpInstance	Indicates the MSTP instance associated with the VLAN. Values include: • none • cist • msti-1-7 **Important:** This column is available only when the switch is operating in the MSTP mode.
ProtocolId	Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is *byProtocolId*. Values include: • ip • ipx802dot3 • ipx802dot2 • ipxSnap • ipxEthernet2 • decLat • sna802dot2 • snaEthernet2 • netBios • xns • vines • ipv6

Variable	Value
	• usrDefined • rarp
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN.
Encap	Indicates the encapsulation type for user defined protocol based VLANs only. Values include: • ethernet2 • llc • snap By default there is no value in this cell.
MacAddress	Indicates the MAC address associated with the VLAN.
Routing	Indicates whether routing is enabled (true) or disabled (false) for the VLAN.

Modifying an existing VLAN in STG mode using EDM

Use this procedure to modify the configuration of an existing VLAN when the Spanning Tree administration operating mode is avayaStpg.

Prerequisites

- Select avayaStpg for the Spanning Tree administration mode.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN to edit, click the VLAN ID.
5. In the VLAN row, double-click the cell in the **Name** column.
6. Type a character string to assign a unique name to the VLAN.
7. In the VLAN row, double-click the cell in the **PortMembers** column.
8. Select ports to add to the VLAN.

   OR

   Deselect ports to remove them from the VLAN.
9. Click **Ok** .
10. In the VLAN row, double-click the cell in the **StgId** column.

11. Type a value.
12. In the VLAN row, double-click the cell in the **Routing** column.
13. Select a value from the list—**true** to enable routing for the VLAN, or **false** to disable routing for the VLAN .
14. Click **Apply** .

Variable definitions

Use the data in this table to modify the configuration of an existing VLAN in STG mode.

Variable	Value
Id	Indicates the ID for the VLAN. This is a read-only value.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
IfIndex	Indicates the interface index. This is a read-only value.
Type	Indicates the type of VLAN: byPort. This is a read-only value. Values include: • byPort • byProtocolId • spbm-bvlan • spbm-switchedUni
PortMembers	Specifies the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.
StgId	Specifies the STG to associate with the selected VLAN or VLANs. This is a read-only value. **Important:** This column is available only when the Spanning Tree administration operating mode is avayaSTG mode, when the operating mode is MSTP or RSTP, this column is not available.
ProtocolId	Specifies the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is *byProtocolId*. Values include: • ip • ipx802dot3 • ipx802dot2 • ipxSnap • ipxEthernet2 • decLat

Variable	Value
	• sna802dot2 • snaEthernet2 • netBios • xns • vines • ipv6 • usrDefined • rarp
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN. This is a read-only value.
Encap	Indicates the encapsulation type for user defined protocol based VLANs only. This is a read-only value. Values include: • ethernet2 • llc • snap • all • notapplicable By default there is no value in this cell.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Specifies whether routing is enabled (true) or disabled (false) for the VLAN.

Modifying an existing VLAN in RSTP mode using EDM

Use this procedure to modify the configuration of an existing VLAN when the Spanning Tree administration operating mode is RSTP.

Prerequisites

- Select RSTP for the Spanning Tree administration mode.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.

3. In the work area, click the **Basic** tab.
4. To select a VLAN to edit, click the VLAN ID.
5. In the VLAN row, double-click the cell in the **Name** column.
6. Type a character string to assign a unique name to the VLAN.
7. In the VLAN row, double-click the cell in the **PortMembers** column.
8. Select ports to add to the VLAN.

   OR

   Deselect ports to remove them from the VLAN.
9. Click **Ok** .
10. In the VLAN row, double-click the cell in the **Routing** column.
11. Select a value from the list—**true** to enable routing for the VLAN, or **false** to disable routing for the VLAN .
12. Click **Apply** .

Variable definitions

Variable	Value
Id	Indicates the ID for the VLAN. This is a read-only value.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
IfIndex	Indicates the interface index. This is a read-only value.
Type	Indicates the type of VLAN: byPort. This is a read-only value. Values include: • byPort • byProtocolId • spbm-bvlan • spbm-switchedUni
PortMembers	Specifies the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.
ProtocolId	Specifies the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is *byProtocolId*. Values include: • ip • ipx802dot3

Variable	Value
	• ipx802dot2 • ipxSnap • ipxEthernet2 • decLat • sna802dot2 • snaEthernet2 • netBios • xns • vines • ipv6 • usrDefined • rarp
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN. This is a read-only value.
Encap	Indicates the encapsulation type for user defined protocol based VLANs only. This is a read-only value. Values include: • ethernet2 • llc • snap • all • notapplicable By default there is no value in this cell.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Specifies whether routing is enabled (true) or disabled (false) for the VLAN.

Modifying an existing VLAN in MSTP mode using EDM

Use this procedure to modify the configuration of an existing VLAN when the Spanning Tree administration operating mode is MSTP.

Prerequisites

- Select MSTP for the Spanning Tree administration mode.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN to edit, click the VLAN ID.
5. In the VLAN row, double-click the cell in the **Name** column.
6. Type a character string to assign a unique name to the VLAN.
7. In the VLAN row, double-click the cell in the **PortMembers** column.
8. Select ports to add to the VLAN.

   OR

   Deselect ports to remove them from the VLAN.
9. Click **Ok** .
10. In the VLAN row, double-click the cell in the **MstpInstance** column, if the switch is in MSTP mode.
11. Select a value from the list.
12. In the VLAN row, double-click the cell in the **Routing** column.
13. Select a value from the list—**true** to enable routing for the VLAN, or **false** to disable routing for the VLAN .
14. Click **Apply** .

Variable definitions

Variable	Value
Id	Indicates the ID for the VLAN. This is a read-only value.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
IfIndex	Indicates the interface index. This is a read-only value.
Type	Indicates the type of VLAN: byPort. This is a read-only value. Values include:

Variable	Value
	• byPort • byProtocolId • spbm-bvlan • spbm-switchedUni
PortMembers	Specifies the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.
MstpInstance	The MSTP instance associated with the VLAN. Values include: • none • cist • msti-1-7 **Important:** This column is available only when the Spanning Tree administration operating mode is MSTP, when the operating mode is avayaSTG or RSTP, this column is not available .
ProtocolId	Specifies the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is *byProtocolId*. Values include: • ip • ipx802dot3 • ipx802dot2 • ipxSnap • ipxEthernet2 • decLat • sna802dot2 • snaEthernet2 • netBios • xns • vines • ipv6 • usrDefined • rarp
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN. This is a read-only value.
Encap	Indicates the encapsulation type for user defined protocol based VLANs only. This is a read-only value. Values include:

Variable	Value
	• ethernet2 • llc • snap • all • notapplicable By default there is no value in this cell.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Specifies whether routing is enabled (true) or disabled (false) for the VLAN.

Creating a VLAN in STP mode using EDM

Use the following procedure to create a new VLAN when the Spanning Tree administration operating mode is avayaStpg.

Prerequisites

- Select avayaStpg for the Spanning Tree administration mode.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. Click **Insert**.
5. In the Id dialog box, type a value.

   OR

   Accept the default ID for the VLAN.
6. In the Name dialog box, type a value.

   OR

   Accept the default name for the VLAN.
7. In the **Type** section, click a radio button.
8. Click **Insert**.

9. In the VLAN row, double-click the cell in the **PortMembers** column.
10. Select ports to add to the VLAN.

    OR

    Deselect ports to remove them from the VLAN.
11. Click **Ok** .
12. In the VLAN row, double-click the cell in the **StgId** column.
13. Type a value.
14. In the VLAN row, double-click the cell in the **Routing** column.
15. Select a value from the list—true to enable routing for the VLAN, or false to disable routing for the VLAN .
16. Click **Apply** .

Variable definitions

Variable	Value
Id	Specifies the ID for the VLAN.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
Type	Indicates the type of VLAN. This is a read-only value. Values include: • byPort • byProtocolId • spbm-bvlan • spbm-switchedUni
PortMembers	Specifies the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.
StgId	Specifies the STG to associate with the selected VLAN or VLANs. This is a read-only value. **Important:** This column is available only when the Spanning Tree administration operating mode is avayaSTG mode, when the operating mode is MSTP or RSTP, this column is not available.
ProtocolId	Specifies the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is *byProtocolId*. Values include:

Variable	Value
	• ip • ipx802dot3 • ipx802dot2 • ipxSnap • ipxEthernet2 • decLat • sna802dot2 • snaEthernet2 • netBios • xns • vines • ipv6 • usrDefined • rarp
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN. This is a read-only value.
Encap	Indicates the encapsulation type for user defined protocol based VLANs only. This is a read-only value. Values include: • ethernet2 • llc • snap • all • notapplicable By default there is no value in this cell.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Specifies whether routing is enabled (true) or disabled (false) for the VLAN.

Creating a VLAN in RSTP mode using EDM

Use the following procedure to create a new VLAN when the switch is in RSTP mode.

Prerequisites

- Select RSTP for the Spanning Tree administration mode.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. Click **Insert**.
5. In the Id dialog box, type a value.

   OR

   Accept the default ID for the VLAN.
6. In the Name dialog box, type a value.

   OR

   Accept the default name for the VLAN.
7. Click **Insert**.
8. In the VLAN row, double-click the cell in the **PortMembers** column.
9. Select ports to add to the VLAN.

   OR

   Deselect ports to remove them from the VLAN.
10. Click **Ok** .
11. In the VLAN row, double-click the cell in the **Routing** column.
12. Select a value from the list—**true** to enable routing for the VLAN, or **false** to disable routing for the VLAN .
13. Click **Apply** .

Variable definitions

Variable	Value
Id	Specifies the ID for the VLAN.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.

Variable	Value
Type	Indicates the type of VLAN. This is a read-only value. Values include: • byPort • byProtocolId • spbm-bvlan • spbm-switchedUni
PortMembers	Specifies the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.
ProtocolId	Specifies the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is *byProtocolId*. Values include: • ip • ipx802dot3 • ipx802dot2 • ipxSnap • ipxEthernet2 • decLat • sna802dot2 • snaEthernet2 • netBios • xns • vines • ipv6 • usrDefined • rarp
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN. This is a read-only value.
Encap	Indicates the encapsulation type for user defined protocol based VLANs only. This is a read-only value. Values include: • ethernet2 • llc • snap • all • notapplicable

Variable	Value
	By default there is no value in this cell.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Specifies whether routing is enabled (true) or disabled (false) for the VLAN.

Creating a VLAN in MSTP mode using EDM

Use the following procedure to create a new VLAN when the switch is in MSTP mode.

Prerequisites

- Select MSTP for the Spanning Tree administration mode.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. Click **Insert**.
5. In the Id dialog box, type a value.

   OR

   Accept the default ID for the VLAN.
6. In the Name dialog box, type a value.

   OR

   Accept the default name for the VLAN.
7. Click the **MstpInstance** box arrow.
8. Select a value from the list.
9. Click **Insert**.
10. In the VLAN row, double-click the cell in the **PortMembers** column.
11. Select ports to add to the VLAN.

    OR

    Deselect ports to remove them from the VLAN.

12. Click **Ok** .
13. In the VLAN row, double-click the cell in the **Routing** column.
14. Select a value from the list—**true** to enable routing for the VLAN, or **false** to disable routing for the VLAN .
15. Click **Apply** .

Variable definitions

Variable	Value
Id	Specifies the ID for the VLAN.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
IfIndex	Indicates the interface index. This is a read-only value.
Type	Indicates the type of VLAN. This is a read-only value. Values include: • byPort • byProtocolId • spbm-bvlan • spbm-switchedUni
PortMembers	Specifies the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.
MstpInstance	The MSTP instance associated with the VLAN. Values include: • none • cist • msti-1-7 **Important:** This column is available only when the Spanning Tree administration operating mode is MSTP, when the operating mode is avayaSTG or RSTP, this column is not available.
ProtocolId	Specifies the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is *byProtocolId*. Values include: • ip • ipx802dot3

Variable	Value
	• ipx802dot2 • ipxSnap • ipxEthernet2 • decLat • sna802dot2 • snaEthernet2 • netBios • xns • vines • ipv6 • usrDefined • rarp
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN. This is a read-only value.
Encap	Indicates the encapsulation type for user defined protocol based VLANs only. This is a read-only value. Values include: • ethernet2 • llc • snap • all • notapplicable By default there is no value in this cell.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Specifies whether routing is enabled (true) or disabled (false) for the VLAN.

Deleting a VLAN using EDM

Use this procedure to delete a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN to delete, click the VLAN ID.
5. Click **Delete**.
6. Click **Yes**.

Creating an RSPAN VLAN using EDM

Use the following procedure to create an RSPAN VLAN.

Procedure

1. From the navigation tree, double-click **`VLAN`**.
2. Double-click **`VLANs`**.
3. In the work area, click the **`Basic`** tab.
4. Click **`Insert`**.
5. In the **`Id`** dialog box, type a value.
6. In the **`Name`** dialog box, type a value.
7. In the **`StgId`** dialog box, type a value.
8. In the **`Type`** section, click the **`byPort`** radio button.
9. Select the RspanEnabled check box.
10. Click **`Insert`**.

Note:

A VLAN cannot be VOICE VLAN and RSPAN VLAN at the same time.

Variable definitions

Variable	Value
Id	Specifies the ID for the VLAN.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
StgId	Specifies the Spanning Tree Group ID
Type	Indicates the type of VLAN. This is a read-only value.
VoiceEnabled	Indicates whether VLAN is a voice VLAN (true) or not (false).
RspanEnabled	Indicates whether VLAN is an RSPAN VLAN (true) or not (false).

Configuring VLAN Snoop

Use this procedure to enable or disable IGMP snooping on a switch.

For information on the IGMP snooping feature, refer to *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4000 Series*, NN47205-506.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **VLANs**.
3. Select the **Snoop** tab.

Variable definitions

The following table outlines the parameters of the **Snoop** tab.

Table 9: VLAN Snoop tab parameters

Variable	Value
Id	Specifies the ID of the VLAN.
ReportProxyEnable	A flag to note whether IGMP Report Proxy is enabled on this VLAN.

Variable	Value
Enable	A flag to note whether IGMP Snooping is enabled on this VLAN.
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

VLAN IPv4 address management using EDM

Use the information in this section to display and delete IPv4 address information for a VLAN.

Viewing VLAN IPv4 address information using EDM

Use this procedure to display IPv4 addresses associated with VLANs.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN to edit, click the VLAN ID.

5. On the toolbar, click **IP**.
6. In the work area, click the **IP Address** tab.

Variable definitions

Variable	Value
IpAddress	Indicates the IPv4 address associated with the VLAN.
NetMask	Indicates the network mask for the IPv4 address associated with the VLAN.
VlanId	Indicates the VLAN identifier.
MacOffset	Indicates the offset used to translate the IPv4 address into a MAC address. Values range from 1 to 256.

Assigning an IPv4 address to a using EDM

Use this procedure to assign an IPv4 address to a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN to edit, click the VLAN ID.
5. On the toolbar, click **IP**.
6. In the work area, click the **IP Address** tab.
7. Click **Insert** .
8. In the IpAddress dialog box, type an IP address.
9. In the NetMask dialog box, type a network mask.
10. In the MacOffset dialog box, type a value.
11. Click **Insert** .
12. Click **Apply** .

