Avaya Ethernet Routing Switch 3500 Series Configuration — Layer 2

5.0
NN47203-500
Issue 01.02
March 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 reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller 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 RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; 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.

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

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: Purpose of this document

This document provides procedures and conceptual information to configure Layer 2; can include VLANs, Spanning Tree, Link Aggregation Control Protocol, Link Layer Discovery Protocol, and Multi-Link Trunking.

Chapter 2: New in this release

This is a new document for Avaya Ethernet Routing Switch 3500 Series Release 5.0.

The Avaya ERS 3500 Series is new and supports the following hardware and software features:

ERS 3500 hardware

The following table lists and describes the supported hardware for ERS 3500 Series 5.0. Question marks (?) in the table signify power cord types; substitute the following regional variants:

- A — no power cord
- B — EU power cord
- C — UK / Ireland power cord
- D — Japan power cord
- E — North American power cord
- F — Australia / New Zealand / China power cord

Note:

All switches support autopolarity.

Table 1: Hardware

Hardware	Description
Switch models	
AL3500?01–E6	3526T — 24 10/100BaseT ports supporting autosensing and autonegotiation, in a non-PoE , plus two 10/100/1000 or Small Form Pluggable (SFP) front combination ports, plus two SFP rear ports. Fanless.
AL3500?11–E6	3526T-PWR+ — 24 10/100BaseT PoE+ ports (802.3af/at), plus two 10/100/1000 or Small Form Pluggable (SFP) front combination ports, plus two SFP rear ports.
AL3500?04–E6	3510GT — 8 10/100/1000BaseT ports, plus two SFP ports (ports 9 and 10). Standalone and fanless.
AL3500?14–E6	3510GT-PWR+ — 8 10/100/1000BaseT PoE+ ports (802.3af/at), plus two SFP ports (ports 9 and 10). Standalone. Fanless operation in Low Power mode @ 60W max PoE budget, or normal fan

Hardware	Description
	operation in High Power mode @ 170W max PoE budget.
AL3500?05–E6	3524GT — 24 10/100/1000BaseT ports, four SFP ports shared with ports 21–24, plus two SFP rear ports.
AL3500?15–E6	3524GT-PWR+ — 24 10/100/1000BaseT PoE+ ports (802.3af/at), four SFP ports shared with ports 21–24, plus two SFP rear ports.
Rack Mount Kits	
AL3511001–E6	Spare Rack Mount Kit — this kit can be used as a replacement rack mount kit for ERS 3524GT, ERS 3524GT-PWR+, ERS 3526T or ERS 3526T-PWR + switches.
AL3511002–E6	3510–Pair Rack Mount Kit — this kit is used to connect two ERS 3510GT or ERS 3510GT-PWR+ switches together side by side and mount them in a 19 inch rack.
AL3511003–E6	3510–Single Rack Mount Kit — this kit is used to mount a single ERS 3510GT or ERS 3510GT-PWR+ switch in a standard 19 inch rack.

ERS 3500 software features

The following software features are supported on the ERS 3500 Series Release 5.0:

- BootP or Default IP
- RADIUS password fallback
- Downloading agent & diags without reset
- Username Password enhancement
- Autosave configuration enhancements
- Ping enhancement
- Writemem and save config command
- Configurable SNMP trap port (only SNMP v1 & v2)
- SNTP & SNTP timezone enhancement
- Shutdown, reload enhancement
- Factory-default command
- Show MAC address enhancement
- Show Port enhancement
- Show Running Config (verbose, non-verbose, module) enhancement

- VLAN Tagging enhancement
- 802.1AB (LLDP) Standards Based Auto Topology
- 802.1w&s — rapid and multiple spanning trees
- 802.3ad- Link Aggregation Control Protocol (LACP)
- 802.3af — Power over Ethernet (PoE)
- 802.3at — Power over Ethernet plus (PoE+)
- COS/DSCP — allows mapping the DSCP value (carried by IP frames) to 802.1p priority value
- Rate Limiting
- Remote logging — ability to log on remote servers
- Web Quick Start
- WEB HTTP download of ASCII — allows downloading of ASCII configuration files through HTTP
- HTTP web-based management
- HTTPS/SSL secure web management
- HTTP port change
- CLI Quick Start script
- Auto save Disable
- Telnet (up to four sessions)
- Telnet out — ability to open Telnet sessions from the box
- Domain Name Service (DNS) capability
- 256 port-based VLANs with IVL — VLAN 1 is the default management VLAN
- 802.1Q tagging
- 802.1p traffic class support / remarking
- Advanced QoS (traffic classification, filtering, mark/remarking, metering, shaping)
- Avaya Automatic-QoS
- Single 802.1d Spanning Tree Protocol (STP) on all ports
- Spanning Tree port mode
- Spanning Tree 802.1d compliance mode
- Port mirroring (1–1)
- Multi-Link Trunking (MLT) with up to six trunks and four links per trunk
- MLT enable/disable whole trunk
- IGMP Multicast no flood command enhancements
- IGMPv1/v2 snooping / proxy
- IGMPv3 Snooping/proxy
- MAC address based security with autolearn (BaySecure)

- Sticky MAC
- RADIUS-based security
- TACACS+
- Local password protection
- SNMPv3 security
- SNMP-based network management
- SNMP MIB web page in EDM
- SNMP Trap list web page in EDM
- Extended IP Manager (IPv4 & IPv6)
- IPv6 Management
- IPv6 VLANs (protocol based)
- No Banner & CTRL-Y Skip
- Local console via serial interface
- 802.3x (Flow Control — Gig ports only)
- BootP/TFTP for downloading software and config file
- RMON (RFC1757): per port Statistics, History, Alarm and Events
- ASCII file configuration
- Syslog
- Dual Syslog servers
- ASCII Config Generator (ACG)
- 802.1X EAP (SHSA, MHMA, MHSA, Guest VLAN, Non-EAP & RADIUS MAC)
- 802.1X Enhancement: Dynamic VLAN assignment for NEAP & MHMA
- 802.1X Enhancement: Unicast request, Non-EAP IP Phone support
- 802.1X RFC3576 RADIUS auth extensions - CoA
- 802.1X RFC2866/2869 RADIUS interim accounting updates
- 802.1X NEAP with VLAN names
- 802.1X NEAP last assigned VLAN
- 802.1X NEAP fail-open VLAN
- 802.1X NEAP re-authentication timer
- 802.1X NEAP and Guest VLAN on same port
- RADIUS EAP / NEAP to different servers
- RADIUS Server reachability
- DA Filtering
- Port Naming

- CANA
- SSHv2
- SSH enhancement to support RSA
- Secure FTP (SFTP)
- Auto Detection And Configuration (ADAC) with 802.1AB interaction
- 802.1AB MED (Cisco IP Phones)
- 802.1AB Location TLV
- 802.1AB and ADAC interoperability
- 802.1AB Integration features
- 802.1AB Customization features
- Identify Units (Blink LEDs)
- Cumulative system uptime (hidden command)
- Virtual LACP
- Static Routing with default route
- IP Local and Non-Local static routing
- BootP/DHCP Relay
- Proxy ARP
- UDP forwarding
- DHCP Snooping
- DHCP Client
- DHCP Option 82
- Dynamic ARP Inspection
- IP Source Guard
- BDPU Filtering
- MAC flush
- Software Exception Log
- CPU & Memory Utilization
- Configure Asset ID
- Show environmental
- Show software status

Chapter 3: Introduction

This document provides information you need to configure VLANs, Spanning Tree and Multi-Link Trunking for the Ethernet Routing Switch 3500 Series.

ACLI command modes

Avaya command line interface (ACLI) provides the following configuration modes:

- User EXEC
- Privileged EXEC
- Global Configuration
- Interface Configuration Mode

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

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

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

Command mode and sample prompt	Entrance commands	Exit commands
User EXEC `3526T>`	No entrance command, default mode.	Type `exit`or `logout`
Privileged EXEC `3526T#`	From User EXEC mode, type: `enable`	Type `exit` or `logout`
Global Configuration `3526T(config)#`	From Privileged EXEC mode, type: `configure`	To return to Privileged EXEC mode, type: `end` or `exit` To exit ACLI completely, type: `logout`
Interface Configuration `3526T(config-if)#`	From Global Configuration mode: To configure a port, type: `interface`	To return to Global Configuration mode, type: `exit`

Command mode and sample prompt	Entrance commands	Exit commands

	`fastethernet <port number>`
	To configure a VLAN, type:
	`interface vlan <vlan number>`
		To return to Privileged EXEC mode, type: `end`
		To exit ACLI completely, type: `logout`

For more information about the ACLI configuration modes, see *Avaya Ethernet Routing Switch 3500 Series Fundamentals* (NN47203-102).

Chapter 4: VLAN Fundamentals

Virtual local area networks

In a traditional shared-media network, traffic that a station generates is transmitted to all other stations on the local segment. Therefore, for any given station on the shared Ethernet, the local segment is the collision domain because traffic on the segment has the potential to cause an Ethernet collision. The local segment is also the broadcast domain because any broadcast is sent to all stations on the local segment. Although Ethernet Routing Switches and bridges divide a network into smaller collision domains, they do not affect the broadcast domain.

In simple terms, a virtual local area network (VLAN) provides a mechanism to fine-tune broadcast domains. With the Ethernet Routing Switch 3500 Series , you can to create port-based and IPv6 protocolbased virtual local area networks (VLANs):

- IEEE 802.1Q port-based VLANs

  A port-based VLAN is a VLAN in which the switch ports are explicitly configured to be in the VLAN. When you create a port-based VLAN, you assign a Port VLAN Identifier (PVID) and specify which ports belong to the VLAN. The PVID is used to coordinate VLANs across multiple switches.

- IPv6 protocol-based VLANs

  A protocol-based VLAN is a VLAN in which the switch examines the protocol in use on the port. When you create a protocol-based VLAN, you assign a protocol ID for the VLAN. IPv6 recognition for segmenting IPv6 traffic is supported.

- VLAN Configuration Control

  VLAN Configuration Control (VCC) to modify VLANs. VLAN Configuration Control is a superset of the existing AutoPVID functionality and incorporates this functionality for backward compatibility. VLAN Configuration Control is globally applied to all VLANs on the switch.

For more information, see VLAN Configuration Control on page 28.

VLAN support

The Ethernet Routing Switch 3500 Series supports 256 VLANs, either by-port, under the 802.1d bridging model, or IPv6 protocol-based VLANs.

PVIDs are by port assignment. The AutoPVID option automatically assigns a PVID to all the ports. These ports are the members of the VLAN that are created.

When the Ethernet Routing Switch 3500 Series is installed for the first time, all ports are assigned to the default VLAN (PVID = 1). The default management VLAN is VLAN 1.

You can configure VLANs through the ACLI or EDM interfaces. The Ethernet Routing Switch 3500 Series supports binary and ASCII configuration files. You can also configure VLANs using both SNMP and ASCII scripts.

IEEE 802.1Q tagging

The Ethernet Routing Switch 3500 Series allows tagging by port on all ports. Tagging status applies on all ports of a Multi-Link trunk (a port member in a Multi-Link trunk cannot be configured independently of the other members in the same Multi-Link trunk). You can configure untagged frame dropping by port.

Ethernet Routing Switch 3500 Series supports the Independent VLAN Learning (IVL) model. IVL allows duplicate MAC address to be present in different sets, but not in the same set or VLAN.

IEEE 802.1Q VLAN workgroups

The Ethernet Routing Switch 3500 Series supports up to 256 VLANs and the Ethernet Routing Switch 3500 Series supports IEEE 802.1Q tagging available for each per port. Ports are grouped into broadcast domains by assigning them to the same VLAN.

Frames received in one VLAN can only be forwarded within that VLAN, and multicast frames and unknown unicast frames are flooded only to ports in the same VLAN. When you set up VLANs, you segment networks to increase network capacity and performance without changing the physical network topology. With network segmentation, each switch port connects to a segment that is a single broadcast domain.

When a switch port is configured to be a member of a VLAN, it is added to a group of ports (workgroup) that belong to one broadcast domain. You can use the Ethernet Routing Switch 3500 Series to assign ports to VLANs using the console, Telnet or an appropriate SNMP-based application. You can assign different ports (and therefore the devices attached to these ports) to different broadcast domains. This feature allows network flexibility because you can reassign VLANs to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.

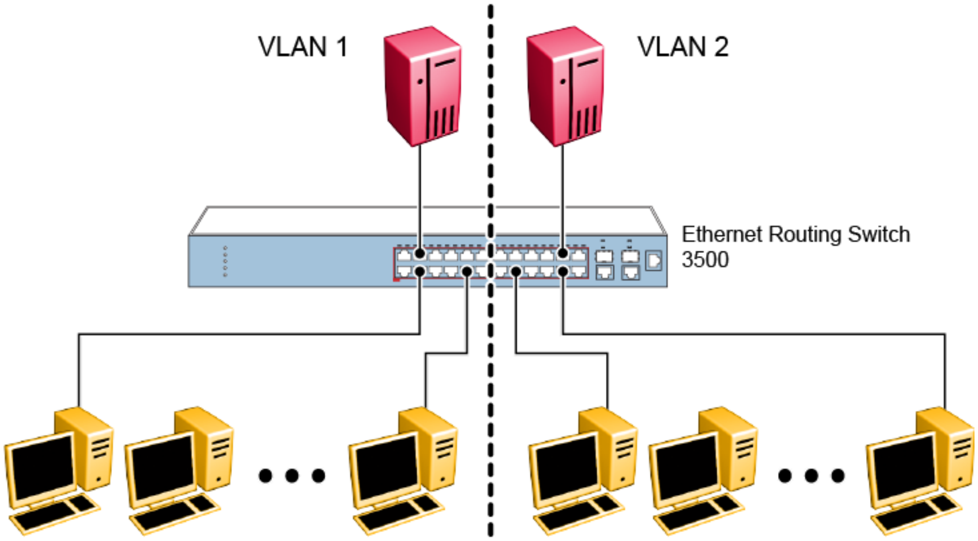

Figure 1: Port-based VLAN example

IEEE 802.1Q tagging

The Ethernet Routing Switch 3500 Series operates in accordance with the IEEE 802.1Q tagging rules. Important terms used with the 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.
- 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—the 32-bit field (VLAN tag) in the frame header that identifies the frame as belonging to a specific VLAN. Untagged frames are marked (tagged) with this classification as they leave the switch through a port that is configured as a tagged port.
- Untagged frame—a frame that does not carry any VLAN tagging information in the frame header. • VLAN port members—a set of ports that form a broadcast domain for a specific VLAN. A port can be a member of one or more VLANs.
- Untagged member—a port that is configured as an untagged member of a specific VLAN. When an untagged frame exits the switch through an untagged member port, the frame header remains unchanged. When a tagged frame exits the switch through an untagged member port, the tag is stripped and the tagged frame is changed to an untagged frame.
- Tagged member—a port that is configured as a member of a specific VLAN. When an untagged frame exits the switch through a tagged member port, the frame header is modified to include the 32-bit tag associated with the 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, and therefore has a value of 0 to 7. This field allows the tagged frame to carry the user priority across bridged LANs in which the individual LAN segments are sometimes unable to signal priority information.
- Port priority—the priority level assigned to untagged frames received on a port. This value becomes the user priority for the frame. Tagged packets get their user priority from the value contained in the 802.1Q frame header.
- Unregistered packet—a tagged frame that contains a VID where the receiving port is not a member of that VLAN.

By default, all Ethernet Routing Switch 3500 Series ports are set as untagged members of VLAN 1 with all ports configured as PVID = 1. Every VLAN is assigned a unique VID that distinguishes it from all other VLANs. In the default configuration example shown below, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID =1). Untagged packets enter and leave the switch unchanged.

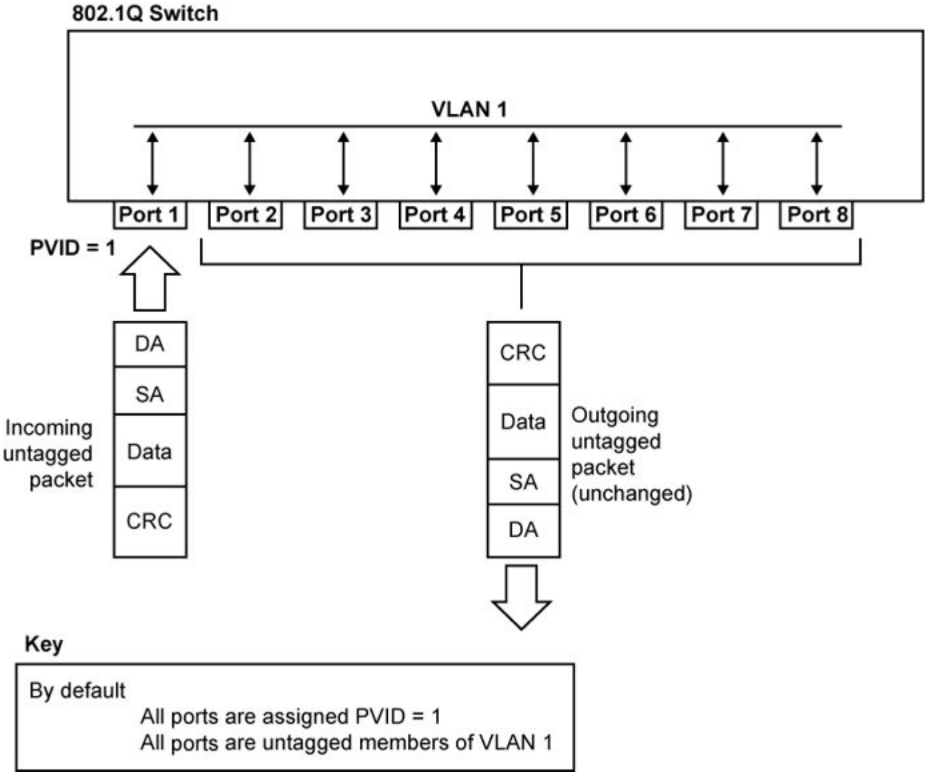

Figure 2: Default VLAN settings

When you configure VLANs, you configure the switch ports as tagged or untagged members of specific VLANs.In the figure below, untagged incoming packets are assigned directly to VLAN 2 (PVID = 2). Port 5 is configured as a tagged member of VLAN 2, and port 7 is configured as an untagged member of VLAN 2.

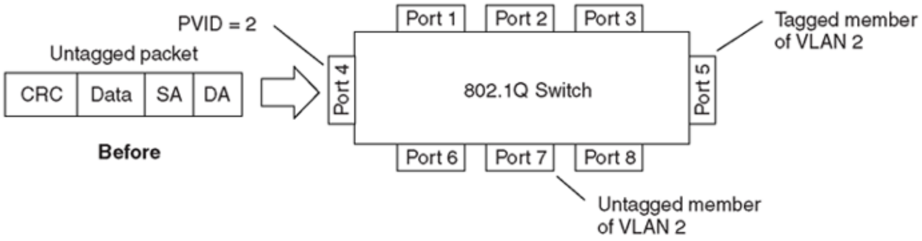

Figure 3: Port-based VLAN assignment

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

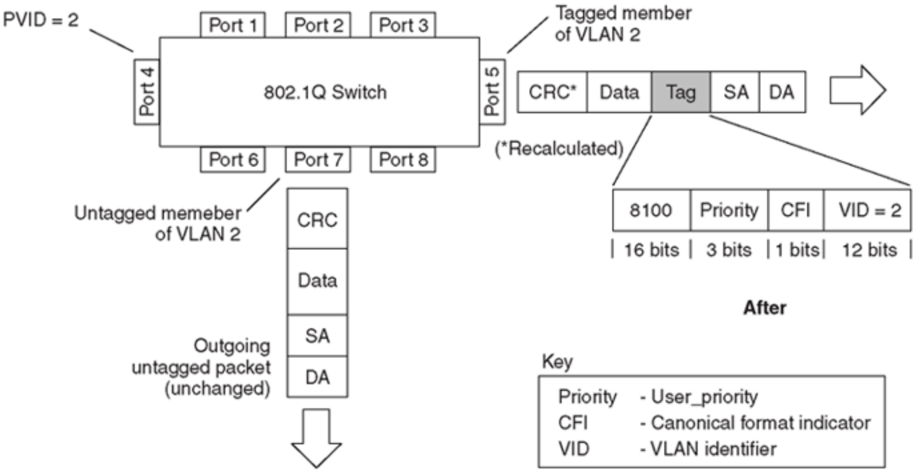

Figure 4: 802.1Q tag assignment (after port-based VLAN assignment)

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

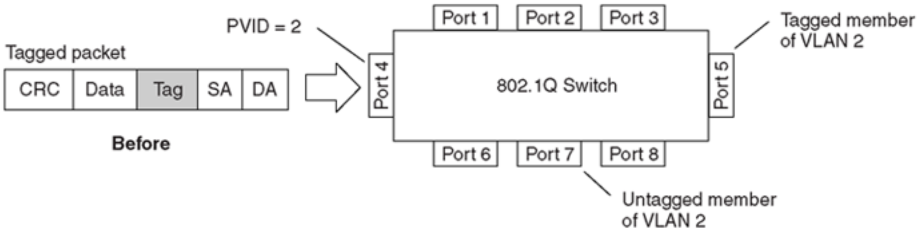

Figure 5: 802.1Q tag assignment

As shown in the figure below, the tagged packet remains unchanged as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. However, the tagged packet is stripped (untagged) as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.

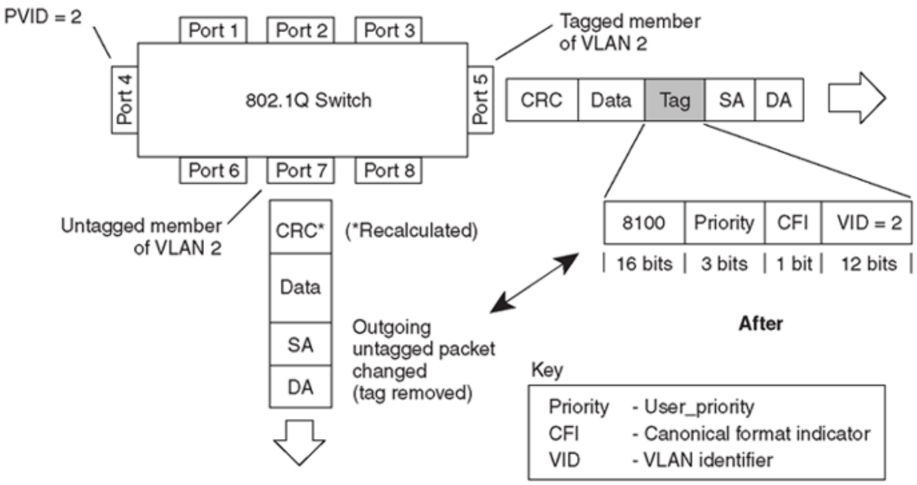

Figure 6: 802.1Q tagging (after 802.1Q tag assignment)

VLAN Tagging Enhancement

Release 5.0 or later provides additional options for VLAN port tagging. Rather than setting a port to untagged or tagged mode, you can also choose to enable or disable PVID tagging.

Following table summarizes the new tagging options:

Tagging mode	Definition	
	PVID Tagging	Non-PVID Tagging
Untag All (Untagged Access)	Disabled	Disabled
Tag All (Tagged Trunk)	Enabled	Enabled
Tag PVID Only	Enabled	Disabled
Untag PVID Only	Disabled	Enabled

VLAN Configuration Control

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

VLAN Configuration Control offers four options for controlling VLAN modification:

1. **Strict**—This option restricts the addition of an untagged port to a VLAN if the port 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 of before adding it to the new VLAN. The PVID of the port will be changed to the new VID to which it was added.

Important:

Strict is the factory default setting.

2. **Automatic**—This option automatically adds an untagged port to a new VLAN and automatically removes it from any previous VLAN membership. The PVID of the port is automatically changed to the VID of the VLAN it joins. Because the port is first added to the new VLAN and then removed from any previous membership, the Spanning Tree Group participation of the port will not be disabled as long as the VLANs involved are in the same Spanning Tree Group.
3. **AutoPVID**—This option functions in the same manner as previous AutoPVID functionality. When an untagged port is added to a new VLAN, the port is added to the new VLAN and the PVID assigned to the new VID without removing it from any previous VLAN memberships. When using this option, an untagged port has membership in multiple VLANs.
4. **Flexible**—This option functions in a similar manner to disabling AutoPVID functionality. When this option is used, there are no restrictions on the number of VLANs to which an untagged port can belong. Any new additions of an untagged port to a new VLAN does not change the PVID of that port.

VLAN Configuration Control is only applied to ports with the tagging modes of Untag All and Tag PVID Only. VLAN Configuration Control does not control 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 their PVID must be manually changed.

VLANs spanning multiple switches

You can use VLANs to segment a network within a switch. When you connect multiple switches, it is possible to connect users of one VLAN with users of the same VLAN in another switch. However, the configuration guidelines depend on whether both switches support 802.1Q tagging.

With 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 specific 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 Ethernet Routing Switch 3500 Series devices. The 802.1Q tagging is enabled on S1, port 2 and on S2, port 1 for VLAN 1 and VLAN 2. Both ports are tagged members of VLAN 1 and VLAN 2.

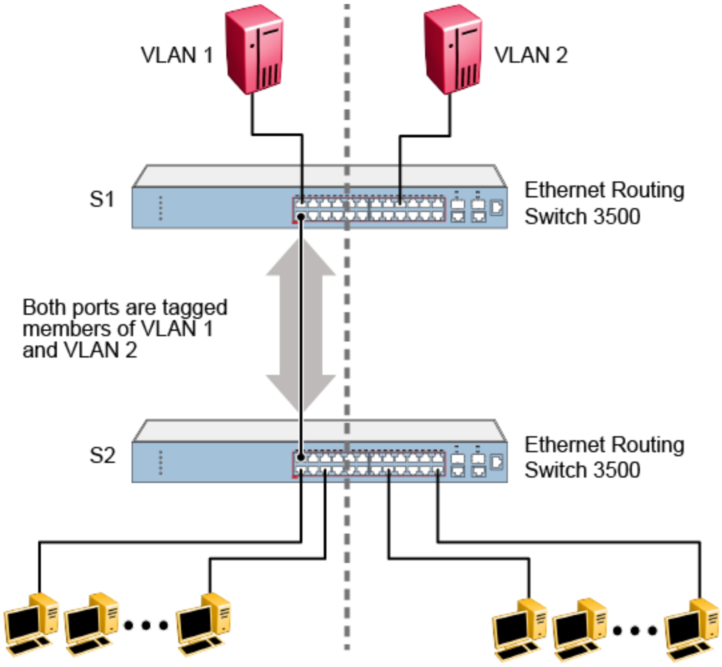
VLAN 1
VLAN 2
S1
Ethernet Routing Switch 3500
Both ports are tagged members of VLAN 1 and VLAN 2
S2
Ethernet Routing Switch 3500

Figure 7: VLANs spanning multiple 802.1Q tagged switches

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

VLANs spanning multiple untagged switches

The figure below shows VLANs spanning multiple untagged switches. In this configuration, S2 does not support 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).

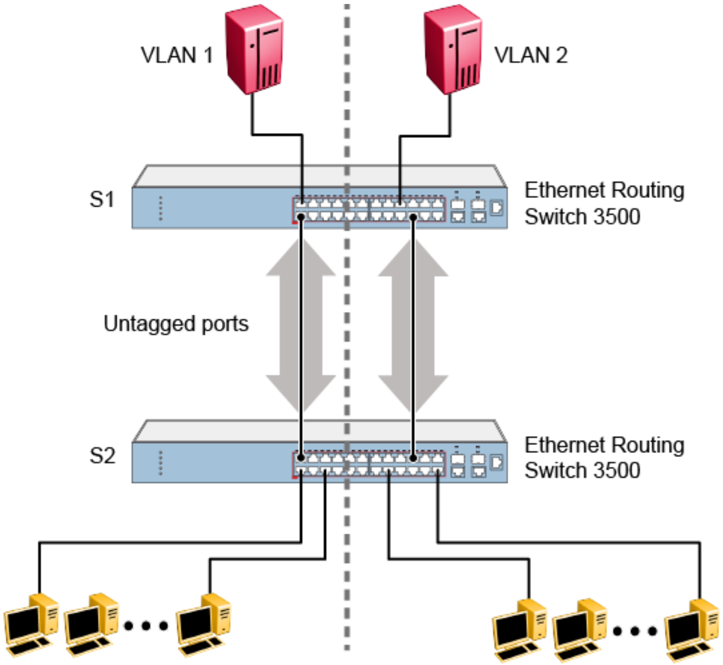

Figure 8: VLANs spanning multiple untagged switches

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

To connect multiple VLANs across switches with redundant links, you must disable the STP on all participating switch ports. The figure below shows possible consequences of enabling the STP when using VLANs between untagged (non-802.1Q tagged) switches.