Variable definitions

Variable	Value
IpAddress	Indicates the IPv4 address associated with the VLAN.
NetMask	Indicates the network mask for the IPv4 address associated with the VLAN.
VlanId	Indicates the VLAN identifier.
MacOffset	Indicates the offset used to translate the IPv4 address into a MAC address. Values range from 1 to 256.

Deleting an IPv4 address from a VLAN using EDM

Use this procedure to delete VLAN IPv4 address from a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN to edit, click the VLAN ID.
5. On the toolbar, click **IP**.
6. In the work area, click the **IP Address** tab.
7. Click the IPv4 address row.
8. On the toolbar, click **Delete** .

Configuring DHCP for a VLAN using EDM

Use this procedure to disable or enable, and configure Dynamic Host Configuration Protocol (DHCP) for a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN to edit, click the VLAN ID.
5. On the toolbar, click **IP**.
6. In the work area, click the **DHCP** tab.
7. Select the **Enable** check box to enable DHCP for the VLAN.

   OR

   Clear the **Enable** check box to disable DHCP for the VLAN.
8. In the MinSec dialog box, type a value.
9. In the **Mode** section, click a radio button.
10. Select the **AlwaysBroadcast** check box to enable the broadcast of DHCP reply packets for the VLAN.

    OR

    Clear the **AlwaysBroadcast** check box to disable the broadcast of DHCP reply packets for the VLAN.
11. Select the **Option82Enabled** check box to enable DHCP option 82 for the VLAN.

    OR

    Clear the **Option82Enabled** check box to disable DHCP option 82 for the VLAN.
12. In the **ClearCounters** section, click a radio button.
13. Click **Apply** .

Variable definitions

Variable	Value
Enable	Enables or disables DHCP for the VLAN.
MinSec	Specifies the minimum period of time (in seconds) before a DHCP packet received on this VLAN, is forwarded to the destination

Variable	Value
	device. Values range from 0 to 65535 seconds.
Mode	Specifies the type of DHCP packets this VLAN supports. Values include: • none—all received DHCP and BOOTP packets are dropped • bootp—only BOOTP packets are supported • dhcp—only DHCP packets are supported • both—DHCP and BOOTP packets are supported
AlwaysBroadcast	When selected, broadcasts DHCP reply packets from the VLAN to the DHCP client.
Option82Enabled	When selected, enables DHCP option 82 for the VLAN.
ClearCounters	Clears the DHCP counters. • clear—resets the DHCP counters to 0 and sets the counter clear time to the current system up time value. • dummy—the read-only default value.
CounterClearTime	Indicates the time the DHCP counters for this VLAN were last reset to 0.

Configuring RIP for a VLAN using EDM

Use this procedure to configure Routing Information Protocol (RIP) for a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN to edit, click the VLAN ID.
5. On the toolbar, click **IP**.

6. In the work area, click the **RIP** tab.
7. In the **Poison** section, click a radio button.
8. Select the **DefaultSupply** check box to enable ABC for the VLAN.

   OR

   Clear the **DefaultSupply** check box to disable ABC for the VLAN .
9. Select the **DefaultListen** check box to enable ABC for the VLAN.

   OR

   Clear the **DefaultListen** check box to disable ABC for the VLAN .
10. Select the **AutoAggregateEnable** check box to enable ABC for the VLAN.

    OR

    Clear the **AutoAggregateEnable** check box to disable ABC for the VLAN .
11. Select the **AdvertiseWhenDown** check box to enable ABC for the VLAN.

    OR

    Clear the **AdvertiseWhenDown** check box to disable ABC for the VLAN .
12. In the Cost dialog box, type a value.
13. Click **Apply** .

Variable definitions

Variable	Value
Poison	Enables or disables the operation of poison reverse on this VLAN. The default is disabled.
DefaultSupply	Enables or disables the advertising of default routes on this VLAN.
DefaultListen	Enables or disables listening for default rout advertisements on this VLAN.
AutoAggregateEnable	Enables or disables automatic aggregation on this VLAN.
AdvertiseWhenDown	Enables or disables the sending of advertisements from this VLAN when the VLAN is down.
Cost	Specifies the RIP cost for this VLAN. Values range from 1 to 15.

Graphing OSPF statistics for a VLAN using EDM

Use this procedure to display a graphical representation of OSPF statistics for a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN, click the VLAN ID.
5. On the toolbar, click **IP**.
6. In the work area, click the **OSPF Stats** tab.
7. Select a **Poll Interval** from the list on the toolbar.
8. To select statistics to graph, click a statistic type row under one of the displayed columns.
9. Click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

VLAN IPv6 interface management using EDM

Use the information in this section to configure and manage IPv6 interfaces for a VLAN.

Viewing IPv6 interface information for a VLAN using EDM

Use this procedure to display existing IPv6 interface information for a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. Click on the management VLAN ID.

5. On the toolbar, click **IPv6**.
6. In the work area, click the **IPv6 Interface** tab.

Variable definitions

Variable	Value
IfIndex	Identifies a physical interface or a logical interface (VLAN). For a VLAN, it is the Ifindex of the VLAN.
Identifier	Indicates the IPv6 address interface identifier, which is a binary string of up to 8 octets in network byte order.
IdentifierLength	Indicates the length of the interface identifier in bits.
Descr	Indicates a text string containing information about the interface. The network management system also sets this string.
VlanId	Identifies the Virtual LAN associated with the entry. This value corresponds to the lower 12 bits in the IEEE 802.1Q VLAN tag.
Type	Indicates Unicast, the only supported type.
ReasmMaxSize(MTU)	Indicates the MTU for this IPv6 interface. This value must be same for all the IP addresses defined on this interface. The default value is 1280.
PhysAddress	Indicates the media-dependent physical address. The range is 0 through 65535. For Ethernet, this is a MAC address.
AdminStatus	Indicates whether the administration status of the interface is enabled (true) or disabled (false). The default is enabled (true).
OperStatus	Indicates whether the operation status of the interface is up or down.
ReachableTime	Indicates the time (3600000 ms) that a neighbor is considered reachable after receiving a reachability confirmation.
RetransmitTime	Indicates the retransmit time, which is the time (3600000 ms) between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

Variable	Value
MulticastAdminStatus	Indicates the multicast status as either True or False.

Adding an IPv6 interface to a VLAN using EDM

Use this procedure to add an IPv6 interface to a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN, click the VLAN ID.
5. On the toolbar, click **IPv6**.
6. In the work area, click the **IPv6 Interface** tab.
7. On the toolbar, click **Insert** .
8. In the Identifier dialog box, type a value.
9. In the Descr dialog box, type a value.
10. In the ReasmMaxSize(MTU) dialog box, type a value.
11. Select the **AdminStatus** check box to enable the interface administration status for the VLAN.

    OR

    Clear the **AdminStatus** check box to disable the interface administration status for the VLAN .
12. In the ReachableTime dialog box, type a value.
13. In theRetransmitTime dialog box, type a value.
14. Click **Insert** .
15. Click **Apply** .

Variable definitions

Variable	Value
Identifier	Specifies the IPv6 address interface identifier, which is a binary string of up to 8 octets in network byte order.
Descr	Specifies a text string containing information about the interface. The network management system also sets this string.
ReasmMaxSize(MTU)	Specifies the MTU for this IPv6 interface. This value must be same for all the IP addresses defined on this interface. The default value is 1280.
AdminStatus	Specifies whether the administration status of the interface is enabled (true) or disabled (false). The default is enabled (true).
ReachableTime	Specifies the time (3600000 ms) that a neighbor is considered reachable after receiving a reachability confirmation.
RetransmitTime	Specifies the retransmit time, which is the time (3600000 ms) between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

Deleting an IPv6 interface from a VLAN using EDM

Use this procedure to remove an IPv6 interface from a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN, click the VLAN ID.
5. On the toolbar, click **IPv6**.
6. In the work area, click the **IPv6 Interface** tab.

7. To select an interface to delete, click the IfIndex.
8. On the toolbar, click **Delete** .

VLAN IPv6 address management using EDM

Use the information in this section to configure and manage IPv6 addresses for a VLAN.

Viewing IPv6 address information for a VLAN using EDM

Use this procedure to display existing IPv6 address information for a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. Click on the management VLAN ID.
5. On the toolbar, click **IPv6**.
6. In the work area, click the **IPv6 Addresses** tab.

Variable definitions

Variable	Value
IfIndex	Indicates of the VLAN.
Addr	Indicates the VLAN IPv6 address.
AddrLen	Indicates the VLAN IPv6 prefix length.
Type	Indicates the VLAN IPv6 address type. Values include: • unicast • anycast
Origin	Indicates the origin of the VLAN IPv6 address. Values include: • other • manual • dhcp

Variable	Value
	• linklayer • random
Status	Indicates the status of the VLAN IPv6 address. Values include: • preferred • deprecated • invalid • inaccessible • unknown • tentative • duplicate
Created	Indicates the value of the system up time when this address was created. A value of 0 indicates that this address was created before the last network management subsystem initialization.
LastChanged	Indicates the value of the system up time when this address was last updated. A value of 0 indicates that this address was updated before the last network management subsystem initialization.

Adding an IPv6 address to a VLAN using EDM

Use this procedure to add an IPv6 address to a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN, click the VLAN ID.
5. On the toolbar, click **IPv6**.
6. In the work area, click the **IPv6 Addresses** tab.
7. In the **Addr** box, type an IPv6 address.
8. In the **AddrLen** box, type the IPv6 prefix length.
9. In the **Type** section, click a radio button.

10. Click **Insert**.
11. Click **Apply** .

Variable definitions

Variable	Value
Addr	Specifies the VLAN IPv6 address.
AddrLen	Specifies the VLAN IPv6 prefix length.
Type	Specifies the VLAN IPv6 address type. Values include: • unicast • anycast

Deleting an IPv6 address from a VLAN using EDM

Use this procedure to remove an IPv6 address from a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN, click the VLAN ID.
5. On the toolbar, click **IPv6**.
6. In the work area, click the **IPv6 Addresses** tab.
7. To select an address to delete, click the **IfIndex**.
8. On the toolbar, click **Delete** .

VLAN configuration for ports using EDM

Use the information in this section to view and configure VLAN membership for specific ports.

Viewing VLAN membership port information using EDM

Use this procedure to display the VLAN membership information for switch ports.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **VLANs** .
3. Click the **Ports** tab.

Variable definitions

Variable	Value
Index	Indicates the switch position in the stack and the port number. This is a read-only value.
VlanIds	Indicates the VLAN IDs of which this port is a member. This is a read-only value.
DiscardUntaggedFrames	Indicates how untagged frames received on this port are processed. • true—untagged frames are discarded by the forwarding process • false—untagged frames are assigned to the VLAN specified by the VLAN ID. This column applies to trunk ports only.
FilteredUnregisteredFrame	Indicates how unregistered frames received on this port are processed. • true—unregistered frames are discarded by the forwarding process • false—unregistered frames are assigned to the VLAN specified by the VLAN ID. This column applies to access ports only.
DefaultVlanId	Indicates the VLAN ID assigned to untagged and unregistered frames received on a port.
PortPriority	Indicates the port priority for the switch to consider as it forwards received packets. Values range from 0 to 7.
Tagging	Indicates the type of VLAN port. Values include:

Variable	Value
	• untagAll (access) • tagAll (trunk) • untagPvidOnly • tagPvidOnly If the port is a trunk port, the port is often a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN.

Configuring VLAN membership ports using EDM

Use this procedure to configure VLAN membership for one or more switch ports.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **VLANs** .
3. Click the **Ports** tab.
4. To select a port to edit, click the port row.
5. In the port row, double-click the cell in the **DiscardUntaggedFrames** column.
6. Select a value from the list—**true** to discard untagged frames for the port, or **false** to accept untagged frames for the port.
7. In the port row, double-click the cell in the **FilteredUnregisteredFrame** column.
8. Select a value from the list—**true** to discard unregistered frames for the port, or **false** to process unregistered frames normally for the port.
9. In the port row, double-click the cell in the **DefaultVlanId** column.
10. Type a value for the default VLAN ID.
11. In the port row, double-click the cell in the **PortPriority** column.
12. Select a value from the list.
13. In the port row, double-click the cell in the **Tagging** column.
14. Select a value from the list.
15. You can repeat steps **5** through **14** to configure VLAN memberships for additional ports.
16. Click **Apply** .

Variable definitions

Variable	Value
Index	Indicates the switch position in the stack and the port number. This is a read-only value.
VlanIds	Indicates the VLAN IDs of which this port is a member. This is a read-only value.
DiscardUntaggedFrames	Specifies how untagged frames received on this port are processed. • true—untagged frames are discarded by the forwarding process • false—untagged frames are assigned to the VLAN specified by the VLAN ID. This column applies to trunk ports only.
FilteredUnregisteredFrame	Specifies how unregistered frames received on this port are processed. • true—unregistered frames are discarded by the forwarding process • false—unregistered frames are assigned to the VLAN specified by the VLAN ID. This column applies to access ports only.
DefaultVlanId	Specifies the VLAN ID assigned to untagged and unregistered frames received on a port.
PortPriority	Specifies the port priority for the switch to consider as it forwards received packets. Values range from 0 to 7.
Tagging	Specifies the type of VLAN port. Possible values are: • untagAll (access) • tagAll (trunk) • untagPvidOnly • tagPvidOnly If the port is a trunk port, the port is often a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN.

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 dialog box, type a value.
5. In the **VlanConfigControl** section, click a radio button.
6. On the toolbar, click **Apply**.

Variable Definitions

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: • 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. • 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 any previous VLAN memberships. Using this option, an untagged port can have membership in multiple VLANs. • 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.

Variable	Value
	Any new additions of an untagged port to a new VLAN does not change the PVID of that port. • 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.

Enabling AutoPVID using EDM

Use this procedure to automatically assign a port VLAN ID to any port by enabling the AutoPVID functionality on the switch.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Chassis**.
4. In the work area, click the **System** tab.
5. In the AutoPVID section, click the enabled radio button.
6. Click **Apply**.

Port configuration for VLANs using EDM

Use the information in this section to view and configure specific ports for VLAN membership.

Viewing port VLAN membership information using EDM

Use this procedure to display the VLAN membership information for switch ports.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis** .
3. In the Chassis tree, double-click **Ports** .
4. Click the **VLAN** tab.

Variable definitions

Variable	Value
VlanIds	Indicates the VLAN IDs of which this port is a member. This is a read-only value.
DiscardUntaggedFrames	Indicates how untagged frames received on this port are processed. • true—untagged frames are discarded by the forwarding process • false—untagged frames are assigned to the VLAN specified by the VLAN ID. This column applies to trunk ports only.
FilteredUnregisteredFrame	Indicates how unregistered frames received on this port are processed. • true—unregistered frames are discarded by the forwarding process • false—unregistered frames are assigned to the VLAN specified by the VLAN ID. This column applies to access ports only.
DefaultVlanId	Indicates the VLAN ID assigned to untagged and unregistered frames received on a port.
PortPriority	Indicates the port priority for the switch to consider as it forwards received packets. Values range from 0 to 7.
Tagging	Indicates the type of VLAN port. Possible values are: • untagAll (access) • tagAll (trunk) • untagPvidOnly • tagPvidOnly

Variable	Value
	If the port is a trunk port, the port is often a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN.