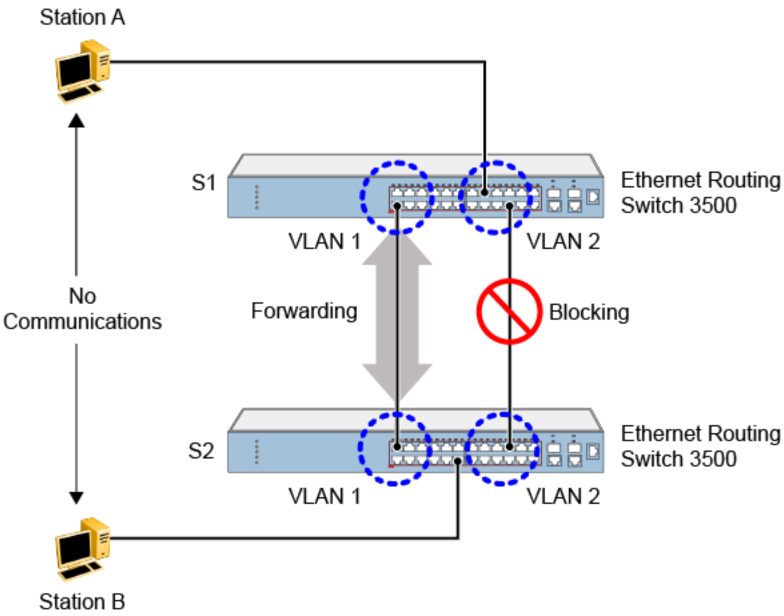

Figure 9: Possible problems with VLANs and Spanning Tree Protocol

As shown, with STP enabled, only one connection between S1 and S2 is forwarding at any time.

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

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

Shared servers

The Ethernet Routing Switch 3500 Series allows ports to exist in multiple VLANs for shared resources, such as servers, printers, and switch-to-switch connections. Resources can also exist in multiple VLANs on one switch, as shown in the figure below.

In this example, clients on different broadcast domains share resources. The broadcasts from ports configured in VLAN 3 can be seen by all VLAN port members of VLAN 3.

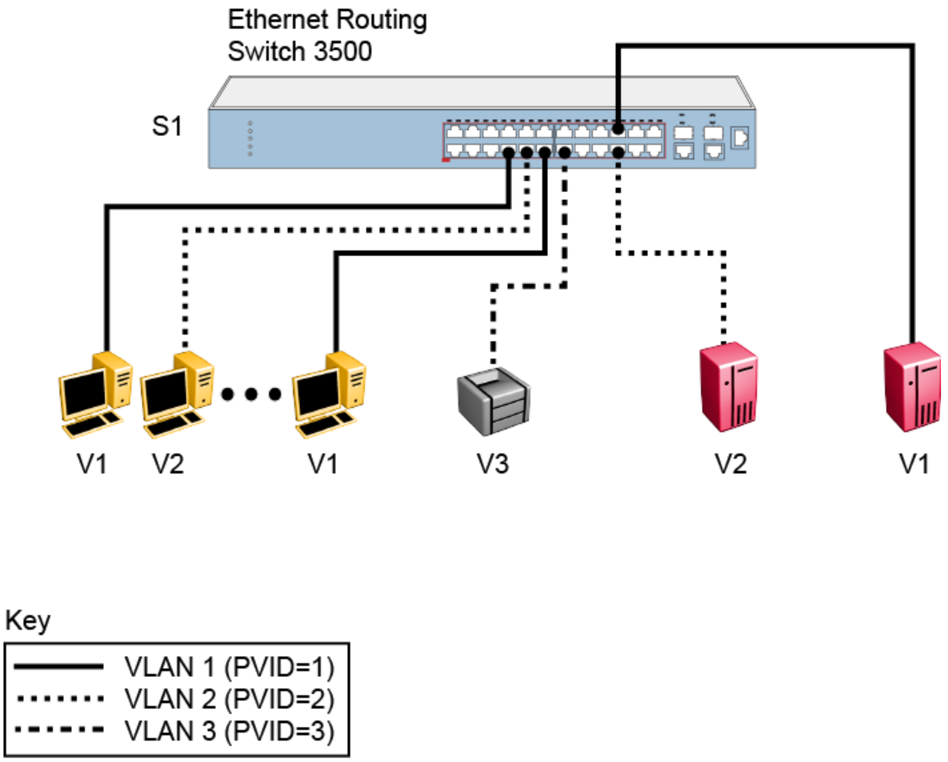

Figure 10: Multiple VLANs sharing resources

In the preceding configuration, all of the switch ports are set to participate as VLAN port members. This arrangement allows the switch to establish the appropriate broadcast domains within the switch.

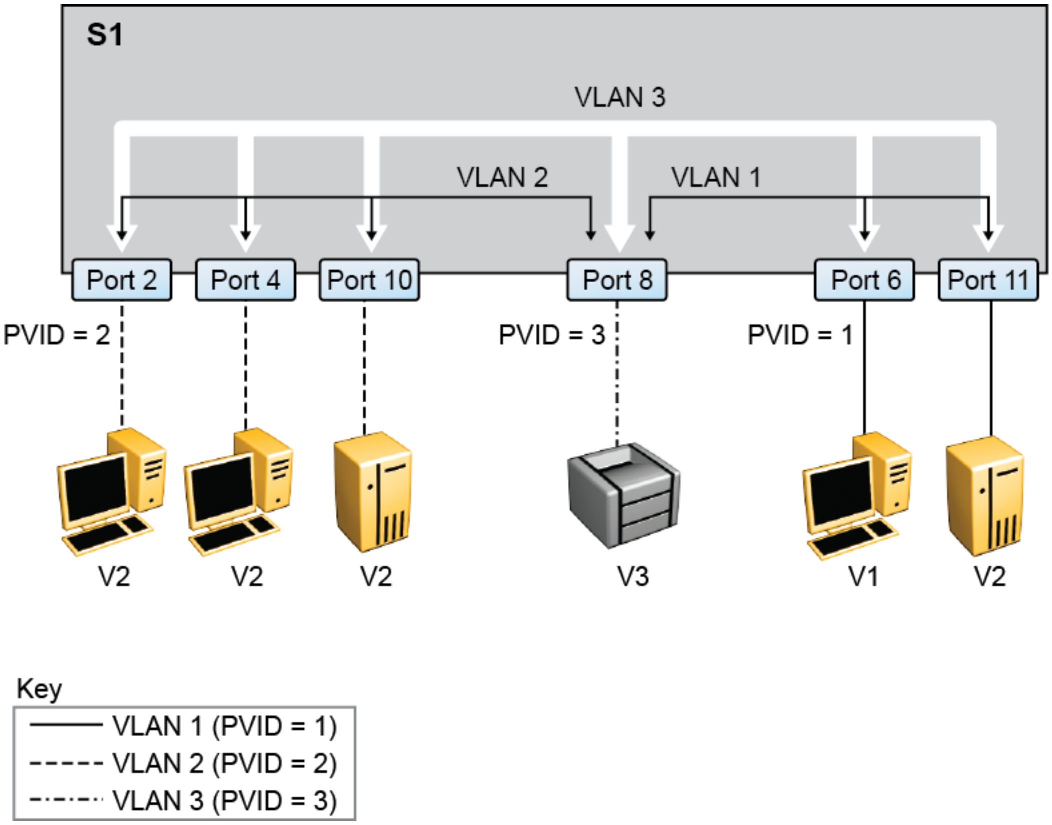

Figure 11: VLAN broadcast domains within the switch

For example, to create a broadcast domain for each VLAN, configure each VLAN with a port membership, and each port with the appropriate PVID/VLAN association:

- Ports 8, 6, and 11 are untagged members of VLAN 1.
- The PVID/VLAN association for ports 6 and 11 is: PVID = 1.
- Ports 2, 4, 10, and 8 are untagged members of VLAN 2.
- The PVID/VLAN association for ports 2, 4, and 10 is: PVID = 2.
- Ports 2, 4, 10, 8, 6, and 11 are untagged members of VLAN 3.
- The PVID/VLAN association for port 8 is: PVID = 3.

VLAN workgroup summary

This section summarizes the VLAN workgroup examples discussed in the previous sections of this chapter.

As shown in the figure below, S1 (Ethernet Routing Switch 3500 Series) is configured with multiple VLANs:

- Ports 1, 6, 11, and 12 are in VLAN 1.
- Ports 2, 3, 4, 7, and 10 are in VLAN 2.
- Port 8 is in VLAN 3.

Because S4 does not support 802.1Q tagging, a single switch port on each switch must be used for each VLAN (see 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 Ethernet Routing Switch 3500 Series devices that support 802.1Q tagging (see VLANs spanning multiple 802.1Q tagged switches on page 30).

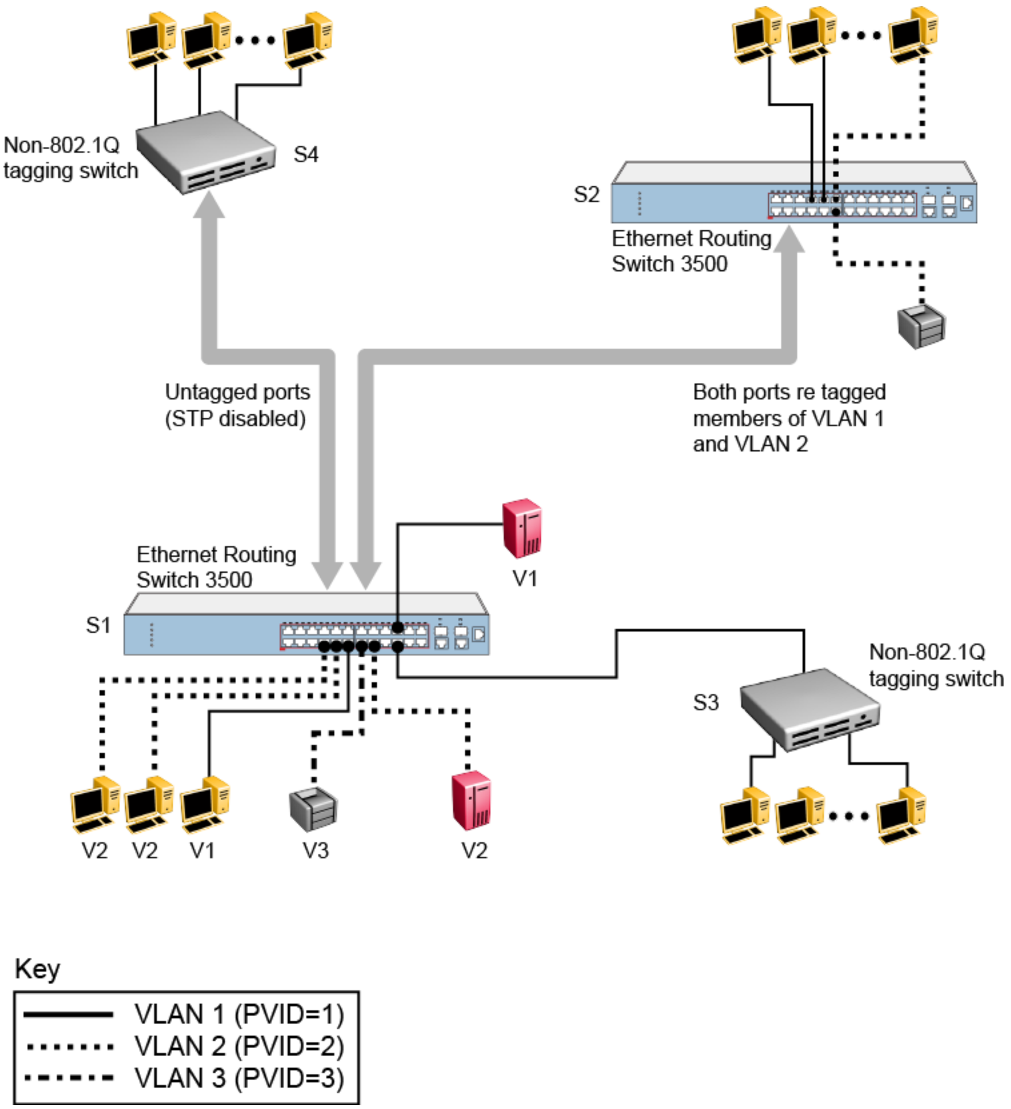

Figure 12: VLAN configuration spanning multiple switches

VLAN configuration rules

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

- If a port is a trunk group member, all trunk members are added or deleted from the VLAN.
- All ports involved in trunking and port mirroring must have the same VLAN configuration. If a port is on a trunk with a mirroring port, the VLAN configuration cannot be changed.
- Auto PVID can be activated by creating a VLAN and enabling Auto PVID for it.

MAC Flush

You can use the MAC Flush feature to clear MAC Address entries directly from the MAC Address Table (or Forwarding Data Base). 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 connection on 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 addresses in the MAC address table
- 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

MAC Flush clears only dynamically learned 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.

Chapter 5: Spanning Tree Protocol Fundamentals

The Ethernet Routing Switch 3500 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 configures the network to make another path become active, thus sustaining network operations.

Ethernet Routing Switch 3500 Series Software Release 5.0 or later supports Rapid Spanning Tree Protocol and Multiple Spanning Tree Protocol.

Spanning Tree Protocol

The Ethernet Routing Switch 3500 Series supports transparent bridging by implementing the IEEE 802.1D standard. This standard is also known as the Spanning Tree Protocol (STP) and Spanning Tree Algorithm (STA) standards. STP runs on all ports to provide automatic network configuration of a loop-free topology. You can configure redundant links to provide network fault tolerance with STP.