Configuring ports for VLAN membership using EDM

Use this procedure to configure one or more switch ports for VLAN membership.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs** .
3. Click on the **Ports** tab .
4. To select a port to edit, click the port row.
5. In the port row, double-click the cell in the **DiscardUntaggedFrames** column.
6. Select a value from the list—**true** to discard untagged frames for the port, or **false** to accept untagged frames for the port.
7. In the port row, double-click the cell in the **FilteredUnregisteredFrame** column.
8. Select a value from the list—**true** to discard unregistered frames for the port, or **false** to process unregistered frames normally for the port.
9. In the port row, double-click the cell in the **DefaultVlanId** column.
10. Type a value for the default VLAN ID.
11. In the port row, double-click the cell in the **PortPriority** column.
12. Select a value from the list.
13. In the port row, double-click the cell in the **Tagging** column.
14. Select a value from the list.
15. You can repeat steps **4** through **14** to configure VLAN memberships for additional ports.
16. Click **Apply** .

Variable definitions

Variable	Value
VlanIds	Indicates the VLAN IDs of which this port is a member. This is a read-only value.
DiscardUntaggedFrames	Specifies how untagged frames received on this port are processed. • true—untagged frames are discarded by the forwarding process • false—untagged frames are assigned to the VLAN specified by the VLAN ID. This column applies to trunk ports only.
FilteredUnregisteredFrame	Specifies how unregistered frames received on this port are processed. • true—unregistered frames are discarded by the forwarding process • false—unregistered frames are assigned to the VLAN specified by the VLAN ID. This column applies to access ports only.
DefaultVlanId	Specifies the VLAN ID assigned to untagged and unregistered frames received on a port.
PortPriority	Specifies the port priority for the switch to consider as it forwards received packets. Values range from 0 to 7.
Tagging	Specifies the type of VLAN port. Possible values are: • untagAll (access) • tagAll (trunk) • untagPvidOnly • tagPvidOnly If the port is a trunk port, the port is often a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN.

Adding static addresses to the MAC address table using EDM

Use the following procedure to add static addresses to the MAC address table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Bridge**.
3. In the work area, click the **Static FDB** tab.
4. To add a static MAC address, on the toolbar, click **Insert**.
5. Click the **Id** ellipsis (…)
6. Select a VLAN Id.
7. Click **Ok**.
8. In the **Address** dialog box, type a MAC address.
9. In the Interface dialog box, select **Port** or **Mlt**.
10. Select listed ports or trunks and click **Ok**
11. Click **Insert**.

Variable definitions

Variable	Value
Id	Indicates the VLAN ID for the VLAN
Address	Indicates the MAC address to be added, range from 0:0:0:0:0 to FE:FF:FF:FF:FF:FF. Address can only be a unicast address.
Interface	Specifies the interface (port or mlt) to add the MAC address.

Removing a static address from the MAC address table using EDM

Use the following procedure to remove a static address from the MAC address table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Bridge**.
3. In the work area, click the **Static FDB** tab.
4. To select an address to remove, click the address.
5. Click **Delete**.
6. Click **Yes** to confirm.

MAC address table management using EDM

Use the information in this section to manage the MAC address table by clearing entries.

Important:

In certain situations, due to the hash algorithm used by switch to store MAC addresses into memory, some MAC addresses cannot be learned.

Flushing the MAC address table using EDM

Use the following procedure to clear MAC addresses from the MAC address table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. In the work area, click the **MAC Flush** tab.
4. In the **FlushMacAddrTableAll** section, select a radio button.

   Select **flush** to remove all MAC entries

   OR

   Select **dynamic** to remove all dynamic MAC entries

   OR

   Select **static** to remove all static MAC entries
5. On the toolbar, click **Apply**.

Flushing Ethernet interface-based MAC addresses from the MAC address table using EDM

Use the following procedure to clear Ethernet interface-based MAC addresses from the MAC address table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. On the work area, click the **MAC Flush** tab.
4. In the **FlushMacAddrTableAll** section, select a radio button.

   Select **flush** to remove all MAC entries

   OR

   Select **dynamic** to remove all dynamic MAC entries

   OR

   Select **static** to remove all static MAC entries
5. Click the **FlushMacAddrTableByPortList** ellipsis **(...)**.
6. Select one or more specific ports.

   OR

   Click **ALL** to select all the ports.
7. Click **Ok**.
8. On the toolbar, click **Apply**.

Flushing VLAN-based MAC addresses from the MAC address table using EDM

Use the following procedure to clear VLAN-based MAC addresses from the MAC address table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. On the work area, click the **MAC Flush** tab.
4. In the **FlushMacAddrTableAll** section, select a radio button.

   Select **flush** to remove all MAC entries

   OR

   Select **dynamic** to remove all dynamic MAC entries

   OR

   Select **static** to remove all static MAC entries
5. In the **FlushMacAddrTableByVlan** dialog box, type a VLAN ID ranging from 1 to 4094.
6. On the toolbar, click **Apply**.

Flushing trunk-based MAC addresses from the MAC address table using EDM

Use the following procedure to clear trunk-based MAC addresses from the MAC address table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. On the work area, click the **MAC Flush** tab.
4. In the **FlushMacAddrTableAll** section, select a radio button.

   Select **flush** to remove all MAC entries

   OR

   Select **dynamic** to remove all dynamic MAC entries

   OR

   Select **static** to remove all static MAC entries

5. In the **FlushMacAddrTableByTrunk**dialog box, type a trunk value ranging from 1 to 32.
6. On the toolbar, click **Apply**.

Flushing a specific MAC address from the MAC address table using EDM

Use the following procedure to remove a single specific MAC address from the MAC address table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. On the work area, click the **MAC Flush** tab.
4. In the FlushMacAddrTableByAddress dialog box, type a MAC address.
5. On the toolbar, click **Apply**.

Configuring MAC address learning using EDM

Use the following procedure to configure the MAC address learning and to configure the aging time.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. On the work area, click the **Transparent** tab.
4. In the **AgingTime** dialog box, type a value.
5. To select a port to enable learning, click the **MacAddrTableLearningPorts** ellipsis (...).
6. To enable MAC learning, select one or more port numbers.

   OR

   To disable MAC learning, deselect one or more port numbers.

> **Note:**
>
> If you disable or enable a port that is part of an active MLT trunk or has the same LACP key, you also disable or enable the other ports in the trunk so that all ports in the trunk share the same behavior.

7. Click **Ok**.
8. On the tool bar, click **Apply**.

Variable definitions

Variable	Value
LearnedEntryDiscards	Indicates the number of Forwarding Database entries learned that are discarded due to insufficient space in the Forwarding Database. If this counter increases, it indicates that the Forwarding Database is becoming full regularly. This condition affects the performance of the subnetwork. If the counter has a significant value and is not presently increasing, it indicates that the problem has occurred but is not persistent.
AgingTime	Indicates the time-out period in seconds for removing old dynamically learned forwarding information. **Important:** The 802.1D-1990 specification recommends a default of 300 seconds.
MacAddrTableLearningPorts	Specifies the ports which are enabled for MAC learning.

Chapter 14: MultiLink Trunk configuration using Enterprise Device Manager

This chapter provides information you can use to create and manage Multi Link Trunks using Enterprise Device Manager (EDM).

MLT configuration using EDM

Use the information in this section to create a MultiLink Trunk (MLT) and to modify existing MLT port memberships.

Viewing MLT configurations using EDM

Use this procedure to display MLT configuration information.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **Multi Link Trunks** tab.

Variable Definitions

Variable	Value
Id	Indicates the number of the MLT (assigned consecutively). Displays the vlan based on port selected.
PortType	Indicates the port type. Values include:

Variable	Value
	• access • trunk
Name	Indicates a unique alphanumeric identifier for the MLT.
PortMembers	Indicates the switch or stack ports to assign to the MLT.
VlanIds	Indicates the VLAN identifier. Displays the vlan based on port selected.
Loadbalance (Mode)	Indicates the mode of load balancing. Options are basic and advanced.
Enable	Indicates whether the MLT is enabled (true) or disabled (false) . **Important:** You cannot enable an MLT if trunk port members are enabled for LACP.

Creating an MLT using EDM

Create an MLT to form a link from the switch to another switch or server.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **Multi Link Trunks** tab.
4. To select a trunk to create, click the trunk **Id**.
5. In the trunk row, double-click the cell in the **Name** column.
6. In the box, type a name for the MLT.

   OR

   Accept the default MLT name.
7. In the trunk row, double-click the cell in the **PortMembers** column.
8. From the list , select ports to add to the trunk.
9. Click **Ok**.

10. In the trunk row, double-click the cell in the **Loadbalance(Mode)** column.
11. From the list, select a load balancing mode.
12. In the trunk row, double-click the cell in the **Enable** column.
13. From the list, select a value—**true** to enable the MLT, or **false** to disable the MLT.
14. You can repeat steps **4** through **13** to create additional MLTs.
15. Click **Apply**.

Variable Definitions

Variable	Value
Id	Specifies the number of the MLT (assigned consecutively). Displays the vlan based on port selected.
PortType	Specifies the port type. Values include: • access • trunk
Name	Specifies a unique alphanumeric identifier for the MLT.
PortMembers	Specifies the switch or stack ports to assign to the MLT.
VlanIds	Specifies the VLAN identifier. Displays the vlan based on port selected.
Loadbalance (Mode)	Specifies the mode of load balancing. Options are basic and advanced.
Enable	Enables (true) or disables (false) the MLT. ❗ **Important:** You cannot enable an MLT if trunk port members are enabled for LACP.

Modifying MLT port memberships using EDM

Modify MLT port memberships to change configuration parameters for an existing MLT.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **Multi Link Trunks** tab.
4. To select a trunk to modify, click the trunk **Id** of an existing trunk.
5. In the trunk row, double-click the cell in the **Enable** column.
6. From the list box, select **false** to disable the MLT.
7. Click **Apply**.
8. In the trunk row, double-click the cell in the **Name** column.
9. In the box, edit the MLT name as required.
10. In the trunk row, double-click the cell in the **PortMembers** column.
11. From the list box, select ports to add to or remove from the trunk.
12. Click **Ok**.
13. In the trunk row, double-click the cell in the **Loadbalance(Mode)** column.
14. From the list box, select a load balancing mode.
15. You can repeat steps **4** through **14** to modify additional MLTs.
16. Click **Apply**.

Variable Definitions

Variable	Value
Id	Specifies the number of the MLT (assigned consecutively). Displays the vlan based on port selected.
PortType	Indicates the port type. Values include: • access • trunk
Name	Specifies a unique alphanumeric identifier for the MLT.
PortMembers	Specifies the switch or stack ports to assign to the MLT.

Variable	Value
VlanIds	Specifies the VLAN identifier. Displays the vlan based on port selected.
Loadbalance (Mode)	Specifies the mode of load balancing. Options are basic and advanced.
Enable	Enables (true) or disables (false) the MLT. **Important:** You cannot enable an MLT if trunk port members are enabled for LACP.

Viewing MLT utilization using EDM

Use this procedure to display MLT utilization information.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, click **MLT/LACP**.
3. In the work area, click the **MLT Utilization** tab.

Variable definition

Variable	Value
Id	Displays the MLT ID.
PortIfIndex	Displays the port number.
TrafficType	Displays the traffic type.
TrafficLast5Min	Displays MLT utilization for the last 5 minutes.
TrafficLast30Min	Displays MLT utilization for the last 30 minutes.
TrafficLast1Hour	Displays MLT utilization for the last hour.

Graphing MLT statistics using EDM

Use the following procedure to display and graph MLT interface statistics.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **Multi Link Trunks** tab.
4. Select an MLT row.
5. Click **Graph**.
6. Click the **Interface** tab.
7. Click the **Poll Interval** box.
8. From the list, select a poll interval time.
9. Click **Clear Counters**.
10. To select statistics to graph, click a row under one of the available column headings.
11. Click a **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.
12. To return to the MultiLink Trunks-Graph, Interface work area, click **Close**.

Variable definitions

Variable	Value
Poll Interval	Specifies the time interval in seconds, minutes, or hours that the switch polls the interface for MLT statistics. Located on menu bar.
InMulticastPkts	Indicates the number of packets delivered to this MLT that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.
OutMulticastPkts	Indicates the total number of packets that higher-level protocols requested be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
InBroadcastPkts	Indicates the number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
OutBroadcastPkts	Indicates the total number of packets that higher-level protocols requested be transmitted, and that were addressed to a

Variable	Value
	broadcast address at this MLT, including those that were discarded or not sent.
HCInOctets	Indicates the total number of octets received on the MLT interface, including framing characters.
HCOutOctets	Indicates the total number of octets transmitted out of the MLT interface, including framing characters.
HCInUcastPkts	Indicates the number of packets delivered by this MLT to a higher MLT that were not addressed to a multicast or broadcast address at this sublayer.
HCOutUcastPkts	Indicates the number of packets that high-level protocols requested be transmitted that were not addressed to a multicast address at this MLT. This total number includes those packets discarded or unsent.
HCInMulticastPkt	Indicates the number of packets delivered to this MLT that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.
HCOutMulticast	Indicates the total number of packets that high-level protocols requested be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
HCInBroadcastPkt	Indicates the number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
HCOutBroadcast	Indicates the total number of packets that high-level protocols requested be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.

Graphing MLT Ethernet error statistics using EDM

Use the following procedure to view and graph MLT Ethernet error statistics.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.

3. In the work area, click the **MultiLink Trunks** tab.
4. Select an MLT row.
5. Click **Graph**.
6. Click the **Ethernet Errors** tab.
7. Click the **Poll Interval** box.
8. From the list, select a poll interval time.
9. Click **Clear Counters**.
10. To select error statistics to graph, click a row under one of the available column headings.
11. Click a **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.
12. To return to the MultiLink Trunks-Graph, Ethernet Errors work area, click **Close**.

Variable definitions

Variable	Value
Poll Interval	Specifies the time interval in seconds, minutes, or hours that the switch polls the interface for MLT Ethernet error statistics. Located on menu bar.
AlignmentErrors	Indicates a count of frames received on a particular MLT that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
FCSErrors	Indicates a count of frames received on an MLT that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
IMacTransmit Error	Indicates a count of frames for which transmission on a particular MLT fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object.

Variable	Value
IMacReceive Error	Indicates a count of frames for which reception on a particular MLT fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object. The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted.
CarrierSense Error	Indicates the number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular MLT. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
FrameTooLong	Indicates a count of frames received on a particular MLT that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
SQETestError	Indicates a count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular MLT. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
Deferred Transmiss	Indicates a count of frames for which the first transmission attempt on a particular MLT is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollFrames	Indicates a count of successfully transmitted frames on a particular MLT for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object.
MultipleColl Frames	Indicates a count of successfully transmitted frames on a particular MLT for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	Indicates the number of times that a collision is detected on a particular MLT later than 512 bit-times into the transmission of a

Variable	Value
	packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
ExcessiveCollis	Indicates a count of frames for which transmission on a particular MLT fails due to excessive collisions.

Selecting an SLPP Guard Ethernet type using EDM

Use this procedure to select an SLPP Guard Ethernet type for the switch.

❗ **Important:**

You must configure Ethertype to match the SLPP Ethernet type on the adjacent core or distribution switches that have SLPP enabled.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **SLPP**.
3. In the work area, click the **Global** tab.
4. Type a value in the **SlppGuardEtherType** box.
5. On the toolbar, click **Apply**.

Configuring SLPP Guard using EDM

Use this procedure to configure SLPP Guard for switch ports.

✳ **Note:**

SLPP packets are generated only on switches that are configured with SLPP - for example ERS 5000 Series or ERS 8300. The ERS 4000 switches do not support SLPP. When you enable SLPP Guard on an ERS 4000, the switch must be connected to another Avaya switch that supports SLPP and SLPP must be enabled on that switch.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **SLPP**.
3. In the work area, click the **SLPP Guard** tab.
4. To select a specific switch port, click an **IfIndex**.
5. In the IfIndex row, double-click the cell in the **Enabled** column.
6. Select a value from the list—**true** to enable SLPP Guard, **false** to disable SLPP Guard.
7. In the IfIndex row, double-click the cell in the **Timeout** column.
8. Type a value in the **Timeout** box.
9. On the toolbar, click **Apply**.

Variable definition

Variable	Value
IfIndex	Specifies the port on which to configure SLPP Guard.
Enable	Enables (true) or disables (false) SLPP Guard for the port.
Timeout	Specifies the time period, in seconds, for which SLPP Guard disables the port. After the timeout period expires, the switch re-enables the port. The timeout value can be 0 or a value ranging from 10 to 65535. With a value of 0, the port remains disabled until it is manually re-enabled. The default Timeout value is 60 seconds.
Status	Displays the SLPP Guard status for the port.
TimerCount	Indicates the time, in seconds, that elapses after SLPP Guard disables a port. When the TimerCount value equals the Timeout value, the switch re-enables the port.

Viewing the SLPP Guard configuration using EDM

Use this procedure to display SLPP Guard configuration information for switch ports.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **SLPP**.
3. In the work area, click the **SLPP Guard** tab.

Variable definition

Variable	Value
IfIndex	Indicates the port for which the SLPP Guard information is displayed.
Enable	Enables (true) or disables (false) SLPP Guard for the port.
Timeout	Specifies the time period, in seconds, for which SLPP Guard disables the port. After the timeout period expires, the switch re-enables the port. The timeout value can be 0 or a value ranging from 10 to 65535. With a value of 0, the port remains disabled until it is manually re-enabled. The default Timeout value is 60 seconds.
Status	Displays the SLPP Guard status for the port.
TimerCount	Indicates the time, in seconds, that elapses after SLPP Guard disables a port. When the TimerCount value equals the Timeout value, the switch re-enables the port.

Chapter 15: Spanning Tree Protocol Configuration using Enterprise Device Manager

This chapter describes how you can configure the Spanning Tree Protocol (STP) and Spanning Tree Groups (STGs) using Enterprise Device Manager (EDM).

Configuring the STP mode using EDM

Use the following procedure to configure the STP operational mode.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **Globals**.
4. Choose the STP mode in the **SpanningTreeAdminMode** field.
5. On the toolbar, 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**.

For information about resetting the switch, see the following section.

Resetting the switch using EDM

Use the following procedure to reset the switch.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Chassis**.
4. On the work area, click the **System** tab.
5. In the ReBoot section, click the **reboot** radio button.
6. Click **Apply**.

Configuring STP BPDU filtering for specific ports using EDM

Use this procedure to configure STP BPDU filtering for one or more ports.

You can configure STP BPDU filtering in either STG, RSTP, or MSTP operational mode.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. On the work area, click the **STP BPDU-Filtering** tab.
5. To select a port to edit, click the port index.
6. In the port row, double-click the cell in the **AdminEnabled** column.
7. 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.
8. In the port row, double-click the cell in the **Timeout** column.
9. Type a value in the dialog box.
10. You can repeat steps **5** through **9** to configure STP BPDU filtering for additional ports.
11. On the toolbar, click **Apply**.

Variable Definitions

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 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.

Configuring STG globally using EDM

Use the following procedure to configure the STG for the switch.

Prerequisites

- Select avayaStpg for the Spanning Tree administration mode.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. In the work area, click the **Globals** tab.
5. In the **SpanningTreePathCostCalculationMode** section, click a radio button.
6. In the **SpanningTreePortMode** section, select a radio button.
7. In the SpanningTreeAdminCompatibility section, select the **port802dot1dLearning** check box to enable 8021d compliancy support.

   OR

In the SpanningTreeAdminCompatibility section, clear the **port802dot1dLearning** check box to disable 8021d compliancy support.

8. Click **Apply**.

Variable Definitions

Variable	Value
SpanningTreePathCostCalculationMode	Specifies the spanning-tree path cost calculation mode. Values include: • ieee802dot1dCompatible • ieee802dot1tCompatible You can select ieee802dot1dCompatible only when the global STP mode avayaStpg is selected.
SpanningTreePortMode	Specifies the STG port membership mode for all Spanning Tree Groups on the switch. Values are: • normal • auto
SpanningTreeAdminCompatibility	Specifies the administrative feature compatibility mode. • port802dot1dLearning—enables or disables STP 802.1D compliancy support for the switch
SpanningTreeOperCompatibility	Indicates the operational feature compatibility mode. For some features, this read-only display will not change until the system is reset.

Configuring STP BPDU filtering ignore self using EDM

Use this procedure to configure whether or not local bridge BPDUs are ignored during the STP BPDU filtering process.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. In the work area, click the **Globals** tab.

5. Select the **SpanningTreeBpduFilterIgnoreSelf** check box to enable STP BPDU filtering ignore self.

   OR

   Clear the **SpanningTreeBpduFilterIgnoreSelf** check box to disable STP BPDU filtering ignore self.

6. Click **Apply**.

STG configuration using EDM

Use the information in this section to create and manage STGs on your network.

STG configuration prerequisites

- Select avayaStpg for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see Configuring the STP mode using EDM on page 239.

Viewing an STG using EDM

Use the following procedure to display STG configuration information.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. On the work area, click the **Configuration** tab.

Variable Definitions

Use the data in the following table to help you understand the STG display.

Variable	Value
Id	Indicates the identifier for the STG. Values range from 1 to 8. The default STG ID is 1.

Variable	Value
BridgeAddress	Indicates the MAC address used by a bridge when the bridge must be referred to in a unique fashion. The bridge MAC address can be integrated with the priority value to form a unique bridge identifier that is used in the Spanning Tree Protocol.
NumPorts	Indicates the number of ports controlled by this bridging entity.
Protocol Specification	Indicates the version of the spanning tree protocol being run. Values include: • decLb100: Indicates the DEC LANbridge 100 Spanning Tree Protocol. • ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version, a new value will be defined.
Priority	Indicates the first two octets of the 8-octet bridge ID. Values range from 0 to 65535.
BridgeMaxAge	Indicates the maximum time you want to allow before the specified STG times out, in seconds; the range, measured in hundredths of a second, is 600 (6 seconds) to 4000 (40 seconds).
BridgeHelloTime	Indicates the maximum time between hellos, in seconds; the range, measured in hundredths of a second, is 100 (1 second) to 1000 (10 seconds).
BridgeForwardDelay	Indicates the maximum delay in forwarding, in seconds; the range, measured in hundredths of a second) is 400 (4 seconds) to 3000 (30 seconds).
EnableStp	Indicates whether STP is enabled (true) or disablesd (false) for the STG.
TaggedBpduAddress	Indicates the destination MAC address assigned to tagged BPDUs.
TaggedBpduVlanId	Indicates the VLAN ID for tagged BPDUs. This value must be unique for each specific STG.

Modifying an STG using EDM

Use the following procedure to edit an existing STG configuration.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. On the work area, click the **Configuration** tab.
5. To select an STG to edit, click the STG ID.
6. In the STG row, double-click the cell in the **Priority** column.
7. Type a value in the dialog box.
8. In the STG row, double-click the cell in the **BridgeMaxAge** column.
9. Type a value in the dialog box.
10. In the STG row, double-click the cell in the **BridgeHelloTime** column.
11. Type a value in the dialog box.
12. In the STG row, double-click the cell in the **EnableStp** column.
13. Select a value from the list—**true** to enable STP for the STG, or **false** to disable STP for the STG.
14. In the STG row, double-click the cell in the **TaggedBpduAddress** column.
15. Type a value in the dialog box.
16. In the STG row, double-click the cell in the **TaggedBpduVlanId** column.
17. Type a value in the dialog box.
18. You can repeat steps **6** through **17** to create additional STGs.
19. Click **Apply**.

Variable Definitions

Use the data in the following table to edit an existing STG.

Variable	Value
Id	Indicates the identifier for the STG. Values range from 1 to 8. The default STG ID is 1. This is a read-only cell.
BridgeAddress	Indicates the MAC address used by a bridge when the bridge must be referred to in a unique fashion. The bridge MAC address can be integrated with the priority

Variable	Value
	value to form a unique bridge identifier that is used in the Spanning Tree Protocol. This is a read-only cell.
NumPorts	Indicates the number of ports controlled by this bridging entity. This is a read-only cell.
Protocol Specification	Version of the spanning tree protocol being run. Values include: • decLb100: Indicates the DEC LANbridge 100 Spanning Tree Protocol. • ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version, a new value will be defined. This is a read-only cell.
Priority	Specifies the first two octets of the 8-octet bridge ID. Values range from 0 to 65535.
BridgeMaxAge	Specifies the maximum time you want to allow before the specified STG times out, in seconds; the range, measured in hundredths of a second, is 600 (6 seconds) to 4000 (40 seconds).
BridgeHelloTime	Specifies the maximum time between hellos, in seconds; the range, measured in hundredths of a second, is 100 (1 second) to 1000 (10 seconds).
BridgeForwardDelay	Specifies the maximum delay in forwarding, in seconds; the range, measured in hundredths of a second) is 400 (4 seconds) to 3000 (30 seconds).
EnableStp	Enables (true) or disables (false) STP for the STG.
TaggedBpduAddress	Specifies the destination MAC address assigned to tagged BPDUs.
TaggedBpduVlanId	Specifies the VLAN ID for tagged BPDUs. This value must be unique for each specific STG.

Creating an STG using EDM

Use the following procedure to create an STG.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. On the work area, click the **Configuration** tab.
5. On the toolbar, click **Insert**.
6. Edit the default information in the dialog boxes to create an STG.
7. Click **Insert**.
8. You can repeat steps **5** through **7** to create additional STGs.
9. Click **Apply**.

Variable Definitions

Use the data in the following table to create an STG.

Variable	Value
Id	Identifies the STG. Vlaue range is 1–8; 1 is the default STG.
Priority	Specifies the first two octets of the 8-octet bridge ID; the range is 0−65535.
BridgeMaxAge	Specifies the maximum time you want to allow before the specified STG times out, in seconds; the range, measured in hundredths of a second, is 600 (6 seconds) to 4000 (40 seconds).
BridgeHelloTime	Specifies the maximum time between hellos, in seconds; the range, measured in hundredths of a second, is 100 (1 second) to 1000 (10 seconds).
BridgeForwardDelay	Specifies the maximum delay in forwarding, in seconds; the range, measured in hundredths of a second) is 400 (4 seconds) to 3000 (30 seconds).
TaggedBpduVlanId	Specifies the VLAN ID for tagged BPDUs.

Deleting an STG using EDM

Use this procedure to delete an STG.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. On the work area, click the **Configuration** tab.
5. To select an STG to edit, click the STG ID.
6. Click **Delete**.

Moving a VLAN between STGs using EDM

You cannot use EDM to move VLANs between STGs on the Avaya Ethernet Routing Switch 4000 Series. Instead, delete the VLAN to be moved and add a replacement VLAN in the STG to which you want to move the VLAN.

Viewing STG Status using EDM

Use this procedure to display the status of configured STGs.

Prerequisites

- Select avayaStpg for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see Configuring the STP mode using EDM on page 239.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. On the work area, click the **Status** tab.

Variable Definitions

Use the data in the following table to help you understand the STG status display.

Variable	Value
Id	Indicates the STG ID.
BridgeAddress	Indicates the MAC address used by this bridge.
NumPorts	Indicates the number of ports controlled by this bridging entity.
ProtocolSpecification	Indicates the version of spanning tree that is running.
TimeSinceTopology Change	Indicates the time, in hundredths of seconds, since the last topology change.
TopChanges	Indicates the number of topology changes since the switch was reset.
DesignatedRoot	Indicates the MAC address of the STP designated root.
RootCost	Indicates the cost of the path to the root.
RootPort	Indicates the port number of the port with the lowest-cost path from this bridge to the root bridge.
MaxAge	Indicates the maximum age, in hundredths of a second, of STP information learned from any port in the network before the information is discarded.
HelloTime	Indicates the amount of time, in hundredths of seconds, between Hello messages.
HoldTime	Indicates the interval, in hundredths of seconds, during which no more than two Hello messages can be transmitted.
ForwardDelay	Indicates 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.

STG port membership management using EDM

Use the information in this section to view and modify STG membership configurations for switch ports.

STG port membership management prerequisites

- Select avayaStpg for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see Configuring the STP mode using EDM on page 239.

Viewing STG port information using EDM

Use this procedure to display STG port membership status.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. On the work area, click the **Ports** tab.

Variable Definitions

Variable	Value
Port	Indicates the unit and port number.
StgId	Indicates the STG ID number.
Priority	Indicates the port priority
State	Indicates the STP state of the port—Disabled, Blocking, Listening, Learning, and Forwarding.
EnableStp	Indicates whether STP is enabled (true) or disabled (false) on the port.
FastStart	Indicates whether Fast Start STP is enabled (true) or disabled (false) on the port.
AdminPathCost	Indicates the PathCost value. The field displays 0 if no user-configured value exists.
PathCost	Indicates the contribution of this port to the cost path of the spanning tree root.

Variable	Value
DesignatedRoot	Indicates the MAC address of the STP designated root.
DesignatedCost	Indicates the path cost of the designated port of the segment connected to this port.
DesignatedBridge	Indicates the MAC address of the designated bridge this port considers the designated bridge for this segment.
DesignatedPort	Indicates the port ID of the designated bridge for this port segment.
ForwardTransitions	Specifies the number of times the port transitioned from STP Learning to Forwarding state.

Configuring STG for port using EDM

Use this procedure to configure STG membership for switch ports.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. On the work area, click the **Ports** tab.
5. To select an STG port to edit, click the port row.
6. In the port row, double-click the cell in the **Priority** column.
7. Type a value in the dialog box.
8. In the port row, double-click the cell in the **EnableStp** column.
9. Select a value from the list—**true** to enable STP for the port, or **false** to disable STP for the port.
10. In the port row, double-click the cell in the **FastStart** column.
11. Select a value from the list—**true** to enable fast start for the port, or **false** to disable fast start for the port.
12. In the port row, double-click the cell in the **AdminPathCost** column.
13. Type a value in the dialog box.
14. In the port row, double-click the cell in the **PathCost** column.

15. Type a value in the dialog box.
16. You can repeat steps **5** through **15** to configure STG for additional ports.
17. Click **Apply**.

Variable Definitions

Use the data in the following table to edit STG port configurations.

Variable	Value
Port	Specifies the unit and port number.
StgId	Specifies the STG ID number.
Priority	Specifies the port priority
State	Specifies the STP state of the port—Disabled, Blocking, Listening, Learning, and 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	Specifies the contribution of this port to the cost path of the spanning tree root.
DesignatedRoot	Specifies the MAC address of the STP designated root.
DesignatedCost	Specifies the path cost of the designated port of the segment connected to this port.
DesignatedBridge	Specifies the MAC address of the designated bridge this port considers the designated bridge for this segment.
DesignatedPort	Specifies the port ID of the designated bridge for this port segment.
ForwardTransitions	Specifies the number of times the port transitioned from STP Learning to Forwarding state.