Port states

The port will always be in one of the five states as described in the following table:

State	Rx BPDUs	Tx BPDUs	Learn Addresses	Forward Frames
Disabled	no	no	no	no
Blocking	yes	no	no	no
Listening	yes	yes	no	no
Learning	yes	yes	yes	no
Forwarding	yes	yes	yes	yes

After a switch is powered-up or reset and the initialization process is completed, all the ports are transformed from the Disabled state to the Blocking state.

If a port is not connected, the port remains in the Forwarding state until it is connected. If you connect a station to a port, the port does not forward packets immediately. You must wait for the port to transit through the Listening and Learning states to have access to any resources located on another segment.

If you connect a hub or another bridging device to a port, it creates a loop in the network topology and a broadcast storm can occur. This problem can occur if one of the ports causing the loop is in the Forwarding state instead of the Blocking state. The loop will disappear when this port receives a superior BPDU frame.

Use the MIB variable dot1dStpPortEnable to disable or enable a port. A port is enabled by default. In this mode of operation, the port is in one of the following STP states:

- Blocking
- Listening
- Learning
- Forwarding

If you disable a port, it will not forward any frames and will not participate in the Spanning Tree Algorithm and Spanning Tree Protocol.

STP port mode

With the STP port mode feature, a switch port can maintain participation in an STP if the port is moved from one VLAN to another.

When the STP port mode is configured to auto and a port which does not belong to any VLAN is added to a VLAN, the STP participation of the port is automatically enabled. If the STP port mode is configured to normal and a port which does not belong to any VLAN is added to a VLAN, the STP participation of the port is disabled. The default STP port mode is set to auto.

STP 802.1d compliance mode

STP 802.1d compliance mode can ensure that STP conforms to the IEEE 802.1d standard. When STP 802.1d compliance mode is disabled, the switch is provided a fast recovery mechanism for a port that frequently changes state from up to down.

This fast recovery mechanism does not comply with the IEEE 802.1d standard, so when STP 802.1d compliance mode is enabled, the fast recovery mechanism is no longer available and the passing from blocking to forwarding state is done through listening and learning states. When a port link fails, the STP state of the port is Forwarding if STP 802.1d compliance mode is disabled and the STP state of the port is Disabled if STP 802.1d compliance mode is enabled.

Aging of dynamic entries in Forwarding Database

Dynamic MAC address entries are automatically removed from the Forwarding Database after a specified time.

If the network topology did not change, the aging timeout value is specified by the dot1dTpAgingTime MIB variable. This can be configured through the user interface console. The range of applicable values specified in the IEEE standard is 10 to 1000000 seconds, whereas Avaya recommends a default value 300 seconds.

If the root bridge notifies other bringing devices of topology changes, to other bridging devices, a short aging timeout value is used. The timeout value is set equal to the Forward Delay parameter contained in BPDUs originating from the root. The range of values for the Forward Delay parameter specified in the IEEE standard is 4 to 30 seconds. Avaya recommend a default value is of 15 seconds.

Port path cost

You can assign the path cost or the switch can automatically calculate the path cost associated with a port. By default the path cost is automatically calculated. Also by default, the cost of a given link is originally specified (IEEE90) to be inversely proportional to the data rate of the link. Thus, a 10 Mb/s Ethernet has a link cost of 100. This formula does not work well for Gigabit Ethernet or even for emerging technologies such as packets-over-SONET at OC-48 rates and above.

Following table describes a range of values for a given data rate, and a recommended value that has a nonlinear relationship between link cost and data rate for very high-speed LANs.

Data rate	Recommended link cost range	Recommended link cost value
10 Mb/s	50 to 600	100
100 Mb/s	10 to 60	10
1 Gb/s	3 to 10	1
10 Gb/s	1 to 5	1

The valid range for path cost values is between 0 and 65535. If you enter a value between 1 and 65535, the port path cost is set to the new value.

802.1t path cost calculation

In release 5.0 software and later, you can set the switch to calculate the STG path cost using either the IEEE 802.1d standard or the IEEE 802.1t standard. The 802.1t standard is a maintenance extension to the 802.1d standard.

Rapid Spanning Tree Protocol

The current Spanning Tree implementation in Ethernet Routing Switch 3500 Series is based on IEEE 802.1d, which is slow to respond to a topology change in the network (such as a dysfunctional link in a network). The Rapid Spanning Tree Protocol (RSTP or IEEE 802.1w) reduces the recovery time after a network breakdown. In certain configurations the RSPT recovery time is less than 1 second. It also maintains a backward compatibility with the IEEE 802.1d, which was the Spanning Tree implementation prior to RSTP. The backward compatibility can be maintained by configuring a port to be in STP compatible mode. A port operating in the STP compatible mode transmits and receives only STP BPDUs and drops any RSTP BPDUs.

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

Multiple Spanning Tree Protocol

With Multiple Spanning Tree Protocol (MSTP or IEEE 802.1s), you can 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 Ethernet Routing Switch 3500 Series use RSTP and MSTP to achieve the following:

- Reduce converging time from 30 seconds to less than 1 or 2 seconds when there is topology change in the network (such as, a port in or out of service).
- Eliminate unnecessary flushing of the MAC database and flooding of traffic to the network, using new Topology Change mechanism.
- Backward compatibility with other switches that run legacy 802.1d STP.
- Under MSTP mode, eight instances of RSTP can be supported simultaneously. Instance 0 or CIST is the default group, which includes default VLAN 1. Instances 1 to 7 are called MSTIs 1 to 7.
- You can configure the switch to run avayaStpg, RSTP, or MSTP configuration.

Interoperability with legacy STP

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

- An STP compatible port transmits and receives only STP BPDUs. Any RSTP BPDU that the port receives in this mode will be discarded.
- An RSTP compatible port transmits and receives only RSTP BPDU. If an RSTP port receives a STP BPDU it becomes an STP port. User intervention is required to bring this port back to RSTP mode. This process is called Port Protocol Migration.

Differences in port roles

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

Following table lists the differences in port roles for STP and RSTP. STP supports two port roles while RSTP supports four port roles.

Port role	STP	RSTP	Description
Root	Yes	Yes	This port is receiving a better BPDU than its own and it 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. Designated port is in Forwarding state.
Alternate	No	Yes	This port is receiving a better BPDU than its own BPDU and there is a Root port within the same switch. Alternate port is in Discarding state.
Backup	No	Yes	This port is receiving a better BPDU than its own BPDU and this BPDU is from another port within the same

Port role	STP	RSTP	Description
			switch. Backup port is in Discarding state.

Edge port

Edge port is a new parameter that RSTP supports. When you connect a port to a nonswitch device such as a PC or a workstation, you must configure it as an Edge port. An active Edge port goes directly to Forwarding state without any delay. An Edge port becomes a non-Edge port if it receives a BPDU.

Path cost values

RSTP and MSTP recommend new path cost values that support a wide range of link speeds. Following table lists the recommended path cost values.

Link speed	Recommended value

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

1 Gb/s
10 Gb/s
100 Gb/s
	20 000
	2 000
	200

1 Tb/s 10 Tb/s	20 2

Rapid convergent

In RSTP and MSTP the environment root port or the designated port can ask its peer for permission to go to the Forwarding state. If the peer agrees then the root port can move to the Forwarding state without any delay. This procedure is called negotiation process.

RSTP and MSTP also lets the switch send information received on a port immediately if the port becomes dysfunctional instead of waiting for the Maximum Age time.

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

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

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

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

Switch A is the Root.

Negotiation process

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

Switch A port 1 and switch B port 1 exchange BPDUs. Switch A is the Root and switch A port 1 is the Designated port. Switch B learns that switch A has better priority. Switch B port 1 becomes Root port. Both switch A port 1 and switch B port 1 are still in Discarding state.

Switch A starts negotiation process by sending BPDU with proposal bit set. Switch B receives the proposal BPDU and sets its non-Edge ports to Discarding state. This operation is called the synchronization process.

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

Switch A sets port 1 to Forwarding state and switch B sets port 1 to Forwarding state. PC 1 and PC 2 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.

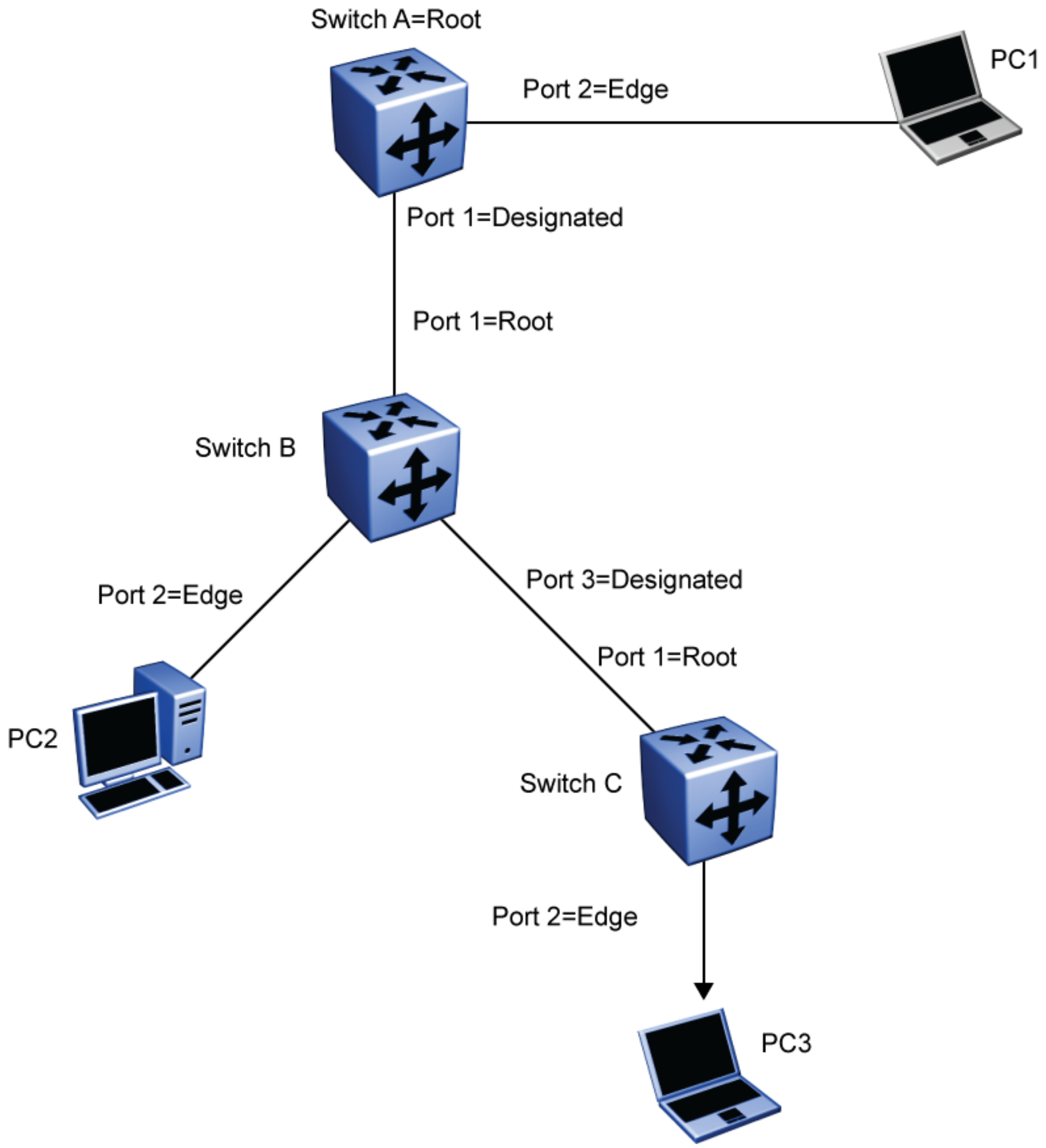

Figure 13: Negotiation process

Spanning Tree BPDU Filtering

Release 5.0 or later Software supports the BPDU-Filtering feature for STPG, RSTP, and MSTP.

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

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

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

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

Note:

The STP BPDU-Filtering feature is not supported on Multi-Link Trunk (MLT) ports. When a port has BPDU-Filtering enabled and it receives an STP BPDU, the following actions take place:

- The port is immediately put in the operational disabled state.
- A trap is generated and the following log message is written to the log: `BPDU received on port with BPDU-Filtering enabled. Port <x> has been disabled`
- The port timer starts.
- The port stays in the operational disabled state until the port timer expires.

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

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

Chapter 6: Multi-Link Trunking Fundamentals

About Multi-Link Trunking

The Multi-Link Trunking (MLT) feature is a point to point link aggregation function that allows you to group multiple switch ports together, when forming a link to another switch or server. This provides additional link redundancy and increases the aggregate throughput of the interconnection between two devices.

The Ethernet Routing Switch 3500 Series can be configured with up to six (6) Multi-Link Trunk groups, of up to four (4) links within each group. Multi-Link Trunking software detects broken trunk links and redirects traffic from the broken trunk link(s) to other trunk members within that trunk.

The MLT feature supports the grouping of ports on one switch or across multiple switches in a switch stack. This provides additional link redundancy while also building a higher bandwidth connection between two network devices, with the traffic load balanced across the physical ports in the trunk group.

Trunking can be described in the following terms:

- Network Trunk (NT) - A NT is connected to another internetworking device.
- Server Trunk (ST) - A ST is attached to a server that utilizes the same MAC address on each of its links.

The two basic switching requirements of MLTs are:

- The ability to treat multiple links as a single one for the purposes of learning and migration.
- The ability to select one of the member paths as the destination for a forwarding function without sending any duplicate packets.

MLT operation

Ethernet Routing Switch 3500 Series supports a maximum of six trunks, scaling up to four ports per trunk. The MLT operation is based on the concept of trunk groups. A trunk group is a collection of ports that represent a single link for learning, forwarding and other bridge functions.

Forwarding Model

The trunk forwarding function is based on the following:

- Destination Address (DA)
- Source Address (SA)

The forwarding model has two modes, Basic and Advanced. To select the egress link in a trunk configuration, Basic mode uses the source and destination MAC addresses of learned packets, while Advanced mode uses the source and destination IP addresses.