Port STG membership configuration using EDM

Use the information in this section to view and modify switch port STG memberships.

Prerequisites

- Ensure that STP is enabled before enabling FastStart.

Viewing STG port membership information using EDM

Use this procedure to display information about switch port STG memberships.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. In the work area, click the **STG** tab.

Variable Definitions

Use the data in the following table to help you understand the switch port STG display.

Variable	Value
Port	Indicates the unit and port number.
StgId	Indicates the STG ID number.
Priority	Indicates the port priority
State	Indicates the STP state of the port—Disabled, Blocking, Listening, Learning, and Forwarding.
EnableStp	Indicates whether STP is enabled (true) or disabled (false) on the port.
FastStart	Indicates whether fast start STP is enabled (true) or disabled (false) on the port.
AdminPathCost	Indicates the PathCost value. The field displays 0 if no user-configured value exists.
PathCost	Indicates the contribution of this port to the cost path of the spanning tree root.
DesignatedRoot	Indicates the MAC address of the STP designated root.
DesignatedCost	Indicates the path cost of the designated port of the segment connected to this port.

Variable	Value
DesignatedBridge	Indicates the MAC address of the designated bridge this port considers the designated bridge for this segment.
DesignatedPort	Indicates the port ID of the designated bridge for this port segment.
ForwardTransitions	Indicates the number of times the port transitioned from STP Learning to Forwarding state.

Configuring STG port membership using EDM

Use this procedure to configure switch ports as STG members.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. In the work area, click the **STG** tab.
5. To select an port to edit, click the port row.
6. In the port row, double-click the cell in the **Priority** column.
7. Type a value in the dialog box.
8. In the port row, double-click the cell in the **EnableStp** column.
9. Select a value from the list—**true** to enable STP for the port, or **false** to disable STP for the port.
10. In the port row, double-click the cell in the **FastStart** column.
11. Select a value from the list—**true** to enable fast start for the port, or **false** to disable fast start for the port.
12. In the port row, double-click the cell in the **AdminPathCost** column.
13. Type a value in the dialog box.
14. In the port row, double-click the cell in the **PathCost** column.
15. Type a value in the dialog box.
16. You can repeat steps **5** through **15** to configure additional ports as STG members.
17. Click **Apply**.

Variable Definitions

Use the data in the following table to configure switch ports as STG members.

Variable	Value
Port	Specifies the unit and port number.
StgId	Specifies the STG ID number.
Priority	Specifies the port priority
State	Specifies the STP state of the port—Disabled, Blocking, Listening, Learning, and 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	Specifies the contribution of this port to the cost path of the spanning tree root.
DesignatedRoot	Specifies the MAC address of the STP designated root.
DesignatedCost	Specifies the path cost of the designated port of the segment connected to this port.
DesignatedBridge	Specifies the MAC address of the designated bridge this port considers the designated bridge for this segment.
DesignatedPort	Specifies the port ID of the designated bridge for this port segment.
ForwardTransitions	Specifies the number of times the port transitioned from STP Learning to Forwarding state.

Chapter 16: RSTP configuration using Enterprise Device Manager

This chapter describes how you can configure Rapid Spanning Tree protocol (RSTP) using Enterprise Device Manager (EDM).

RSTP (or IEEE 802.1w) provisions the following:

- It reduces the recovery time after a network breakdown
- It 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
- It reduces the amount of flooding in the network by enhancing the way the Topology Change Notification (TCN) packet is generated

Prerequisites

- Select RSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see Configuring the STP mode using EDM on page 239.

Viewing global RSTP information using EDM

Use this procedure to display global RSTP information .

Prerequisites

- Select RSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see Configuring the STP mode using EDM on page 239.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **RSTP**.
4. On the work area, click the **Globals** tab to display the RSTP information.

Variable Definitions

Variable	Value
PathCostDefault	Sets the version of the Spanning Tree default Path Costs that the Bridge uses. A value of 16-bit uses the 16-bit default Path Costs from IEEE Std. 802.1D-1998. A value of 32-bit uses the 32-bit default Path Costs from IEEE Std. 802.1t.
TXHoldCount	Specifies the value used by the Port Transmit state machine to limit the maximum transmission rate. The value can range from 1–10.
Version	Specifies the version of the Spanning Tree Protocol the bridge is currently running: • stpCompatible—indicates that the bridge uses the Spanning Tree Protocol specified in IEEE 802.1D. • rstp—indicates that the bridge uses the Rapid Spanning Tree Protocol specified in IEEE 802.1w.
Priority	Specifies 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	Specifies 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 600–4000.
BridgeHelloTime	Specifies 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 100–1000.
BridgeForward Delay	Specifies the value in 1/100 seconds that all bridges use for ForwardDelay when this bridge is acting as the root. The 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 400–3000.
DesignatedRoot	Specifies 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	Specifies the cost of the path to the root as seen from this bridge.
RootPort	Specifies the port number of the port that offers the lowest cost path from this bridge to the root bridge.

Variable	Value
MaxAge	Specifies 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	Specifies 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	Specifies 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	Specifies the number of times the RSTP Module is enabled. A trap is generated on the occurrence of this event.
RstpDownCount	Specifies the number of times the RSTP Module is disabled. A trap is generated on the occurrence of this event
NewRootIdCount	Specifies the number of times this Bridge has detected a Root Identifier change. A trap is generated on the occurrence of this event.
TimeSinceTopologyChange	Specifies 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	Specifies the total number of topology changes detected by this bridge since the management entity was last reset or initialized.

Viewing RSTP port information using EDM

Prerequisites

Use the following procedure to display RSTP port information.

- Select RSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see Configuring the STP mode using EDM on page 239.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **RSTP**.
4. On the work area, click the **RSTP Ports** tab.

Variable Definitions

Variable	Value
Port	Specifies the port number.
State	Specifies the port state in this RSTP instance. The port state is cataloged as discarding, learning, and forwarding.
Priority	Specifies the value of the priority field which is in the first (in network byte order) octet of the (2 octet long) Port ID.
PathCost	Specifies the contribution of this port to the cost of paths towards the spanning tree root.
ProtocolMigration	Specifies 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	Specifies 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	Specifies the operational value of the Edge Port parameter. The object is initialized to false on reception of a BPDU.
AdminPointToPoint	Specifies the administrative point-to-point status of the LAN segment attached to this port. • forceTrue—indicates that this port is always treated as being connected to a point-to-point link. • forceFalse—indicates that this port is treated as having a shared media connection. • auto—indicates that this port is considered to have a point-to-point link if it is an Aggregator and all of its

Variable	Value
	members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means.
OperPointToPoint	Specifies 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 autodetection.
Participating	Specifies this field specifies whether a port is participating in the 802.1w protocol.
DesignatedRoot	Specifies the bridge identifier of the old root of the Spanning Tree as determined by the Spanning Tree Protocol as executed by this node.
DesignatedCost	Specifies 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	Specifies the Bridge Identifier of the bridge which this port considers to be the Designated Bridge for this port segment.
DesignatedPort	Specifies the Port Identifier for the port segment which is on the Designated Bridge.
ForwardTransitions	Specifies the number of times this port has transitioned from the Learning state to the Forwarding state.

Viewing RSTP statistics using EDM

Use the following procedure to display the RSTP statistics.

Prerequisites

- Select RSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see Configuring the STP mode using EDM on page 239.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.

3. In the Spanning Tree tree, double-click **RSTP**.
4. On the work area, click the **RSTP Status** tab.

Variable Definitions

Variable	Value
Port	Specifies the port number.
Role	Represents a functionality characteristic or capability of a resource to which policies are applied.
OperVersion	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	Specifies the 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 using EDM

Use the following procedure to display and graph RSTP port statistics.

Prerequisites

- Select RSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see Configuring the STP mode using EDM on page 239.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **RSTP**.
4. On the work area, click the **RSTP Status** tab.

5. In the table, select a port for which you want to display the statistic graph.
6. On the toolbar, click **Graph** to get the statistics of the selected port.

Variable Definitions

Variable	Value
RxRstBpduCount	Specifies the number of RST BPDUs received on the port.
RxConfigBpduCount	Specifies the number of Config BPDUs received on the port.
RxTcnBpduCount	Specifies the number of TCN BPDUs received on the port.
TxRstBpduCount	Specifies the number of RST BPDUs transmitted by this port.
TxConfigBpduCount	Specifies the number of Config BPDUs transmitted by this port.
TxTcnBpduCount	Specifies the number of TCN BPDUs transmitted by this port.
InvalidRstBpduRxCount	Specifies the number of invalid RSTP BPDUs received on this port.
InvalidConfigBpduRxCount	Specifies the number of invalid Configuration BPDUs received on this port.
InvalidTcnBpduRxCount	Specifies the number of invalid TCN BPDUs received on this port.
ProtocolMigrationCount	Specifies the number of times this Port is migrated from one STP protocol version to another. The relevant protocols are STP-COMPATIBLE and RSTP.

Chapter 17: MSTP configuration using Enterprise Device Manager

This chapter describes how you can configure Multiple Spanning Tree Protocol (MSTP) using Enterprise Device Manager (EDM).

With 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 4000 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.

Prerequisites

- Select MSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see Configuring the STP mode using EDM on page 239.

Viewing global MSTP using EDM

Use this procedure to display global MSTP information.

Prerequisites

- Select MSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see Configuring the STP mode using EDM on page 239.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.

3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **Globals** tab.

Variable Definitions

Variable	Value
PathCostDefaultType	Specifies 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	Specifies the value used by the Port Transmit state machine to limit the maximum transmission rate. The range in 1–10
MaxHopCount	Specifies the Maximum Hop Count value in 1/100 seconds. The value must be a multiple of 100. The range is 100–4000.
NoOfInstancesSupported	Specifies the maximum number of spanning tree instances supported.
MSTPUpCount	Specifies the number of times the MSTP Module is enabled. A trap is generated on the occurrence of this event.
MSTPDownCount	Specifies 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. • stpCompatible—indicates that the bridge is using the Spanning Tree Protocol as specified in IEEE 802.1D. • rstp—indicates that the bridge is using the Rapid Spanning Tree Protocol as specified in IEEE 802.1w. • MSTP—indicates that the bridge is running the Multiple Spanning Tree Protocol as specified in IEEE 802.1s.
BrgAddress	Specifies the bridge address is generated when events like protocol up or protocol down occurs.
Root	Specifies the bridge identifier of the root of the common spanning tree as determined by the

Variable	Value
	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	Specifies 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.
RootCost	Specifies the cost of the path to the CIST Root as seen from this bridge.
RegionalRootCost	Specifies the cost of the path to the CIST Regional Root as seen from this bridge.
RootPort	Specifies the port number of the port which offers the lowest path cost from the bridge to the CIST Root Bridge
BridgePriority	Specifies 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	Specifies 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 600–4000.
BridgeForwardDelay	Specifies 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 400–3000.
HoldTime	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	Specifies 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	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

Variable	Value
	before moving to the next state. This value is measured in units of hundredths of a second.
TimeSinceTopology Change	Specifies 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	Specifies the number of times that at least one non-zero TcWhile Timer occurred on this Bridge for the Common Spanning Tree context.
NewRootBridgeCount	Specifies 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.
RegionName	Specifies the region name of the configuration. By default, the Region Name is equal to the Bridge Mac Address.
RegionVersion	Specifies the version of the MST Region.
ConfigIdSel	Specifies 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.
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	Specifies the number of times a Region Configuration Identifier Change is detected. A trap is generated when this event occurs.

Viewing CIST port information using EDM

Use this procedure to display CIST port information.

Prerequisites

- Select MSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see Configuring the STP mode using EDM on page 239.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **CIST Ports** tab.

Variable Definitions

Variable	Value
Port	Specifies the port number of the port containing Spanning Tree information.
PathCost	Specifies the contribution of this port to the cost of paths towards the CIST Root.
Priority	Specifies the four most significant bits of the Port Identifier of the Spanning Tree instance. It can be modified by setting the CISTPortPriority value. The values that are set for Port Priority must be in steps of 16.
DesignatedRoot	Specifies the unique Bridge Identifier of the bridge. Recorded as the CIST Root in the configuration BPDUs which are transmitted.
DesignatedCost	Specifies the path cost of the Designated Port of the segment connected to this port.
DesignatedBridge	Specifies the unique Bridge Identifier of the bridge which the port considers to be the Designated Bridge for the port segment.
DesignatedPort	Specifies 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	Specifies the contribution of this port to the cost of paths towards the CIST Regional Root.
ProtocolMigration	Specifies the Protocol migration state of this port. When operating in MSTP mode, set this field to true to

Variable	Value
	force the port to transmit MSTP BPDUs without instance information. **Important:** 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	Specifies 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	Specifies 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	Specifies 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	Indicates the operational point-to-point status of the LAN segment attached to the port. It also indicates whether a port is considered to have a point-to-point connection. The value is determined by management or by autodetection, as described in the AdminP2P object.
HelloTime	Specifies 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	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	Specifies the operational state of the port for CIST. This is set to true only when the port is operationally

Variable	Value
	up in the Interface level and Protocol level for CIST. This is set to false for all other times.
State	Specifies the current state of the port as defined by the Common Spanning Tree Protocol.
ForcePortState	Specifies the current state of the port which can be changed to either Disabled or Enabled for the base Spanning Tree instance.
SelectedPortRole	Specifies the selected port role for the Spanning Tree instance.
CurrentPortRole	Specifies the current port role for the Spanning Tree instance.

Graphing CIST port statistics using EDM

Use this procedure to display and graph CIST port statistics.

Prerequisites

- Select MSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see Configuring the STP mode using EDM on page 239.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **CIST Ports** tab.
5. Select a port for which you want to view the statistic graph.
6. On the toolbar, click **Graph** to get the statistics for the CIST Port.

Variable Definitions

Variable	Value
ForwardTransitions	Specifies the number of times this port transitioned to the Forwarding State.
RxMstBpduCount	Specifies the number of MST BPDUs received on this port.
RxRstBpduCount	Specifies the number of RST BPDUs received on this port.
RxConfigBpduCount	Specifies the number of Configuration BPDUs received on this port.
RxTcnBpduCount	Specifies the number of TCN BPDUs received on this port.
TxMstBpduCount	Specifies the number of MST BPDUs transmitted from this port.
TxRstBpduCount	Specifies the number of RST BPDUs transmitted from this port.
TxConfigBpduCount	Specifies the number of Configuration BPDUs transmitted from this port.
TxTcnBpduCount	Specifies the number of TCN BPDUs transmitted from this port.
InvalidMstBpduRxCount	Specifies the number of Invalid MST BPDUs received on this port.
InvalidRstBpduRxCount	Specifies the number of Invalid RST BPDUs received on this port.
InvalidConfigBpdu RxCount	Specifies the number of Invalid Configuration BPDUs received on this port.
InvalidTcnBpduRxCount	Specifies the number of Invalid TCN BPDUs received on this port.
ProtocolMigrationCount	Specifies 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.

Viewing MSTI bridge information using EDM

Use this procedure to display MSTI bridge information..

Prerequisites

- Select MSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see Configuring the STP mode using EDM on page 239.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **MSTI Bridges** tab.