The formula used for forwarding traffic in Basic mode is:

A = macsa(42,40))^macsa(34,32)^macsa(26,24)^macsa(18,16)^macsa(10,8)^macsa(2,0)^macda(42,40)^macda(34,32)^macda(26,24)^macda(18,16)^macda(10,8)^macda(2,0)^vlan(10,8)^vlan(2,0)^ether_type(10,8)^ether_type(2,0)

where A mode is the number of active trunk links

macsa= MAC source address

macda= MAC destination source

The formula used for forwarding traffic in Advanced mode is:

B = sip(122,120)^sip(114,112)^sip(106,104)^sip(98,96)^sip(90,88)^sip(82,80)^sip(74,72)^sip(66,64)^sip(58,56)^sip(50,48)^sip(42,40)^sip(34,32)^sip(26,24)^sip(18,16)^sip(10,8)^sip(2,0)^tcp_src_port(10,8)^tcp _src_port(2,0)

C = dip(122,120)^dip(114,112)^dip(106,104)^dip(98,96)^dip(90,88)^dip(82,80)^dip(74,72)^dip(66,64)^dip(58,56)^dip(50,48)^dip(42,40)^dip(34,32)^dip(26,24)^dip(18,16)^dip(10,8)^dip(2,0)^tcp_dst_ port(10,8)^tcp_dst_port(2,0);

where the Forwarding link = (B ^ C) mod (the number of active trunk links)

sip = Source IP

dip= Destination IP

tcp_dst_port = TCP destination port

tcp_src_port= TCP source port

A maximum of four ports will be assigned to a trunk. The source address is associated with the trunk group rather than the individual port it was learned on. From here, the forwarding function points the packets to that particular trunk group.

For proper network operation, packets cannot be replicated to more than one port of a trunk group. The operation that creates this selection is based on the SA. SA selects one of the possible egress ports that is a member of the trunk group. For any DA, the egress path will always be defined by the SA.

Packets to a certain DA can appear on any member link of the trunk. Packets with the same SA always appear on the same egress port irrespective of DA. The exception to this is when the BCAST/MCAST/DLF traffic is sent out using the same port within the MLT regardless of the SA.

MLT configuration examples

You can use the Trunk Configuration screen to create switch-to-switch and switch-to-server Multi-Link Trunk links. The figure below shows two trunks (T1 and T2) connecting Switch S1 to switches S2 and S3.

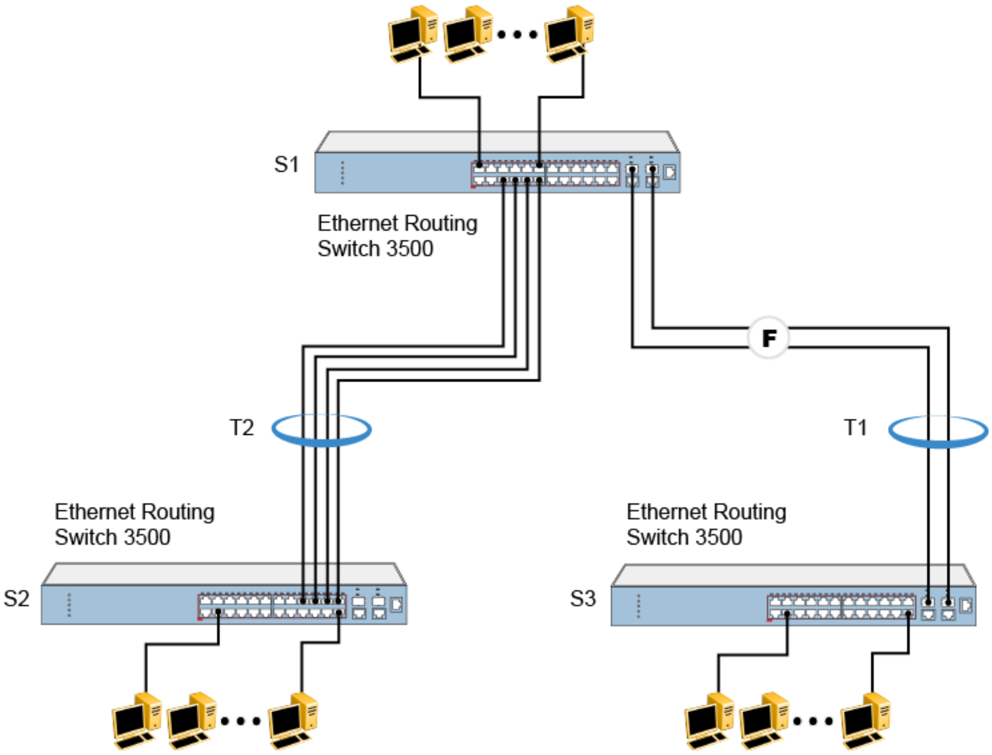

Figure 14: Switch-to-switch trunk configuration example

As shown below, you can configure each trunk with a maximum of four ports on the Ethernet Routing Switch 3500 Series to provide 400 Mb/s aggregate bandwidth through T2 or 2Gb/s aggregate bandwidth through T1, in full-duplex mode. As shown in the example, creating a Multi-Link Trunk can supply additional bandwidth required to improve the performance when the traffic between switch-to-switch connections approach single port bandwidth limitations.

The figure shows a typical switch-to-server trunk configuration. In this example, file server FS1 uses dual MAC addresses, using one MAC address for each network interface card (NIC). For this reason, FS1 does not require a trunk assignment. FS2 is a single MAC server (with a four-port NIC) and is set up as trunk configuration T1.

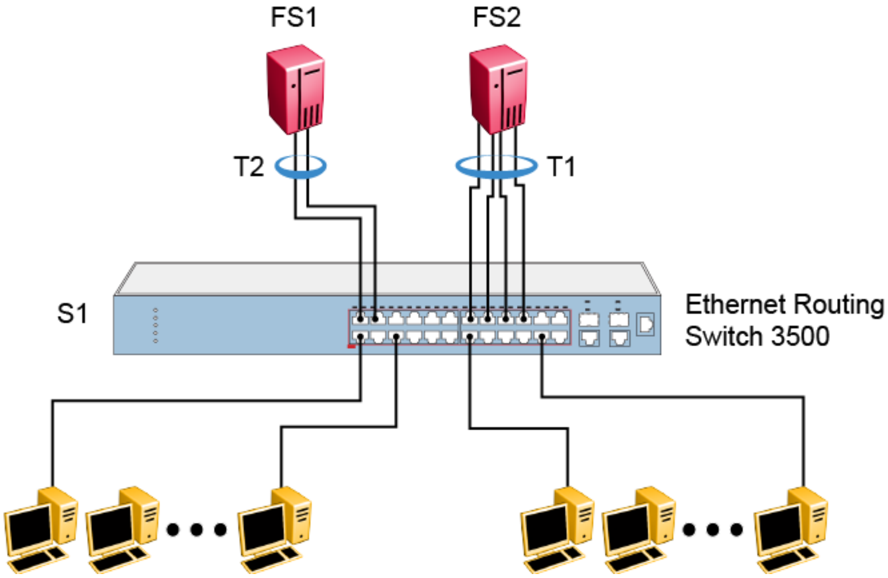

Figure 15: Switch-to-server trunk configuration example

Client server configuration using Multi-Link Trunks

The figure below shows an example of how Multi- Link Trunking can be used in a client/server configuration. In this example, both servers connect directly to Switch S1. FS2 is connected through a trunk configuration (T1). The switch-to-switch connections are through trunks (T3, T4, and T5).

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

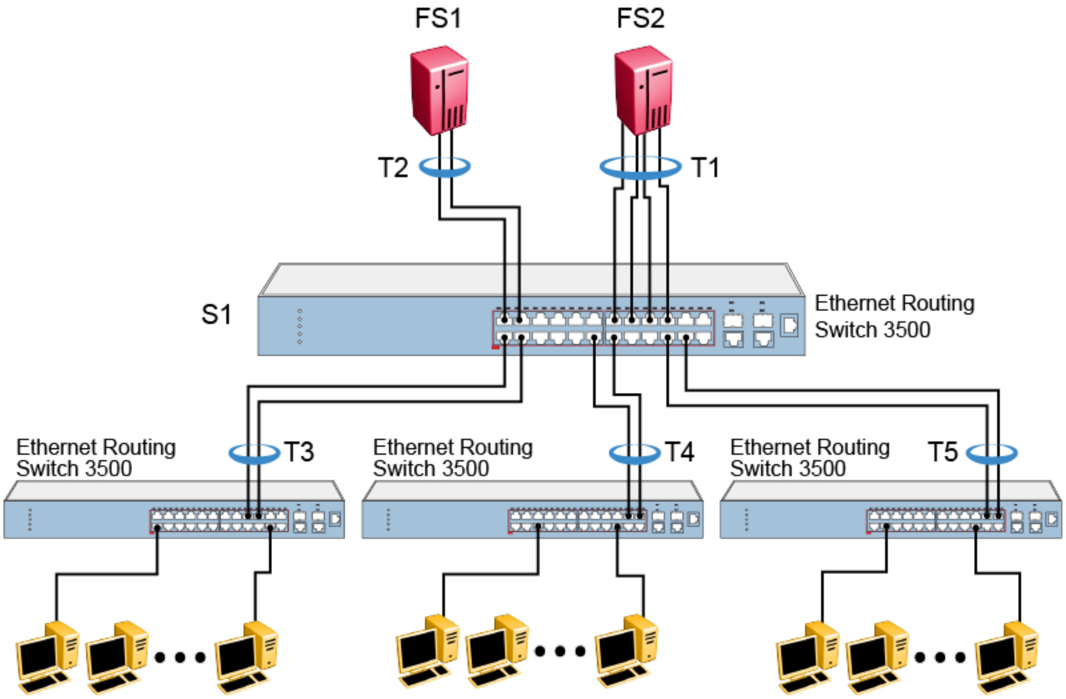
FS1
FS2
T2
T1
S1
Ethernet Routing Switch 3500
Ethernet Routing Switch 3500
T3
Ethernet Routing Switch 3500
T4
Ethernet Routing Switch 3500
T5

Figure 16: Client/server configuration example

For detailed information about configuring trunks, see Configuring a Multi-Link Trunk using ACLI on page 117 and Configuring Multi-Link Trunking using Enterprise Device Manager on page 235.

Before you configure trunks

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

Before you configure your Multi-Link Trunk, you must consider these settings, along with specific configuration rules, as follows:

1. Read the configuration rules provided in the next section, Spanning tree considerations for Multi-Link Trunks on page 54.
2. Determine which switch ports (up to four) are to become trunk members (the specific ports making up the trunk). A minimum of two ports are required for each trunk.

   Disabled ports can belong to MLTs. To enable traffic to flow to your configured MLT ports, ensure that the chosen switch ports are set to Enabled.

   Trunk member ports must have the same VLAN and VLACP configuration. LACP should not be enabled on the selected trunk ports.
3. All network cabling should be complete and stable before configuring any trunks, to avoid configuration errors.

4. Consider how the existing spanning tree reacts to the new trunk configuration (see Spanning tree considerations for Multi-Link Trunks on page 54).
5. Consider how existing VLANs are affected by the addition of a trunk.

Spanning tree considerations for Multi-Link Trunks

The spanning tree Path Cost parameter is recalculated based on the aggregate bandwidth of the trunk. For example, the figure below shows a 4–port trunk (T1) with two port members operating at 100 Mb/s and two at 10 Mb/s. Trunk T1 provides an aggregate bandwidth of 220 Mb/s. The Path Cost for T1 is 4 (Path Cost = 1000/ LAN speed, in Mb/s). Another three-port trunk (T2) is configured with an aggregate bandwidth of 210 Mb/s, with a comparable Path Cost of 4. When the path cost calculation for both trunks is equal, the spanning tree software chooses the trunk with the lowest Spanning Tree PortID, regardless of the aggregate bandwidth.

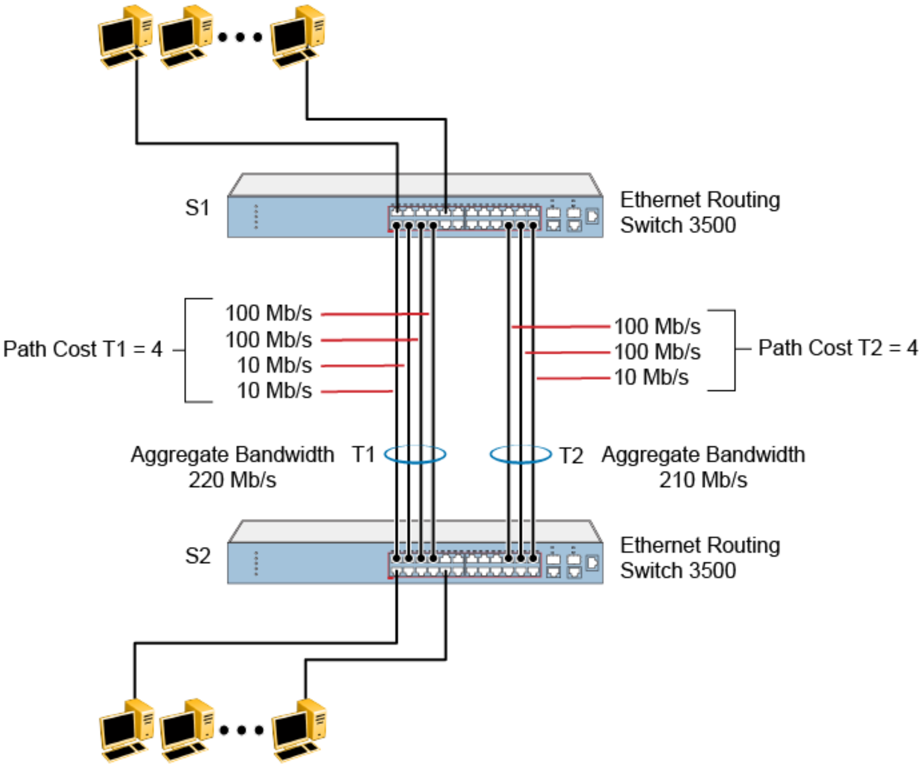
S1
Ethernet Routing Switch 3500
Path Cost T1 = 4
100 Mb/s
100 Mb/s
10 Mb/s
10 Mb/s
100 Mb/s
100 Mb/s
10 Mb/s
Path Cost T2 = 4
Aggregate Bandwidth 220 Mb/s
T1
T2
Aggregate Bandwidth 210 Mb/s
S2
Ethernet Routing Switch 3500

Figure 17: Path Cost arbitration example

Additional tips about the Multi-Link Trunking feature

When you create a Multi-Link 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.