Variable Definitions

Variable	Value
Instance	Specifies the Spanning Tree Instance to which the information belongs.
RegionalRoot	Specifies 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	Specifies 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	Specifies the cost of the path to the MSTI Regional Root as seen by this bridge.
RootPort	Specifies the number of the port which offers the lowest path cost from this bridge to the MSTI Region Root Bridge.

Variable	Value
Enabled	Used to control whether the bridge instance is enabled or disabled.
TimeSinceTopology Change	Specifies 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	Specifies the number of times that at least one non-zero TcWhile Timer occurred on this Bridge for this Spanning Tree instance.
NewRootCount	Specifies 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	Specifies the number of times a new Spanning Tree instance was created. A Trap is generated on the occurrence of this event.
InstanceDownCount	Specifies the number of times a Spanning Tree instance was deleted. A Trap is generated on the occurrence of this event.

Inserting MSTI Bridges using EDM

Use the following procedure to insert an MSTI bridge.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **MSTI Bridges** tab.
5. On the toolbar, click **Insert**.

   The Insert MSTI Bridges dialog box appears with the next available instance shown.
6. Click **Insert**.

Deleting MSTI Bridges using EDM

Use the following procedure to delete an MSTI bridge.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **MSTI Bridges** tab.
5. In the table, select the MSTI bridge instance that you want to delete.
6. On the toolbar, click **Delete**.

   The selected instance is deleted from the MSTI Bridges tab.

Viewing MSTI port information using EDM

Use this procedure to display MSTI port information.

Prerequisites

- Select MSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see Configuring the STP mode using EDM on page 239.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **MSTI Port** tab.

Variable Definitions

Variable	Value
Port	Specifies the port number.
Instance	Specifies the number of times a Spanning Tree instance was deleted. A Trap is generated when this event occurs.

Variable	Value
State	Specifies 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	Specifies the current state of the port which can be changed to either Disabled or Enabled for the specific Spanning Tree instance.
PathCost	Specifies the contribution of this port to the cost of paths towards the MSTI Root which includes this port.
Priority	Specifies 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 supported by the Bridge. The values set for Port Priority must be in steps of 16.
DesignatedRoot	Specifies the unique Bridge Identifier of the bridge recorded as the MSTI Regional Root in the configuration BPDUs that are transmitted.
DesignatedBridge	Specifies the unique Bridge Identifier of the bridge which this port considers to be the Designated Bridge for the port segment.
DesignatedPort	Specifies the Port identifier of the port on the Designated Bridge for this port segment.
DesignatedCost	Specifies the path cost of the Designated Port of the segment connected to this port.
CurrentPortRole	Specifies the Current Port Role of the port for this spanning tree instance.
EffectivePortState	Specifies 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 MSTI port statistics using EDM

Use this procedure to display and graph MSTI port statistics.

Prerequistes

- Select MSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see Configuring the STP mode using EDM on page 239.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **MSTI Port** tab.
5. In the table, select the port for which you want to view the statistics.
6. On the toolbar, click **Graph** to get the statistics for the MSTI Port.

Variable Definitions

Variable	Value
ForwardTransitions	Specifies the number of times this port transitioned to the Forwarding State for the specific instance.
ReceivedBPDUs	Specifies the number of BPDUs received by this port for this spanning tree instance.
TransmittedBPDUs	Specifies the number of Invalid BPDUs received on this Port for this Spanning Tree instance.
InvalidBPDUsRcvd	Specifies the number of BPDUs transmitted on this port for this Spanning Tree instance.

Chapter 18: ADAC configuration using Enterprise Device Manager

This chapter provides information you can use to configure Autodetection and Autoconfiguration (ADAC) using Enterprise Device Manager (EDM).

Configuring ADAC globally using EDM

Use the following procedure to configure ADAC for the switch.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **ADAC**.
3. Click the **ADAC** tab.
4. Select the **AdminEnable** check box to enable ADAC.

   OR

   Clear the **AdminEnable** check box to disable ADAC.
5. In the **OperatingMode** section, select a radio button.
6. Select the **NotificationControlEnable** check box to enable trap notifications.

   OR

   Clear the **NotificationControlEnable** check box to disable trap notifications.
7. Double-click the **Voice VLAN** dialog box to edit the value as required.
8. Click the **CallServerPortList** ellipsis.
9. From the call server port list, select call server ports.
10. Click **Ok**.
11. Click the **UplinkPortList** ellipsis.
12. From the uplink port list, select uplink ports.
13. Click **Ok**.

14. In the **MacAddrRangeControl** section, select a radio button.
15. Click **Apply**.

Important:

You cannot apply the global ADAC configuration if VoiceVLAN, CallServerPort, or UplinkPort boxes are set to 0 or empty when AdminEnable is selected and the operating mode is tagged frames or advanced untagged frames.

Important:

You cannot configure the same port values for Call Server and Uplink.

Variable Definitions

Variable	Value
AdminEnable	Enables or disables ADAC.
OperEnable	Indicates ADAC operational state: true is enabled and false is disabled. **Important:** If AdminEnable is True and OperEnable is False, this indicates an error condition such as missing Uplink and Call Server ports.
OperatingMode	Selects the ADAC operation mode: • untaggedFramesBasic—IP Phones send untagged frames, and the Voice VLAN is not created. • untaggedFramesAdvanced—IP Phones send untagged frames, and the Voice VLAN is created. • taggedFrames—IP Phones send tagged frames.
NotificationControlEnable	Enables or disables ADAC trap notifications.
VoiceVLAN	Sets the Voice VLAN ID.
CallServerPort	Selects the Call Server port. A maximum of 8 Call Server ports are supported.
UplinkPort	Selects the Uplink port. A maximum of 8 Uplink ports are supported.
MacAddrRangeControl	Selects a MAC address range table control option.

Variable	Value
	• none—default • clearTable—clears all MAC address range table entries. • defaultTable—replaces all MAC address range table entries to default values.

ADAC MAC address range configuration using EDM

Use the information in this section to manage the ADAC MAC address range table.

Creating a ADAC MAC address range using EDM

Use the following procedure to add an Avaya IP Phone MAC address range to the ADAC MAC address range table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **ADAC**.
3. Click the **ADAC MAC Ranges** tab.
4. Click **Insert**.
5. In the **MacAddrRangeLowEndIndex** box, type the MAC address for the low end of the IP Phone MAC address range.
6. In the **MacAddrRangeHighEndIndex** box, type the MAC address for the high end of the IP Phone MAC address range.
7. Click **Insert**.
8. Click **Apply**.

Deleting MAC address ranges using EDM

Use the following procedure to remove Avaya IP Phone MAC address ranges from the ADAC MAC address range table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **ADAC**.
3. Click the **ADAC MAC Ranges** tab.
4. Click the MAC address range to delete.
5. Click **Delete**.

ADAC port configuration using EDM

Use the information in this section to configure ADAC for switch ports and to display port-based ADAC information.

Viewing the ADAC configuration for ports using EDM

Use the following procedure to display the ADAC configuration for ports on the switch.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis** then double-click **Ports**.

   OR

   In the Edit tree, double-click **ADAC** .
3. In the Ports work area, click the **ADAC** tab.

   OR

   In the ADAC work area, click the **ADAC Ports** tab.

Variable Definitions

Variable	Value
Index	Indicates the switch position in a stack and the port number. The default value for a standalone switch is 1.
AdminEnable	Indicates whether ADAC is enabled (true) or disabled (false) for the port.
OperEnable	Indicates whether the port ADAC operational state is true (enabled) or false (disabled). This is a read-only cell. ❗ **Important:** If OperEnable is false and AdminEnable is true, ADAC is disabled. This can occur if you reach the maximum number of devices supported on a port.
ConfigStatus	Indicates the ADAC status for the port. • configApplied—the ADAC configuration is applied to the port. • configNotApplied—the ADAC configuration is not applied to the port. This is a read-only cell.
TaggedFramesPVID	Indicates the unique Port VLAN identifier (PVID). Values range from 0–4094. A value of 0 indicates that Auto-Configuration cannot change the PVID for the port.
TaggedFramesTagging	Indicates the tagging value that Auto-Configuration applies to a port that has ADAC enabled and has tagged frames selected as the operating mode. • tagAll—tagging is enabled on all frames • tagPvidOnly—tagging is enabled on frames with a PVID that matches the PVID of this port • untagPvidOnly—tagging is disabled on frames with a PVID that matches the PVID of this port • noChange—accepts frames without change
AdacPortType	Indicates how ADAC classifies the port: • telephony—autodetection is enabled for the port • callServer—the port is configured as a Call Server

Variable	Value
	• uplink—the port is configured as an Uplink • other—the port is not classified as telephony, callServer, or uplink
MacDetectionEnable	Indicates whether Autodetection of Avaya IP Phones, based on MAC address is enabled (true) or disabled (false) on the interface. ❗ **Important:** You cannot configure MacDetectionEnable to false if no other supported detection mechanism is enabled on the port.
LldpDetectionEnable	Indicates whether Autodetection of Avaya IP Phones, based on 802.1ab is enabled (true) or disabled (false) on the interface. ❗ **Important:** You cannot configure LldpDetectionEnable to false if no other supported detection mechanism is enabled on the port.

Configuring ADAC for specific ports using EDM

Use the following procedure to configure ADAC for one or more ports in a standalone switch or switch stack.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis** then double-click **Ports**.

   OR

   In the Edit tree, double-click **ADAC** .
3. In the Ports work area, click the **ADAC** tab.

   OR

   In the ADAC work area, click the **ADAC Ports** tab.
4. To select a port to edit, click the port **Index**.
5. In the port row, double-click the cell in the **AdminEnable** column.

6. Select a value from the list—**true** to enable ADAC for the port, or **false** to disable ADAC for the port.
7. In the port row, double-click the cell in the **TaggedFramesPvid** column.
8. Type a value in the dialog box.
9. In the port row, double-click the cell in the **TaggedFramesTagging** column.
10. Select a value from the list.
11. In the port row, double-click the cell in the **MacDetectionEnable** column.
12. Select a value from the list—**true** to enable MAC address detection for the port, or **false** to disable MAC address detection for the port.
13. In the port row, double-click the cell in the **LldpDetectionEnable** column.
14. Select a value from the list—**true** to enable LLDP detection for the port, or **false** to disable LLDP detection for the port.
15. You can repeat steps **4** through **14** to configure ADAC for additional ports.
16. Click **Apply**.

Variable Definitions

Variable	Value
Index	Indicates the switch position in a stack and the port number. The default value for a standalone switch is 1.
AdminEnable	Enables (true) or disables (false) ADAC for the port.
OperEnable	Indicates whether the port ADAC operational state is true (enabled) or false (disabled). This is a read-only cell. **Important:** If OperEnable is false and AdminEnable is true, ADAC is disabled. This can occur if you reach the maximum number of devices supported on a port.
ConfigStatus	Indicates the ADAC status for the port. • configApplied—the ADAC configuration is applied to the port. • configNotApplied—the ADAC configuration is not applied to the port. This is a read-only cell.

Variable	Value
TaggedFramesPVID	Specifies a unique Port VLAN identifier (PVID). Values range from 0–4094. A value of 0 indicates that Auto-Configuration cannot change the PVID for the port.
TaggedFramesTagging	Specifies the tagging value that Auto-Configuration applies to a port that has ADAC enabled and has tagged frames selected as the operating mode. • tagAll—tagging is enabled on all frames • tagPvidOnly—tagging is enabled on frames with a PVID that matches the PVID of this port • untagPvidOnly—tagging is disabled on frames with a PVID that matches the PVID of this port • noChange—accepts frames without change
AdacPortType	Indicates how ADAC classifies the port: • telephony—autodetection is enabled for the port • callServer—the port is configured as a Call Server • uplink—the port is configured as an Uplink • other—the port is not classified as telephony, callServer, or uplink
MacDetectionEnable	Specifies whether Autodetection of Avaya IP Phones, based on MAC address is enabled (true) or disabled (false) on the interface. ❗ **Important:** You cannot configure MacDetectionEnable to false if no other supported detection mechanism is enabled on the port.
LldpDetectionEnable	Specifies whether Autodetection of Avaya IP Phones, based on 802.1ab is enabled (true) or disabled (false) on the interface. ❗ **Important:** You cannot configure LldpDetectionEnable to false if no other supported detection mechanism is enabled on the port.

Chapter 19: LACP and VLACP configuration using Enterprise Device Manager

This chapter provides information you can use to configure Link Aggregation Control Protocol (LACP) and Virtual LACP (VLACP) using Enterprise Device Manager (EDM).

Viewing LAG information using EDM

Use the following procedure to display Link Aggregation Group (LAG) configuration information.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **LACP** tab.

Variable Definitions

Variable	Value
Index	Indicates the unique identifier allocated to an Aggregator by the local system.
MacAddress	Indicates the MAC address assigned to an Aggregator.
AggregateOrIndividual	Indicates if an Aggregator represents an Aggregate (TRUE) or an individual link (FALSE).
ActorLagID	Indicates the combined information of ActorSystemPriority, ActorSystemID, and ActorOperKey in ActorSystemPriority-ActorSystemID-ActorOperKey format.

Variable	Value
ActorSystemPriority	Indicates the priority value associated with the Actor's System ID.
ActorSystemID	Indicates the MAC address of the System that contains this Aggregator.
ActorOperKey	Indicates the current operational value of the Aggregator key.
ActorAdminKey	Indicates the current administrative value of the Aggregator key.
PartnerLagID	Indicates the combined of PartnerSystemPriority, PartnerSystemID, and PartnerOperKey in PartnerSystemPriority-PartnerSystemID-PartnerOper Key format.
PartnerSystemPriority	Indicates the priority value associated with the Partner System ID.
PartnerSystemID	Indicates the MAC address of 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	Indicates the operational key value of the current Aggregator protocol partner.
CollectorMaxDelay	Indicates 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.

Link Aggregation Group configuration using EDM

Use the procedures in this section to display or modify LAG member configuration.

Viewing LACP for LAG members using EDM

Use the following procedure to display the existing LACP configuration for LAG members.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **LACP Ports** tab.

Variable Definitions

Variable	Value
Index	Indicates the unique identifier allocated to an Aggregator by the local system.
AdminEnabled	Indicates the current administrative setting for the port. A value of true enables the port to participate in LACP. A value of false disables the port from participating in LACP.
OperEnabled	Indicates 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.
ActorAdminState	Indicates the Actor administrative state for the port. Values include: • lacpActive • aggregation • shortTimeout
ActorOperState	Indicates the current operational values of Actor state transmitted by the Actor in LACPDUs.
AggregateOrIndividual	Indicates whether the port represents an Aggregate or an Individual link.
ActorPortPriority	Indicates the priority value assigned to this Aggregation port. Values range from 0–65535.
ActorAdminKey	Indicates the current administrative value of the Key for the Aggregation Port. Values range from 1–4095.
ActorOperKey	Indicates the current operational value of the Key for the Aggregation Port.
SelectedAggID	Indicates 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

Variable	Value
	Aggregator or because no suitable Aggregator exists for it to select.
AttachedAggID	Indicates 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.
ActorPort	Indicates 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
MltId	Indicates the MLT that the port is assigned to. If the port is not assigned to an MLT, the MltId value is 0.
PartnerOperPort	Indicates the operational port number assigned by the port protocol partner.
OperStatus	Indicates the operational status of the interface. Values are up (operational) or down (not operational).

Configuring LACP for specific LAG members using EDM

Use the following procedure to configure LACP for one or more LAG member ports.