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

Important:

At boot time, the agent verifies the setting consistency for various applications (like Rate Limiting, EAP, and Port Mirroring) on the MLT ports. MLT is disabled if they are inconsistent.

MLT enable or disable whole trunk

The MLT enable or disable whole trunk feature is user configurable and can be enabled or disabled switch-wide with a single CLI command. The feature is disabled by default. With the MLT whole trunk disabled, you can enable or disable MLT or DMLT groups, and the operational states of the bundled links do not change. In this configuration, a network traffic loop can occur when you disable MLT or DMLT groups that have Spanning-Tree disabled on the trunk links. The switch supports the ability to change this operational mode using the MLT whole trunk feature.

If you enable the MLT whole trunk feature, the underlying state of the port changes to reflect the state of the MLT or DMLT bundle regardless of the previous status. With the MLT whole trunk enabled, you can disable the MLT or DMLT and all links that are part of the MLT group are disabled except for the Default Forwarding Link (DFL), which remains active to prevent loss of connectivity to the switch or stack. The DFL link is typically the lowest numbered port of an active MLT or DMLT link. Conversly, if you enable the MLT or DMLT, all links will become active.

You can enable or disable individual links of a MLT or DMLT if the MLT whole trunk feature is enabled.

Important:

For network configuration, Avaya recommends that you enable the MLT whole trunk feature.

Chapter 7: LACP And VLACP Fundamentals

IEEE 802.3ad Link Aggregation

You can create and manage a trunk group with Link Aggregation (LA) . You can control and configure a trunk group automatically using the Link Aggregation Control Protocol (LACP).

The LACP, defined by the IEEE 802.1ax standard, allows the switch to learn the presence and capabilities of a remote switch by exchanging information with the remote switch before a trunk group is formed. Either switch can accept or reject the aggregation request with the far end on a per port basis. A link that can not join a trunk group operates as an individual link. 802.1ax provides an industry standard method for bundling multiple links together to form a single trunk between two networking devices. Trunks that conform to the 802.1ax standard are Link Aggregation Groups (LAGs). Release 5.0 or later software supports 2 types of trunks:

- Dynamic LAG
- MLT

A trunk group that is formed by Link Aggregation is called a Link Aggregation group (LAG), and a trunk group that is formed by Ethernet Multi-link Trunking is called a Multi-link trunk (MLT) group.

The Ethernet Routing Switch 3500 Series supports both Link Aggregation groups and Multilink trunks. By default, Link Aggregation is set to disabled on all ports. A Link Aggregation group or trunk group can be created or deleted automatically using Link Aggregation Control Protocol (LACP).

The maximum number of Link Aggregation and MLT groups is six, and the maximum number of active links per group is four. Link Aggregation allows more than four links to be configured in one Link Aggregation group (LAG).

The first four high priority links are active links and together they form a trunk group. The remaining low priority links remain in standby mode. When one of the active links goes down, one of the standby links becomes active and is added to the trunk group.

The failover process is as follows:

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

Important:

The STP participation for an active MLT or LAG trunk always overrides the STP participation previously configured for individual ports. If a user changes the STP participation on individual trunk ports after the trunk is disabled, the port STP participation will be overridden by the Trunk's STP participation after the trunk is enabled again.

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

Half duplex links are not allowed in LAG, and all links in a LAG must have the same speed.

802.3 Link Aggregation is available through the Avaya Command Line Interface (ACLI). The ACLI supports the following commands:

The following ACLI commands can be executed to enable, disable, or set default values for LACP on a port:

- `lacp aggregation [port <portlist>] enable`
- `no lacp aggregation [port <portlist>] enable`
- `default lacp aggregation [port <portlist>] enable`

To specify the LACP mode:

- `lacp mode [port <portlist>] {off | passive | active}`
- `default lacp mode [port <portlist>]`

To assign an administrative key value to a port:

```
lacp key [port <portlist>] <1–4095>
```

To specify the port priority:

- `lacp priority [port <portlist>] <0–255>`
- `default lacp priority [port <portlist>]`

To set port time-out:

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

To set LACP system priority:

- `lacp system-priority [0-65535]`
- `default lacp system-priority`

ACLI Show commands for LACP:

- `show lacp aggr`
- `show lacp port[<portlist>]`

- `show lacp port aggr <1–65535>`
- `show lacp debug member [portlist]`
- `show lacp system`
- `show lacp stats [port <portlist>]`
- `show lacp stats aggr <1–65535>`
- `lacp clear-stats` (available in Interface Configuration mode)

For more information about the syntax and parameters of the ACLI commands, see Configuring Link Aggregation Group using ACLI on page 120.

VLACP

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

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

Virtual LACP (VLACP) overview

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

Enterprise networks can connect their aggregated Ethernet trunk groups through a service provider network connection (for example, through a VPN), but far-end failures cannot be signaled with Ethernet-based functions that operate end-to-end through a service provider cloud.

In the following example, the MLT (between Enterprise switches S1 and S2) extends through the service provider (SP) network.

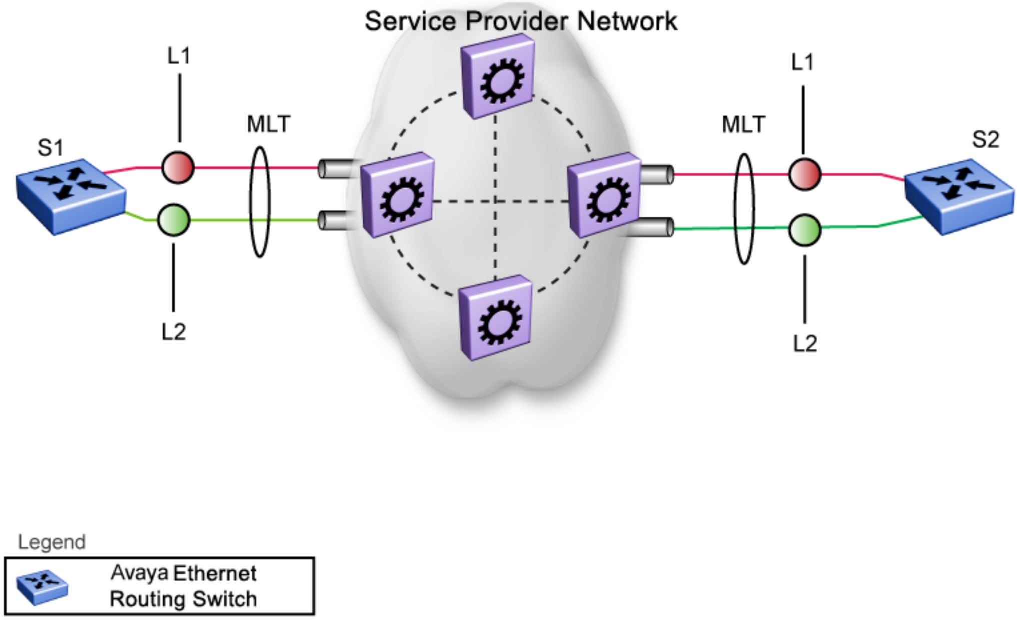

Figure 18: MLT extended through the service provider network

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

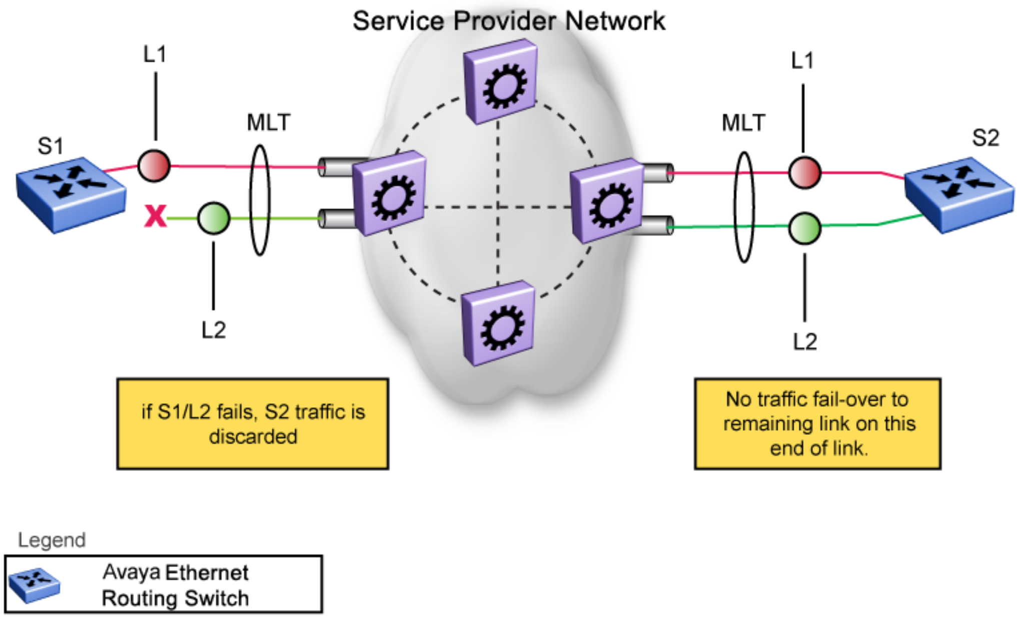
Service Provider Network
L1
MLT
S1
X
L2
L1
MLT
S2
L2
if S1/L2 fails, S2 traffic is discarded
No traffic fail-over to remaining link on this end of link.
Legend
Avaya Ethernet Routing Switch

Figure 19: Link-down failure

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 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.

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 after the port is unblocked)

Chapter 8: ADAC Fundamentals

Ethernet Routing Switch 3500 Series supports the Auto-Detection and Auto-Configuration (ADAC) of Avaya IP Phones. With ADAC, you can automatically configure the switch to support and prioritize IP Phone traffic.

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

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

> **Note:**
>
> Because the ERS 3500 switches have limited QoS resources, the ADAC implementation differs from the other Ethernet Routing Switch platforms. It is necessary to free up some QoS resources in order for ADAC to apply the configuration on ports. For more information, see *Avaya Ethernet Routing Switch 3500 Series-Configuration — Quality of Service*, NN47203–503.

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

- **Untagged-Frames-Basic**:

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

- **Untagged-Frames-Advanced**:

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

- **Tagged Frames**:

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

ADAC operation

The following sections provide detailed explanations of ADAC operation.

Auto-Detection of Avaya IP Phones

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

When you enable auto-detection on a port, the port also becomes operationally enabled. Similarly, after 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 auto-configuration will also be removed. To put the port back into the operational state, disable and then re-enable 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 either before enabling auto-detection on the port, or if ADAC is globally disabled

The two methods of auto-detection are by MAC address or using LLDP (IEEE 802.1AB).

Auto-detection by MAC address is based on using predefined MAC addresses to determine that the specified port is connected to a Avaya IP phone. For more information and the list of defined MAC address ranges, see Auto-Detection by MAC address on page 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 a Avaya IP Phone and initiates the required configuration. ADAC is supported for a maximum of 32 devices per port, but in most cases, there will be only one IP phone and one PC on each port.

Following table shows a list of the default 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

Lower End	Higher End
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 the ACLI or EDM.

ADAC checks a MAC address against the supported ranges only after 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.

ADAC and 802.1AB interoperability

With ADAC and 802.1AB interoperability, an IP phone configured with Avaya automatic QoS can update phone 802.1q priority and DSCP values based on Network Policy 802.1AB TLV values sent by the switch on an ADAC telephony port. The LLDP compliant IP phone then uses the received DSCP when sending voice traffic. Avaya Automatic QoS recognizes and prioritizes the traffic accordingly.

ADAC and 802.1AB interoperability is automatically enabled when Avaya automatic QoS, ADAC, and LLDP Network Policy TLV are enabled.

Note:

Because the ERS 3500 switches do not support user-configurable LLDP-MED network policies, LLDP implementation differs from the other Ethernet Routing Switch platforms. At LLDP default, the ERS 3500 switches tag voice traffic with a VID of ADAC Voice-VLAN ID instead of a VID of 0 (priority-tagged frames).

Auto-Configuration of Avaya IP Phones

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

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

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

The ports are polled every two seconds for their auto-configuration state and to see whether or not auto-configuration should be applied based on the current ADAC settings, both the global setting and the port setting. Auto-configuration will be applied on the port after 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-detection 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.

Chapter 9: Link Layer Discovery Protocol fundamentals

Release 5.0 or later supports the Link Layer Discovery Protocol (LLDP) (IEEE 802.1AB), which lets stations connected to a LAN to advertise their capabilities to each other, enabling the discovery of physical topology information for network management. LLDP-compatible stations can consist of any interconnection device including PCs, IP Phones, switches, and routers. Each LLDP station stores LLDP information in a standard Management Information Base (MIB), making it possible for the information to be accessed by a network management system (NMS) or application.

Each LLDP station:

- advertises connectivity and management information about the local station to adjacent stations on the same 802 LAN (802.3 Ethernet with Ethernet Routing Switch 3500)
- receives network management information from adjacent stations on the same LAN

LLDP makes it possible to discover certain configuration inconsistencies or malfunctions that can result in impaired communications at higher layers. For example, it can be used to discover duplex mismatches between an IP Phone and the connected switch.

LLDP is compatible with IETF PROTO MIB (IETF RFC 2922).

The following figure shows an example of how LLDP works in a network.