Prerequisites

- Ensure members you want to configure are not ADAC Call Server or Uplink ports.
- Disable ADAC for members you want to configure

❗ **Important:**

To configure the port LACP mode to active, you must set the AdminEnabled value to **true** and the ActorAdminState value to **lacpActive.**

❗ **Important:**

To configure the port LACP mode to passive, you must set the AdminEnabled value to **false** and clear the **lacpActive**, **aggregation**, and **shortTimeout** check boxes in ActorAdminState.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **LACP Ports** tab.

4. To select a port to configure, click the port **Index**.
5. In the port row, double-click the cell in the **AdminEnabled** column.
6. Select a value from the list—**true** to enable LACP for the port, or **false** to disable LACP for the port.
7. In the port row, double-click the cell in the **ActorAdminState** column.
8. Select an individual or combination of check boxes.
9. Click **Ok**.
10. In the port row, double-click the cell in the **ActorPortPriority** column.
11. In the dialog box, edit the value as required.
12. In the port row, double-click the cell in the **ActorAdminKey** column.
13. In the dialog box, edit the value as required.
14. You can repeat steps **4** through **13** to configure LACP for additional ports.
15. Click **Apply**.

Variable Definitions

Use the data in this table to configure LACP for LAG members.

Variable	Value
Index	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
AdminEnabled	Specifies the current administrative setting for the port. A value of true enables the port to participate in LACP. A value of false disables the port from participating in LACP. **Important:** You cannot enable ports to participate in LACP if they are members of an enabled MLT.
OperEnabled	Indicates 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. This is a read-only cell.
ActorAdminState	Specifies the Actor administrative state. Values include: • lacpActive • aggregation • shortTimeout

Variable	Value
ActorOperState	Indicates the current Actor operational state. This is a read-only cell.
AggregateOrIndividual	Indicates whether the Aggregator represents an Aggregate or an Individual link. This is a read-only cell.
ActorPortPriority	Specifies the priority value assigned to this Aggregation port. Values range from 0–65535.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation Port. Values range from 1–4095.
ActorOperKey	Indicates the current operational value of the Key for the Aggregation Port. This is a read-only cell.
SelectedAggID	Indicates 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. This is a read-only cell.
AttachedAggID	Indicates 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 is a read-only cell.
ActorPort	Indicates the port number locally assigned to the Aggregation Port. The port number is communicated in LACPDUs as the Actor_Port. This is a read-only cell.
MltId	Indicates the MLT that the port is assigned to. If the port is not assigned to an MLT, the MltId value is 0. This is a read-only cell.
PartnerOperPort	The operational port number assigned by the port's protocol partner. This is a read-only cell.
OperStatus	Indicates the operational status of the interface. Values are up (operational) or down (not operational). This is a read-only cell.

Configuring Static LACP Key to Trunk ID binding using EDM

Use the following procedures to configure and manage Static LACP Key to Trunk ID binding using ACLI.

Note:

Partner configuration is also required. The local ports do not aggregate if the remote ends of the links are not part of a similar configuration.

Binding an LACP key to a specific trunk ID using EDM

Use the following procedure to bind an LACP key to a specific MLT ID.

Procedure

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **LACP key mapping** tab.
4. Click **Insert**.
5. In the **LacpKeyValue** dialog box, type a value.
6. In the **MltId** dialog box, type a value.
7. Click **Insert**.
8. Click **Apply**.

Variable Definitions

Variable	Value
LacpKeyValue	Specifies the LACP key to use.
MltId	Specifies the MLT ID.

Deleting an LACP key binding to a trunk ID using EDM

Use the following procedure to delete an LACP key binding to a trunk ID.

Procedure

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **LACP key mapping** tab.
4. To select an LACP key binding to a trunk ID, click the LACPKeyValue ID.
5. Click **Delete**.
6. Click **Yes** to confirm.
   The selected LACP Key binding is deleted from the LACP key mapping tab.

Viewing LACP key bindings to trunk IDs using EDM

Use this procedure to display LACP key bindings to trunk IDs.

Procedure

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **LACP key mapping** tab.

LACP configuration for ports using EDM

You can use the information in this section to display or modify the LACP configuration for switch ports.

Viewing the LACP configuration for ports using EDM

Use the following procedure to display the existing LACP configuration for switch ports.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. Click the **LACP** tab.

Variable definitions

Variable	Value
ActorSystemPriority	Specifies the priority value associated with the Actor System ID. Values range from 0–65535.
AdminEnabled	Specifies the current administrative setting for the port. A value of true enables the port to participate in LACP. A

Variable	Value
	value of false disables the port from participating in LACP. **Important:** You cannot enable ports to participate in LACP if they are members of an enabled MLT.
OperEnabled	Indicates 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. This is a read-only cell.
ActorAdminState	Specifies the Actor administrative state. Values include: • lacpActive • aggregation • shortTimeout
ActorOperState	Indicates the current Actor operational state. This is a read-only cell.
AggregateOrIndividual	Indicates whether the Aggregator represents an Aggregate or an Individual link. This is a read-only cell.
ActorPortPriority	Specifies the priority value assigned to this Aggregation port. Values range from 0–65535.
ActorSystemID	Indicates the MAC address of the System that contains this Aggregator.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation Port. Values range from 1–4095.
ActorOperKey	Indicates the current operational value of the Key for the Aggregation Port. This is a read-only cell.
SelectedAggID	Indicates 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. This is a read-only cell.
AttachedAggID	Indicates 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 is a read-only cell.
ActorPort	Indicates the port number locally assigned to the Aggregation Port. The port number is communicated in LACPDUs as the Actor_Port. This is a read-only cell.

Variable	Value
PartnerOperPort	Indicates the operational port number assigned by the port's protocol partner. This is a read-only cell.

Important:

To configure the port LACP mode to active, you must set the AdminEnabled value to **true** and the ActorAdminState value to **lacpActive**.

Important:

To configure the port LACP mode to passive, you must set the AdminEnabled value to **false** and clear the **lacpActive**, **aggregation**, and **shortTimeout** check boxes in ActorAdminState.

Configuring LACP for ports using EDM

Use the following procedure to modify the LACP configuration for switch ports.

Prerequisites

- Ensure ports you want to configure are not ADAC Call Server or Uplink ports.
- Disable ADAC for ports you want to configure

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. Click the **LACP** tab.
5. To select a port to configure, click the port **Index**.
6. In the port row, double-click the cell in the **ActorSystemPriority** column.
7. In the dialog box, edit the value as required.
8. In the port row, double-click the cell in the **AdminEnabled** column.
9. Select a value from the list—**true** to enable LACP for the port, or **false** to disable LACP for the port.
10. In the port row, double-click the cell in the **ActorAdminState** column.
11. Select an individual or combination of check boxes
12. Click **Ok**.
13. In the port row, double-click the cell in the **ActorPortPriority** column.

14. In the dialog box, edit the value as required.
15. In the port row, double-click the cell in the **ActorAdminKey** column.
16. In the dialog box, edit the value as required.
17. You can repeat steps **5** through **17** to configure LACP for additional ports as required.
18. Click **Apply**.

Variable definitions

Variable	Value
ActorSystemPriority	Specifies the priority value associated with the Actor System ID. Values range from 0–65535.
AdminEnabled	Specifies the current administrative setting for the port. A value of true enables the port to participate in LACP. A value of false disables the port from participating in LACP. **Important:** You cannot enable ports to participate in LACP if they are members of an enabled MLT.
OperEnabled	Indicates 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. This is a read-only cell.
ActorAdminState	Specifies the Actor administrative state. Values include: • lacpActive • aggregation • shortTimeout
ActorOperState	Indicates the current Actor operational state. This is a read-only cell.
AggregateOrIndividual	Indicates whether the Aggregator represents an Aggregate or an Individual link. This is a read-only cell.
ActorPortPriority	Specifies the priority value assigned to this Aggregation port. Values range from 0–65535.
ActorSystemID	Indicates the MAC address of the System that contains this Aggregator. This is a read-only cell.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation Port. Values range from 1–4095.

Variable	Value
ActorOperKey	Indicates the current operational value of the Key for the Aggregation Port. This is a read-only cell.
SelectedAggID	Indicates 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. This is a read-only cell.
AttachedAggID	Indicates 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 is a read-only cell.
ActorPort	Indicates the port number locally assigned to the Aggregation Port. The port number is communicated in LACPDUs as the Actor_Port. This is a read-only cell.
PartnerOperPort	Indicates the operational port number assigned by the protocol partner of port. This is a read-only cell.

Important:

To configure the port LACP mode to active, you must set the AdminEnabled value to **true** and the ActorAdminState value to **lacpActive**.

Important:

To configure the port LACP mode to passive, you must set the AdminEnabled value to **false** and clear the **lacpActive**, **aggregation**, and **shortTimeout** check boxes in **ActorAdminState**.

Graphing port LACP statistics using EDM

Use the following procedure to display and graph LACP statistics for switch ports.

Procedure steps

1. From the Device Physical View, click a port.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port** .
4. In the work area, click the **LACP** tab.

5. On the toolbar, select a **Poll Interval** from the list.
6. To select statistics to graph, click a statistic type row under a column heading.
7. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

Variable	Value
LACPDUsRx	Denotes the number of valid LACPDUs received on this Aggregation Port. This value is read-only.
MarkerPDUsRx	Signifies the number of valid Marker PDUs received on this Aggregation Port. This value is read-only.
MarkerResponse PDUsRx	The number of valid Marker Response PDUs received on this Aggregation Port. This value is read-only.
UnknownRx	Indicates the number of frames received that can • Carry the Slow Protocols Ethernet Type value (43B.4), but contain an unknown PDU. • Are addressed to the Slow Protocols group MAC Address (43B.3), but do not carry the Slow Protocols Ethernet Type. This value is read-only.
IllegalRx	Denotes the number of frames received that carry the Slow Protocols Ethernet Type value (43B.4), but contain a badly formed PDU or an illegal value of Protocol Subtype (43B.4). This value is read-only.
LACPDUsTx	Signifies the number of LACPDUs that are transmitted on this Aggregation Port. This value is read-only.
MarkerPDUsTx	Displays the number of Marker PDUs transmitted on this Aggregation Port. This value is read-only.
MarkerResponse PDUsTx	Indicates the number of Marker Response PDUs that are transmitted on this Aggregation Port. This value is read-only.

Global VLACP/MLT configuration using EDM

Use the information in this section to:

- Enable or disable VLACP globally.
- Enable or disable MLT ports on shutdown.

Enabling global VLACP using EDM

Use the following procedure to enable VLACP for the switch.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **Global** tab.
4. Select the **VlacpEnable** check box to enable global VLACP.
5. Type a value in the MulticastMACAddress dialog box.
6. On the toolbar, click **Apply**.
7. On the toolbar, you can click **Refresh** to verify the global VLACP configuration.

Variable Definitions

Variable	Value
VlacpEnable	Enables or disables VLACP globally for the switch.
MulticastMACAddress	Specifies a multicast MAC address used exclusively for VLACP PDUs. The default is 01:80:c2:00:11:00. ✱ **Note:** VLACP supports only one multicast MAC address.

Disabling global VLACP using EDM

Use the following procedure to disable VLACP for the switch.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **VLACP Global** tab.

4. Clear the **VlacpEnable** check box.
5. On the toolbar, click **Apply**.

Enabling or disabling MLT ports on shutdown

Use this procedure to configure the system to enable or disable MLT ports on shutdown.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **Global** tab.
4. Select the **MltDisablePortsOnShutdown** check box to disable MLT ports on shutdown.

   OR

   Clear the **MltDisablePortsOnShutdown** check box for MLT ports to remain enabled on shutdown.
5. On the toolbar, click **Apply**.

Variable Definitions

Variable	Value
MltDisablePortsOnShutdown	When selected (enabled), the first port of the MLT continues to operate and all remaining MLT ports are disabled when MLT is shutdown. DEFAULT: cleared (disabled)

VLACP configuration for ports using EDM

Use the procedures in this section to view and configure VLACP at the port level.

Viewing the VLACP configuration for ports using EDM

Use the following procedure to display the VLACP configuration for all ports on a switch or stack.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. Click the **VLACP** tab.

Variable Definitions

Variable	Value
rcPortIndex	Indicates the switch and port number.
AdminEnable	Indicates whether VLACP is enabled (true) or disabled (false) on ports. The default value is disabled.
OperEnable	Indicates whether VLACP is operationally enabled (true) or disabled (false). ❗ **Important:** VLACP is only operational when OperEnable is true and PortState is up.
FastPeriodicTimer	Indicates the number of milliseconds between periodic transmissions using short timeouts. Valid values range from 400-20000 with a default of 500.
SlowPeriodicTimer	Indicates the number of milliseconds between periodic transmissions using long timeouts. Values range from 10000-30000 with a default of 30000.
Timeout	Indicates whether the timeout control value is a short or long timeout.
TimeoutScale	Indicates the scale value used to calculate timeout from periodic time. Values range from 1–10. The default is 3. With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. If the timeout-scale is set to 1, the port timeout value does not take into account the normal travel

Variable	Value
	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. Avaya recommends that you set the timeout scale to a value larger than 1.
EtherType	Indicates VLACP protocol identification. The value can be entered as a numerical value ranging from 33025–33279 or a hexadecimal equivalent (8101–81ff). The default is 8103. Use the prefix **0x** to type a hexadecimal value in the dialog box. Only hexadecimal values display in the EtherType column of the VLACP work area.
EtherMacAddress	Indicates the MAC address of the switch or stack to which this port is sending VLACPDUs. This value cannot be configured as a multicast MAC. The default value is 00:00:00:00:00:00. VLACP uses only the multicast MAC address configured when VLACP is enabled globally. This is the Layer 2 destination address used for the VLACPDUs. The port-specific EtherMACAddress specifies the MAC address of the switch or stack to which this port is sending VLACPDUs. If you do not type a value for the EtherMACAddress, the first VLACP-enabled switch that receives the PDUs from a sending port becomes the intended recipient and processes the PDUs. If you want an intermediate switch to drop VLACP packets, configure EtherMACAddress with the desired destination MAC address. With EtherMACAddress configured, the intermediate switches do not misinterpret the VLACP packets.
PortState	Indicates whether the VLACP port state is up or down. **Important:** VLACP is only operational when OperEnable is true and PortState is up.

Configuring VLACP for multiple ports using EDM

Use the following procedure to configure VLACP for a single port or multiple ports.

Procedure steps

1. From the Device Physical View, click one or more ports.
2. From the navigation tree, double-click **Edit**.
3. In the Edit tree, double-click **Chassis**.
4. In the Chassis tree, double-click **Ports**.
5. Click the **VLACP** tab.
6. To select a port to edit, click **rcPortIndex** row.
7. In the port row, double-click the cell in the **AdminEnable** column.
8. Select a value from the list—**true** to enable VLACP for the port, or **false** to disable VLACP for the port.
9. In the port row, double-click the cell in the **FastPeriodicTimer** column.
10. Type a value in the dialog box.
11. In the port row, double-click the cell in the **SlowPeriodicTimer** column.
12. Type a value in the dialog box.
13. In the port row, double-click the cell in the **Timeout** column.
14. Select a value from the list.
15. In the port row, double-click the cell in the **TimeoutScale** column.
16. Type a value in the dialog box.
17. In the port row, double-click the cell in the **EtherType** column.
18. Type a value in the dialog box.
19. In the port row, double-click the cell in the **EtherMacAddress** column.
20. Type a value in the dialog box.
21. You can repeat steps **4** through **19** to configure VLACP for additional ports as required.
22. Click **Apply**.