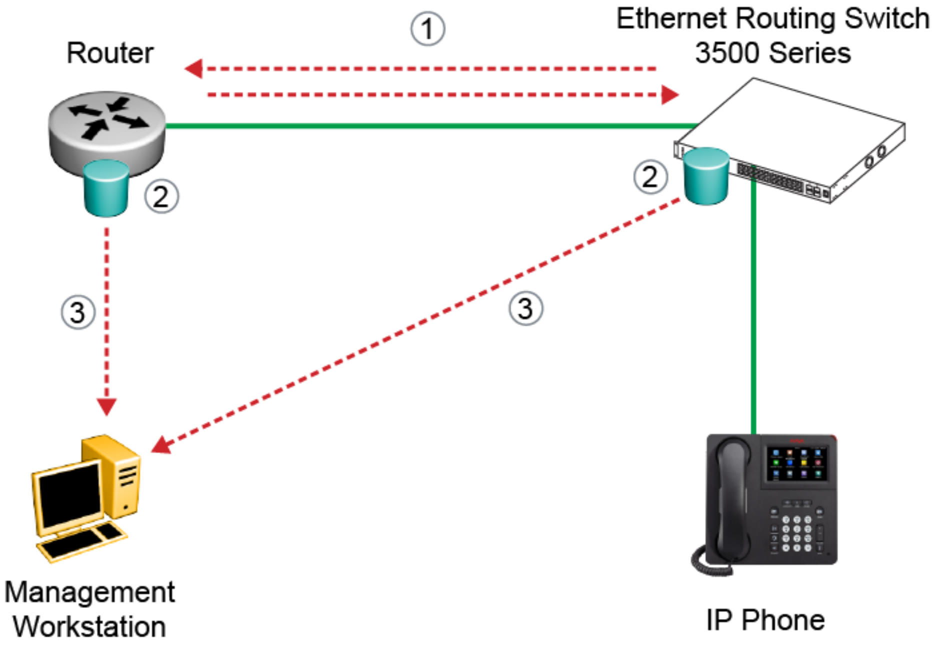

Figure 20: How LLDP works

1. The Ethernet Routing Switch and router advertise chassis or port IDs and system descriptions to each other.
2. The devices store the information about each other in local MIB databases, accessible using SNMP.
3. A network management system retrieves the data stored by each device and builds a network topology map.

LLDP operational modes

LLDP is a one-way protocol. An LLDP agent can transmit information about the capabilities and current status of the system associated with its MAC service access point (MSAP) identifier. The LLDP agent can also receive information about the capabilities and current status of the system associated with a remote MSAP identifier. However, LLDP agents cannot solicit information from each other.

You can set the local LLDP agent to transmit only, receive only, or to both transmit and receive LLDP information. You can configure the state for LLDP reception and transmission using SNMP or ACLI commands.

Connectivity and management information

The information fields in each LLDP frame are in a Link Layer Discovery Protocol Data Unit (LLDPDU) as a sequence of short, variable length, information elements known as type, length, value (TLV). Each LLDPDU includes the following four mandatory TLVs:

- chassis ID TLV
- port ID TLV
- Time to Live TLV
- End Of LLDPDU TLV

The chassis ID and the port ID values are concatenated to form a logical MSAP identifier that is used by the recipient to identify the sending LLDP agent and port.

A non-zero value in the Time to Live (TTL) field of the TTL TLV indicates to the receiving LLDP agent how long the LLDPDU information from the MSAP identifier remains valid. All LLDPDU information is automatically discarded by the receiving LLDP agent if the sender fails to update it in a timely manner. A zero value in TTL field of Time To Live TLV tells the receiving LLDP agent to discard the information associated with the LLDPDU MSAP identifier.

Beginning with Release 5.0, in addition to the four mandatory TLVs, the switch supports the basic management TLV set. You can specify which of these optional TLVs to include in the transmitted LLDPDUs for each port.

Basic management TLV set

The basic management TLV set contains the following TLVs:

- Port Description TLV
- System Name TLV
- System Description TLV
- System Capabilities TLV (indicates both the system supported capabilities and enabled capabilities, such as end station, bridge, or router)
- Management Address TLV

Beginning with Release 5.0 the switch supports IPv4 and IPv6 management addresses and the transmission of all TLVs from the basic management TLV set is enabled by default.

IEEE 802.1 organizationally-specific TLVs

The optional IEEE 802.1 organizationally-specific TLVs are:

- **Port VLAN ID TLV** contains the local port PVID
- **Port and Protocol VLAN ID TLV** contains the VLAN IDs of the port and protocol VLANs that contain the local port
- **VLAN Name TLV** contains the VLAN names of the VLANs that contain the local port
- **Protocol Identity TLV** advertises the protocol supported. The following values are used for supported protocols on the 3500 Series:
  - stp protocol [0x00, 0x26, —x42, 0x03, 0x00,0x00, 0x00}
  - Rstp protocol string {0x00, 0x27, 0xx42, 0x42, 0x03, 0x00, 0x00, 0x02}
  - Mstp protocol string {0x00, 0x69, 0x42, 0x42, 0x03, 0x00, 0x00, 0x03}
  - Eap protocol string {0x88, 0x8E, 0x01}
  - Lldp protocol string {0x88, 0xCC}

IEEE 802.3 organizationally-specific TLVs

The optional IEEE 802.3 organizationally-specific TLVs are:

- **MAC/PHY Configuration/Status TLV** indicates the autonegotiation capability and the speed and duplex status of IEEE 802.3 media access control (MAC)/physical (PHY)s
- **Power-Via-MDI (media dependent interface) TLV** indicates the capabilities and current status of IEEE 802.3 physical media dependents (PMDs) that either require or can provide power over twisted-pair copper links
- **Link Aggregation TLV** indicates the current link aggregation status of IEEE 802.3 MACs
- **Maximum Frame Size TLV** indicates the maximum supported 802.3 frame size

Organizationally-specific TLVs for MED devices

The optional organizationally-specific TLVs for use by Media Endpoint Devices (MED) and MED network connectivity devices are:

- Capabilities TLV enables a network element to advertise the LLDP-MED TLVs it is capable of supporting.
- Network Policy Discovery TLV is a fixed length TLV that enables both network connectivity devices and endpoints to advertise VLAN type, VLAN identifier (VID), and Layer 2 and Layer 3 priorities associated with a specific set of applications on a port. In addition, an LLDP-MED endpoint advertises this TLV for supported application types to enable the discovery of specific policy information and the diagnosis of network policy configuration mismatch issues.
- Location Identification TLV allows network connectivity devices to advertise the appropriate location identifier information for an endpoint to use in the context of locationbased applications. The Location Identification Discovery extension enables the advertisement of location identifier information to Communication Endpoint Devices (Class III), based on the configuration of the Network Connectivity Device to which it is connected. This is expected to be related to wiremap or similar network topology data, such that the configuration of the Network Connectivity Device can uniquely identify the physical location of the connected MED Endpoint, and hence the correct location identifier information for it to use.
- Extended Power-via-MDI TLV enables advanced power management between an LLDPMED endpoint and network connectivity devices. The Extended Power-via-MDI TLV enables the advertisement of fine grained power requirement details, endpoint power priority, and power status for both endpoint and network connectivity devices.
- Inventory TLVs are important in managed Voice over Internet Protocol (VoIP) networks. Administrative tasks in these networks are made easier by access to inventory information about VoIP entities. The LLDP Inventory TLVs consist of the following:
    - LLDP-MED Hardware Revision TLV allows the device to advertise its hardware revision.
    - LLDP-MED Firmware Revision TLV allows the device to advertise its firmware revision.

- LLDP-MED Software Revision TLV allows the device to advertise its software revision.
- LLDP-MED Serial Number TLV allows the device to advertise its serial number.
- LLDP-MED Manufacturer Name TLV allows the device to advertise the name of its manufacturer.
- LLDP-MED Model Name TLV allows the device to advertise its model name.
- LLDP-MED Asset ID TLV allows the device to advertise its asset ID.

Transmitting LLDPDUs

When a transmit cycle is initiated, the LLDP manager extracts the managed objects from the LLDP local system MIB and formats this information into TLVs. TLVs are inserted into the LLDPDU.

LLDPDU are regularly transmitted at a user-configurable transmit interval (tx-interval) or when variables in the LLPDU are modified on the local system (such as system name or management address).

Tx-delay is the minimum delay between successive LLDP frame transmissions.

TLV system MIBs

The LLDP local system MIB stores the information for constructing the various TLVs to be sent. The LLDP remote systems MIB stores the information received from remote LLDP agents.

LLDPDU and TLV error handling

LLDPDUs and TLVs that contain detectable errors are discarded. TLVs that are not recognized, but that also contain no basic format errors, are assumed to be validated and are stored for possible later retrieval by network management.

Configuring LLDP with ACLI

See Configuring LLDP using ACLI on page 145 for information about configuring LLDP with ACLI .

802.1AB integration

802.1AB integration provides a set of LLDP TLVs for Avaya IP telephone support.

You can select which Avaya IP phone support TLVs can be transmitted from individual switch ports by enabling or disabling TLV transmit flags for the port. The TLV transmit flags and TLV configuration operate independently of each other. Therefore, you must enable the transmit flag on a switch port for a specific TLV, before the port can transmit that TLV to an Avaya IP phone.

A switch port does not transmit Avaya IP phone support TLVs unless the port detects a connected Avaya IP phone.

PoE conservation level request TLV

With the PoE conservation level request TLV, you can configure the switch to request that an Avaya IP phone, connected to a switch port, operate at a specific power conservation level. The requested conservation level value for the switch can range from 0 to 255, but the Avaya IP Phone supports only 243 levels. If you request a power conservation level higher than 243, the Avaya IP phone reverts to its maximum power conservation level. If you select a value of 0 for the PoE conservation level request, the switch does not request a power conservation level for an Avaya IP phone.

If you set the PoE conservation level request TLV on a port and you enable energy-saver for the port, the TLV value is temporarily modified for maximum power savings by the switch. When you disable energy-saver for the port, the switch automatically restores the power conservation level request TLV to the previous value.

If you set the PoE conservation level on a port while AES is active on the port and the maximum PoE Conservation level for the switch is 255, the switch replaces the PoE conservation level stored for AES restoration with the new value you set for the port.

By default, the transmission of PoE conservation level request TLV is enabled on all PoE capable switch ports.

You can only configure the PoE conservation level request TLV on switches that support PoE.

PoE conservation level support TLV

With the PoE conservation level support TLV, an Avaya IP phone transmits information about current power save level, typical power consumption, maximum power consumption, and power conservation level of the IP phone, to a switch port.

Call server TLV

With the call server TLV, you can configure the switch to advertise the IP addresses of a maximum of 8 call servers to connected Avaya IP phones. Avaya IP phones use the IP address information to connect to a call server.

Avaya IP phones use the call server TLV to report which call server it is connected to back to the switch.

The call server TLV supports IPv4 addresses only.

By default, the transmission of the call server TLV is enabled for all ports.

File server TLV

With the file server TLV, you can configure the switch to advertise the IP addresses of a maximum of 4 file servers to connected Avaya IP phones. Avaya IP phones use the IP address information to connect to a file server.

Avaya IP phones use the call server TLV to report which file server it is connected to back to the switch.

The file server TLV supports IPv4 addresses only.

By default, the transmission of the file server TLV is enabled for all ports on switches.

> **Note:**
>
> If your Avaya IP Handset uses SIP, 802.1AB (LLDP) TLVs do not provide all information for the IP Phone. You must specify a fileserver IP address TLV so the IP phone can download the SIP configuration information, because the IP Phone retrieves information related to the SIP domain, port number and transport protocol from the file server.

802.1Q framing TLV

With the 802.1Q framing TLV, you can configure the switch to exchange Layer 2 priority tagging information with Avaya IP phones.

Because the 802.1Q framing TLV operates as an extension of the LLDP Network Policy TLV, you must enable the LLDP MED Capabilities and LLDP MED Network Policy TLVs for the 802.1Q framing TLV to function.

By default, the transmission of the 802.1Q framing TLV is enabled for all ports on switches.

Phone IP TLV

Avaya IP phones use the phone IP TLV to advertise IP phone IP address configuration information to the switch.

The phone IP TLV supports IPv4 addresses only.

802.1AB customization

802.1AB, Link Layer Discovery Protocol (LLDP) customization expands LLDP capabilities so that you can customize all of the LLDP advertisements and timers. The enhanced flexibility provided by the additional customization makes LLDP suitable for deployments where a variety of vendor equipment or deployment methods exist.

You can customize the following Type, Length, and Value (TLV) elements for your deployment needs:

- System TLV
- Port Description TLV
- System Name TLV
- System Description TLV
- System Capability TLV
- Management Address TLV
- LLDP MED Capabilities TLV
- Network Policy TLV
- Location Identification TLV
- Extended Power-via-MDI TLV and Inventory TLV

You can also configure the following timers:

- Reinitialization Delay
- Transmit Delay
- Transmit Interval
- Transmit Multiplier Value
- Transmit Hold
- Fast Start Timers
- SNMP Notification Interval

Autotopology

You can enable the Optivity* Autotopology* protocol on the Ethernet Routing Switch 3500 Series with ACLI. For more information about Autopology, go to the Avaya support site. (The product family for Optivity and Autotopology is Data and Internet.)

Autotopology is enabled by default.

Chapter 10: VLAN configuration using ACLI

This section contains procedures to configure VLANs and display VLAN parameters.

Displaying VLANs by type using ACLI

Display all port-based or protocol-based VLANs.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

```
show vlan [type {port | protocol}}
```

Note:

Enter `show vlan` to display all VLANs.

Variable definitions

The following table describes the parameters for the **`show vlan`** command.

Variable	Value
type	Enter the type of VLAN. Values include: • port — show all port-based VLANs • protocol — show all protocol-based VLANs

Displaying VLAN settings per port using ACLI

Display VLAN settings associated with a port, including tagging information, PVID number, priority, and filtering information for tagged, untagged, and unregistered frames.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   show vlan interface info [<portlist>]
   ```

Variable definitions

The following table describes the parameters for the **`show vlan interface info`** command.

Variable	Value
<portlist>	Enter the list of ports for which you want the VLAN information, or enter *ALL* to display all ports.

Displaying port membership using ACLI

Display port membership in VLANs.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   show vlan interface vids [<portlist>]
   ```

Variable definitions

The following table describes the parameters for the **`show vlan interface vids`** command.

Variable	Value
<portlist>	Enter the list of ports for which you want the VLAN information, or enter `all` to display all ports.