Variable Definitions

Variable	Value
rcPortIndex	Specifies the switch and port number.

Variable	Value
AdminEnable	Indicates whether VLACP is enabled (true) or disabled (false) on ports. The default value is disabled.
OperEnable	Indicates whether VLACP is operationally enabled or disabled. This is a read-only cell. **Important:** VLACP is only operational when OperEnable is true and PortState is up.
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	Specifies the scale value used to calculate timeout from periodic time. Values range from 1–10. The default is 3. With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. If the timeout-scale is set to 1, 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. Avaya recommends that you set the timeout scale to a value larger than 1.
EtherType	Specifies VLACP protocol identification. The value can be entered as a numerical value ranging from 33025–33279 or a hexadecimal equivalent (8101–81ff). The default is 8103. Use the prefix 0x to type a hexadecimal value in the dialog box. Only hexadecimal values display in the EtherType column of the VLACP work area.
EtherMacAddress	Specifies the MAC address of the switch or stack to which a port is sending VLACPDUs. The default value is 00:00:00:00:00:00. It cannot be configured as a multicast MAC. VLACP uses only the multicast MAC address configured when VLACP is enabled globally. This is the Layer 2 destination address used for the VLACPDUs. If you do not type a value for the EtherMACAddress, the first VLACP-enabled switch that receives the PDUs from a sending port becomes the intended recipient and processes the PDUs.

Variable	Value
	If you want an intermediate switch to drop VLACP packets, configure EtherMACAddress with the desired destination MAC address. With EtherMACAddress configured, the intermediate switches do not misinterpret the VLACP packets.
PortState	Indicates whether the VLACP port state is up or down. This is a read-only cell. ❗ **Important:** VLACP is only operational when OperEnable is true and PortState is up.

Configuring VLACP for specific ports using EDM

Use the following procedure to configure VLACP for a single port or multiple ports.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. Click the **VLACP Ports** tab.
4. To select a port to edit, click **rcPortIndex** row.
5. In the port row, double-click the cell in the **AdminEnable** column.
6. Select a value from the list—**true** to enable VLACP for the port, or **false** to disable VLACP for the port.
7. In the port row, double-click the cell in the **FastPeriodicTimer** column.
8. Type a value in the dialog box.
9. In the port row, double-click the cell in the **SlowPeriodicTimer** column.
10. Type a value in the dialog box.
11. In the port row, double-click the cell in the **Timeout** column.
12. Select a value from the list.
13. In the port row, double-click the cell in the **TimeoutScale** column.
14. Type a value in the dialog box.
15. In the port row, double-click the cell in the **EtherType** column.
16. Type a value in the dialog box.

17. In the port row, double-click the cell in the **EtherMacAddress** column.
18. Type a value in the dialog box.
19. You can repeat steps **4** through **19** to configure VLACP for additional ports as required.
20. Click **Apply**.

Variable Definitions

Variable	Value
rcPortIndex	Specifies the switch and port number.
AdminEnable	Indicates whether VLACP is enabled (true) or disabled (false) on ports. The default value is disabled.
OperEnable	Indicates whether VLACP is operationally enabled or disabled. This is a read-only cell. ❗ **Important:** VLACP is only operational when OperEnable is true and PortState is up.
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	Specifies the scale value used to calculate timeout from periodic time. Values range from 1–10. The default is 3. With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. If the timeout-scale is set to 1, 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. Avaya recommends that you set the timeout scale to a value larger than 1.
EtherType	Specifies VLACP protocol identification. The value can be entered as a numerical value ranging from 33025–33279 or a hexadecimal equivalent (8101–81ff). The default is 8103. Use the prefix 0x to type a hexadecimal value in the

Variable	Value
	dialog box. Only hexadecimal values display in the EtherType column of the VLACP work area.
EtherMacAddress	Specifies the MAC address of the switch or stack to which a port is sending VLACPDUs. The default value is 00:00:00:00:00:00. It cannot be configured as a multicast MAC. VLACP uses only the multicast MAC address configured when VLACP is enabled globally. This is the Layer 2 destination address used for the VLACPDUs. If you do not type a value for the EtherMACAddress, the first VLACP-enabled switch that receives the PDUs from a sending port becomes the intended recipient and processes the PDUs. If you want an intermediate switch to drop VLACP packets, configure EtherMACAddress with the desired destination MAC address. With EtherMACAddress configured, the intermediate switches do not misinterpret the VLACP packets.
PortState	Indicates whether the VLACP port state is up or down. This is a read-only cell. **Important:** VLACP is only operational when OperEnable is true and PortState is up.

Glossary

ACLI Avaya Command Line Interface (ACLI) is a text-based, common command line interface used for device configuration and management across Avaya products.

ACLI modes Differing command modes are available within the text-based interface, dependant on the level of user permissions determined by logon password. Each successive mode level provides access to more complex command sets, from the most restrictive—show level only, to the highest configuration levels for routing parameters, interface configuration, and security.

Address Resolution Protocol (ARP) Maps an IP address to a physical machine address, for example, maps an IP address to an Ethernet media access control (MAC) address.

American Standard Code for Information Interchange (ASCII) A code to represent characters in computers. ASCII uses uppercase and lowercase alphabetic letters, numeric digits, and special symbols.

Auto-Detection and Auto-Configuration (ADAC) Provides automatic switch configuration for IP phone traffic support and prioritization. ADAC can configure the switch whether it is directly connected to the Call Server or uses a network uplink.

Automatic PVID Automatically sets the port-based VLAN ID when you add the port to the VLAN. The PVID value is the same value as the last port-based VLAN ID associated with the port.

Autonegotiation Allows the switch to select the best speed and duplex modes for communication between two IEEE-capable devices.

bandwidth A measure of transmission capacity for a particular pathway, expressed in megabits per second (Mb/s).

base unit (BU) When you connect multiple switches into a stack, one unit, and only one unit, must be designated as a base unit to perform stack configuration tasks. The position of the unit select switch, on the back of the switch, determines base unit designation.

Bootstrap Protocol (BootP) A User Datagram Protocol (UDP)/Internet Protocol (IP)-based protocol that a booting host uses to configure itself dynamically and without user supervision.

Bridge Protocol Data Unit (BPDU) A data frame used to exchange information among the bridges in local or wide area networks for network topology maintenance.

Bridge Protocol Data Units Filtering (BPDU Filtering)
Prevents end devices from influencing an existing spanning tree topology by disabling any port sending BPDUs for appropriately configured ports.

Bridging
A forwarding process, used on Local Area Networks (LAN) and confined to network bridges, that works on Layer 2 and depends on the Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP). Bridging is also known as MAC forwarding.

common and internal spanning tree (CIST)
The single spanning tree calculated by the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP) to ensure that all LANs in a bridged Local Area Network (LAN) are simply and fully connected.

common spanning tree (CST)
The single spanning tree calculated by STP, RSTP, and MSTP to connect multiple spanning tree (MST) regions.

Differentiated Services Code Point (DSCP)
The first six bits of the DS field. The DSCP uses packet marking to guarantee a fixed percentage of total bandwidth to each of several applications (guarantees quality of service).

Distributed MultiLink Trunking (DMLT)
A point-to-point connection that aggregates similar ports from different modules to logically act like a single port, but with the aggregated bandwidth.

Dynamic Host Configuration Protocol (DHCP)
A standard Internet protocol that dynamically configures hosts on an Internet Protocol (IP) network for either IPv4 or IPv6. DHCP extends the Bootstrap Protocol (BOOTP).

Enterprise Device Manager (EDM)
A Web-based embedded management system to support single-element management. EDM provides complete configuration management functionality for the supported devices and is supplied to the customer as embedded software in the device.

far end fault indication (FEFI)
Determines that one of two unidirectional fibers, that form the connection between two switches, fails.

Frame Check Sequence (FCS)
Frames are used to send upper-layer data and ultimately the user application data from a source to a destination.

graphical user interface (GUI)
A graphical (rather than textual) computer interface.

Institute of Electrical and Electronics Engineers (IEEE)
An international professional society that issues standards and is a member of the American National Standards Institute, the International Standards Institute, and the International Standards Organization.

Internet Group Management Protocol (IGMP) IGMP is a host membership protocol used to arbitrate membership in multicast services. IP multicast routers use IGMP to learn the existence of host group members on their directly attached subnets.

Internet Protocol version 4 (IPv4) The protocol used to format packets for the Internet and many enterprise networks. IPv4 provides packet routing and reassembly.

Internet Protocol version 6 (IPv6) An improved version of the IP protocol, IPv6 improves the IPv4 limitations of security and user address numbers.

Layer 2 Layer 2 is the Data Link Layer of the OSI model. Examples of Layer 2 protocols are: Ethernet and Frame Relay.

Layer 3 Layer 3 is the Network Layer of the OSI model. An example of a Layer 3 protocol is Internet Protocol (IP).

Link Aggregation Provides the mechanism to create and manage trunk groups automatically using Link Aggregation Control Protocol (LACP).

Link Aggregation Control Protocol (LACP) A network handshaking protocol that provides a means to aggregate multiple links between appropriately configured devices.

link aggregation group (LAG) A group that increases the link speed beyond the limits of one single cable or port, and increases the redundancy for higher availability.

Link Layer Discovery Protocol (LLDP) Link Layer Discovery Protocol is used by network devices to advertise their identities. Devices send LLDP information at fixed intervals in the form of Ethernet frames, with each frame having one Link Layer Discovery Protocol Data Unit.

load balancing The practice of splitting communication into two (or more) routes or servers.

Local Area Network (LAN) A data communications system that lies within a limited spatial area, uses a specific user group and topology, and can connect to a public switched telecommunications network (but is not one).

Logical Link Control (LLC) A protocol used in LANs to transmit protocol data units between two end stations. This LLC layer addresses and arbitrates data exchange between two endpoints.

mask A bit string that the device uses along with an IP address to indicate the number of leading bits in the address that correspond with the network part.

maximum transmission unit (MTU) The largest number of bytes in a packet—the maximum transmission unit of the port.

media A substance that transmits data between ports; usually fiber optic cables or category 5 unshielded twisted pair (UTP) copper wires.

Media Access Control (MAC) Arbitrates access to and from a shared medium.

Message Digest 5 (MD5) A one-way hash function that creates a message digest for digital signatures.

MultiLink Trunking (MLT) A method of link aggregation that uses multiple Ethernet trunks aggregated to provide a single logical trunk. A multilink trunk provides the combined bandwidth of multiple links and the physical layer protection against the failure of a single link.

multiple spanning tree bridge A bridge that supports the common spanning tree (CST) and one or more multiple spanning tree instances (MSTI) and selectively maps frames classified in a VLAN to the CST or an MSTI.

multiple spanning tree instance (MSTI) One of a number of spanning trees calculated by the Multiple Spanning Tree Protocol (MSTP) within an MST region, to provide a simple and fully connected active topology for frames that belong to a VLAN mapped to the MSTI.

Multiple Spanning Tree Protocol (MSTP) Configures multiple instances of the Rapid Spanning Tree Protocol (RSTP) on the switch.

multiple spanning tree region A set of LANs and MST bridges physically connected by ports on the MST bridges.

Network Basic Input/Output System (NetBIOS) An application programming interface (API) that augments the DOS BIOS by adding special functions for Local Area Networks (LAN).

nonbase unit (NBU) A nonbase unit is any unit in a stack except the base unit.

NonVolatile Random Access Memory (NVRAM) Random Access Memory that retains its contents after electrical power turns off.

Open Shortest Path First (OSPF) A link-state routing protocol used as an Interior Gateway Protocol (IGP).

port A physical interface that transmits and receives data.

port mirroring A feature that sends received or transmitted traffic to a second destination.

port VLAN ID Used to coordinate VLANs across multiple switches. When you create a port-based VLAN on a switch, assign a VLAN identification number (VLAN ID) and specify the ports that belong to the VLAN.

prefix A group of contiguous bits, from 0 to 32 bits in length, that defines a set of addresses.

Protocol Data Units (PDUs) A unit of data that is specified in a protocol of a specific layer and that consists of protocol-control information of the specific layer and possibly user data of that layer.

quality of service (QoS) QoS features reserve resources in a congested network, allowing you to configure a higher priority to certain devices. For example, you can configure a higher priority to IP deskphones, which need a fixed bit rate, and, split the remaining bandwidth between data connections if calls in the network are more important than the file transfers.

Rapid Spanning Tree Protocol (RSTP) Reduces the recovery time after a network breakdown. RSTP enhances switch-generated Topology Change Notification (TCN) packets to reduce network flooding.

rate limiting Rate limiting sets the percentage of traffic that is multicast, broadcast, or both, on specified ports.

Remote Authentication Dial-in User Service (RADIUS) A protocol that authenticates, authorizes, and accounts for remote access connections that use dial-up networking and Virtual Private Network (VPN) functionality.

Routing Information Protocol (RIP) A distance vector protocol in the IP suite, used by IP network-layer protocol, that enables routers in the same AS to exchange routing information by means of periodic updates. You often use RIP as a very simple interior gateway protocol (IGP) within small networks.

routing switch Virtualizes the physical router interfaces to switches. A virtual router port, or interface, acts as a router port to consolidate switching and routing functions in the broadcast domain, or between broadcast domains, and enable IP routing for higher traffic volumes.

spanning tree A simple, fully-connected active topology formed from the arbitrary physical topology of connected bridged Local Area Network components by relaying frames through selected bridge ports. The protocol parameters and states that are used and exchanged to facilitate the calculation of the active topology and to control the bridge relay function.

Spanning Tree Group (STG) A collection of ports in one spanning tree instance.

Spanning Tree Protocol (STP) MAC bridges use the STP to exchange information across Local Area Networks to compute the active topology of a bridged Local Area Network in accordance with the Spanning Tree Protocol algorithm.

Split MultiLink Trunking (SMLT) An Avaya extension to IEEE 802.1AX (link aggregation), provides nodal and link failure protection and flexible bandwidth scaling to improve on the level of Layer 2 resiliency.

stack Stackable Avaya Ethernet Routing Switches can be connected in a stack configuration of two or more units, up to eight units maximum. A switch stack operates and is managed as a single virtual switch.

stand-alone Refers to a single Avaya Ethernet Routing Switch operating outside a stack.

Transmission Control Protocol (TCP) Provides flow control and sequencing for transmitted data over an end-to-end connection.

trunk A logical group of ports that behaves like a single large port.

User Datagram Protocol (UDP) In TCP/IP, a packet-level protocol built directly on the Internet Protocol layer. TCP/IP host systems use UDP for application-to-application programs.

Virtual Link Aggregation Control Protocol (VLACP) Virtual Link Aggregation Control Protocol (VLACP) is a Layer 2 handshaking protocol that can detect end-to-end failure between two physical Ethernet interfaces.

Virtual Local Area Network (VLAN) A Virtual Local Area Network is a group of hosts that communicate as if they are attached to the same broadcast domain regardless of their physical location. VLANs are layer 2 constructs.

Virtual Private Network (VPN) A Virtual Private Network (VPN) requires remote users to be authenticated and ensures private information is not accessible to unauthorized parties. A VPN can allow users to access network resources or to share data.