Setting or resetting a management VLAN using ACLI

Set a management VLAN or reset the management VLAN to the default.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   [default] vlan mgmt <1–4094>
   ```

Variable definitions

The following table describes the parameters for the **`vlan mgmt`** command.

Variable	Value
<1–4094>	Enter the ID of the VLAN you want to serve as the management VLAN. DEFAULT: 1
default	Reset the management VLAN to the default value.

Deleting a management VLAN IP address using ACLI

Delete the management VLAN IP address.

Important:

This procedure clears the management VLAN IP address from any mode.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   default ip address
   ```

Displaying VLAN ID using ACLI

Display a VLAN ID.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   show vlan id <1–4094>
   ```

Variable definitions

The following table describes the parameters for the **`show vlan id`** command.

Variable	Value
<1–4094>	Specifies the VLAN to be displayed.

Creating a VLAN using ACLI

Create port-based or IPv6 protocol-based VLANs.

Important:

This procedure fails if the VLAN already exists.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   vlan create <1–4094> [name <WORD>] [ type { port | protocol-ipv6Ether2}] {msti [<1–7> | cist]}
   ```

Variable definitions

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

Variable	Value
<1–4094>	Enter the ID of the VLAN you want to create.
name *<WORD>*	Enter the new name you want for the VLAN.
type	Enter the type of VLAN. Values include: • port — port-based VLAN • protocol-ipv6Ether2 — IPv6 protocol-based VLAN
msti *<1–7>* | *cist*	This parameter is available only in MSTP mode. It associates the VLAN with either an MSTI instance or the CIST.

Deleting a VLAN using ACLI

Delete a VLAN.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter one of the following commands:
   - `vlan delete <1–4094>`

     OR
   - `no vlan <1–4094>`

Variable definitions

The following table describes the parameters for the **`vlan delete`** or **`no vlan`** command.

Variable	Value
<1–4094>	Enter the ID of the VLAN to delete.

Configuring VLAN name using ACLI

Configure or change the name of a VLAN.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   vlan name <1–4094> <WORD>
   ```

Variable definitions

The following table describes the parameters for the **`vlan name`** command.

Variable	Value
<1–4094>	Enter the ID of the VLAN for which you want to change the name.
<WORD>	Enter the new name you want for the VLAN.

Displaying VLAN Configuration Control settings using ACLI

Display current VLAN Configuration Control settings.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   show vlan configcontrol
   ```

Modifying VLAN Configuration Control settings using ACLI

Modify current VLAN Configuration Control settings. This procedure applies the selected option to all VLANs on the switch.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   vlan configcontrol <vcc_option>
   ```

Variable definitions

The following table describes the parameters for the **`vlan configcontrol`** command.

Variable	Value
<vcc_option>	This parameters 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.

Enabling or disabling automatic PVID using ACLI

Enable the automatic PVID feature. When auto PVID is active, a port that is assigned to a numbered VLAN has the same number for its PVID. For example, if the port belongs to VLAN 2, the port PVID is 2.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   [no] auto-pvid
   ```

Variable definitions

The following table describes the parameters for the **auto-pvid** command.

Variable	Value
[no]	Disables automatic PVID.

Displaying automatic PVID status using ACLI

Display automatic PVID status.

Procedure

1. Log on to ACLI in User Exec command mode.
2. At the command prompt, enter the following command:
   ```
   show auto-pvid
   ```

Configuring VLAN settings per port using ACLI

Configure VLAN settings for specific ports.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
vlan ports [<portlist>] [tagging{enable | disable | tagAll |
untagALL | tagPVIDOnly | untagPvidOnly}] [pvid <1–4094>]
[filter-unregistered-frames {enable|disable}] [filter-
untagged-frames {enable|disable}][priority <0–7>] [name
<WORD>]
```

Variable definitions

The following table describes the parameters for the **vlan ports** command.

Variable	Value
<portlist>	Enter the port numbers you want to configure for a VLAN.
tagging *{enable* | *disable* | *tagAll* | *untagAll* | *tagPvidOnly* | *untagPvidOnly}*	Specifies the mode for PVID and non-PVID tagging.
pvid *<1–4094>*	Associates the port with a specific 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.
priority *<0–7>*	Sets the port as a priority for the switch to consider as it forwards received packets.
name *<WORD>*	Enter the name you want for this port. **Important:** This option is available only if a single port is specified in the <portlist>

Configuring VLAN members using ACLI

Add a port or delete a port from a specific VLAN.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   vlan members [add|remove] <1–4096> <portlist>
   ```

Variable definitions

The following table describes the parameters for the **`vlan members`** command.

Variable	Value
add | remove	Adds a port or removes a port from a VLAN. ❗ **Important:** If you omit this parameter, you set the exact port membership for the VLAN; the prior port membership of the VLAN is discarded and replaced by a new list of ports.
<1–4094>	Specifies the target VLAN.
portlist	Enter the list of ports you wish to add, remove or assign to the VLAN.

MAC address table configuration using ACLI

This section describes how to view the contents of the MAC address forwarding database table, configure the age-out time for the addresses, and flush the MAC address table.

> ❗ **Important:**
>
> In certain situations, due to the hash algorithm used by the switch to store MAC addresses into memory, some MAC addresses cannot be learned.

Displaying the MAC address forwarding table using ACLI

Display the current contents of the MAC address forwarding database table. You can now filter the MAC Address table by port number. The MAC address table can store up to 16000 addresses.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

```
show mac-address-table [vid <1–4094>] [aging-time] [address
<H.H.H | xx.xx.xx.xx.xx.xx | xx-xx-xx-xx-xx-xx>] [port
<portlist>]
```

Variable definitions

The following table describes the parameters for the **show mac-address-table** command.

Variable	Value
address <*H.H.H* | *xx.xx.xx.xx.xx.xx* | *xx-xx-xx-xx-xx-xx*>	Display a specific MAC addresses if it exists in the database. Enter the MAC address you want displayed using any of the three formats.
aging-time	Display the time in seconds after which an unused entry is removed from the forwarding database.
port <*portlist*>	Specify ports.
vid <*1–4094*>	Enter the ID of the VLAN for which you want to display the forwarding database. DEFAULT: Display the management VLANs database.

Configuring aging time for unseen MAC addresses using ACLI

Configure the time during which the switch retains unseen MAC addresses.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   [default] mac-address-table aging-time <10–1 000 000>
   ```

Variable definitions

The following table describes the parameters for the **`mac-address-table aging-time`** command.

Variable	Value
<10– 1 000 000>	Specifies the aging time in seconds that you want for MAC addresses before they expire.
default	Sets the aging time for MAC addresses to the default value, 300 seconds.

Flushing the MAC address table using ACLI

Flush the MAC address table to clear all addresses in the MAC address table.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   clear mac-address-table
   ```

Variable definitions

The following table describes the parameters for the **`clear mac-address-table interface vlan`** command.

Variable	Value
<1–4094>	Specifies the VLAN for which you want to flush the MAC addresses.

Flushing a VLAN MAC address table using ACLI

Flush the MAC address table for a VLAN to clear the MAC addresses for a specific VLAN.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   clear mac-address-table interface vlan <1–4094>
   ```

Variable definitions

The following table describes the parameters for the **`clear mac-address-table interface vlan`** command.

Variable	Value
<1–4094>	Specifies the VLAN for which you want to flush the MAC addresses.

Flushing a FastEthernet interface MAC address table using ACLI

Flush the MAC address table for a FastEthernet interface to clear the MAC addresses for specified ports. This procedures does not flush the addresses learned on the trunk.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   clear mac-address-table interface FastEthernet <WORD>
   ```

Variable definitions

The following table describes the parameters for the **`clear mac-address-table interface FastEthernet`** command.

Variable	Value
<WORD>	Specifies the list of ports, in the slot/port format, for which you want to flush the MAC addresses.

Flushing a MAC address table for a trunk using ACLI

Flush the MAC address table for a trunk to clear the MAC addresses for the specified trunk. This procedure flushes only addresses that are learned on the trunk.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   clear mac-address-tabe interface mlt <1–32>
   ```

Variable definitions

The following table describes the parameters for the **`clear mac-address-table interface mlt`** command.

Variable	Value
<1–32>	Specifies the trunk for which you want to flush the MAC addresses.

Flushing a single address from the MAC address table using ACLI

Flush a single address from the MAC address table to clear one MAC address from the MAC address table.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.

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

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

Variable definitions

The following table describes the parameters for the **`clear mac-address-table address`**command.

Variable	Value
<H.H.H | *xx.xx.xx.xx.xx.xx*| *xx-xx-xx-xx-xx-xx>*	Specifies the MAC address to clear, using one of the three formats.

Chapter 11: STP configuration using ACLI

STP configuration using ACLI

This section describes how to configure the Spanning Tree Protocol using the Avaya Command Line Interface (ACLI).

Using spanning tree

You can use the ACLI to configure a spanning tree, to add or remove VLANs from the spanning tree, and to configure the usual spanning tree parameters and FastLearn.

For detailed information about spanning tree parameters, Spanning Tree Groups, and configuration guidelines, see Spanning Tree Protocol Fundamentals on page 39.

Displaying spanning tree configuration information using ACLI

Display spanning tree configuration information that is specific to either the spanning tree group or to the port.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show spanning-tree { config|port|port-mode|mode|cost-calc-
   mode}
   ```

Variable definitions

The following table describes the parameters for the **show spanning-tree** command.

Variable	Value
config	Displays spanning tree configuration.
port	Displays spanning tree status of each port.
port-mode	Displays the spanning tree port mode.
mode	Displays the spanning tree mode.
cost-calc-mode	Displays pathcost type.

Setting path cost calculation using ACLI

Set path cost calculation mode for the Spanning Tree Group.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   spanning-tree cost-calc-mode [dot1d|dot1t]
   ```

Configuring STG parameters using ACLI

Configure Spanning Tree Group (STG) parameters or reset STG parameters to default.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   spanning-tree [cost-calc-mode][forward-time <4–30>] [hello-
   time <1–10>] [max-age <6–40>][mode][port-mode][priority
   {0*0000 | 0*1000 | 0*2000 | 0*3000 | ... | 0*E000 | 0*F000}]
   ```
3. To reset to default, use the following command:
   ```
   default spanning-tree [cost-calc-mode][forward-time] [hello-
   time] [max-age][mode][port—mode] [priority]
   ```

Variable definitions

The following table describes the parameters for the **`spanning-tree`** command.

Variable	Value
cost-calc-mode	Specifies pathcost type.
forward-time *<4–30>*	Specifies the forward time of the STG in seconds. RANGE: 4–30 seconds DEFAULT: 15 seconds
hello-time *<1–10>*	Specifies the hello time of the STG in seconds. RANGE: 1–10 seconds DEFAULT: 2 seconds
max-age *<6–40>*	Specifies the max-age of the STG in seconds. RANGE: 6–40 seconds DEFAULT: 20 seconds
mode	Specifies the operation mode as one of the following protocols: • mstp — multiple spanning tree protocol • rstp —rapid spanning tree protocol • stpg — Avaya spanning tree group protocol
port-mode	Specifies the port mode
priority *{0*0000* | *0*1000* | *0*2000* | *0*3000* |... | *0*E000* | *0*F000}*	Sets the spanning tree priority (in Hex); if 802.1T compliant, this value must be a multiple of 0x10000.
default	Sets the STP parameters to their default values.

Configuring STG operation mode using ACLI

Set the operation mode for the Spanning Tree Group (STG).

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

Variable definitions

The following table describes the parameters for the **spanning-tree mode** command.

Variable	Value
mode *{mstp*|*rstp*|*stpg}*	Specifies the operation mode as one of the following protocols: • mstp — multiple spanning tree protocol • rstp —rapid spanning tree protocol • stpg — Avaya spanning tree group protocol

Configuring STP for ports using ACLI

Configure Spanning Tree Protocol for specific ports.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   [default] spanning-tree [port <portlist>] [learning {disable|
   normal|fast}] [cost <1–65535>] [priority <0–255>]
   ```

Variable definitions

The following table describes the parameters for the **spanning-tree** command.

Variable	Value
port <*portlist*>	Enables spanning tree for the specified port or ports; enter the port or ports you want enabled for spanning tree. **Important:** If you omit this parameter, the system uses the port number you specified after you issued the **interface** command.

Variable	Value
learning *{disable*|*normal*|*fast}*	Specifies the STP learning mode: • disable — disable spanning tree on the port • normal — normal learning mode • fast — FastLearn mode If [default] is used with the learning parameter, the learning mode is set to the default mode of normal mode.
cost *<1–65535>*	Enter the path cost of the spanning tree. RANGE: 1 to 65535 DEFAULT: The default value for path cost depends on the type of port.
priority *<0–255>*	Enter the priority value of the spanning tree. RANGE: 0 to 255 DEFAULT: 0x8000. If [default] is used with the priority parameter, the priority is set to the default value of 0x8000.

Configuring STP port mode using ACLI

Configure Spanning Tree port mode to enable a port to maintain STP membership when the port is moved from one VLAN to another.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   spanning-tree port-mode {auto | normal}
   ```

Variable definitions

The following table describes the parameters for the **`spanning-tree port-mode`** command.

Variable	Value
auto	Specifies automatic STP port mode.
normal	Specifies normal STP port mode.

Enabling or disabling STP 802.1d compliance mode using ACLI

Enable STP 802.1d compliance mode to ensure that STP confirms to the IEEE 802.1d standard. You can also disable STP 802.1d compliance mode from this procedure by using the [no] parameter.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   [no] spanning-tree 802dotld-port-compliance enable
   ```

Disabling STP for ports using ACLI

Disable STP for ports in a specific STG.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   no spanning-tree [port <portlist>]
   ```

Variable definitions

The following table describes the parameters for the **`no spanning-tree`** command.

Variable	Value
port <*portlist*>	Disables spanning tree for the specified port or ports. Enter port or ports you want disabled for STP. **Important:** If you omit this parameter, the system uses the port number you specified after you issued the **`interface`** command.

Using Advanced Spanning Tree

The Advanced Spanning Tree Protocol (ASTP) application comprises Rapid Spanning Tree Protocol (RSTP) and Multi Spanning Tree Protocol (MSTP). You can configure the RSTP and MSTP applications.

Displaying RSTP configuration details using ACLI

Display the RSTP related bridge-level configuration details.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   show spanning-tree rstp config
   ```

Displaying RSTP bridge statistics using ACLI

Display RSTP related bridge-level statistics.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   show spanning-tree rstp statistics
   ```

Displaying RSTP status information using ACLI

Display the RSTP related status information for the selected bridge.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

```
show spanning-tree rstp status
```

Displaying RSTP port configuration details using ACLI

Display RSTP related port-level configuration details.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   show spanning-tree rstp port config [<portlist>]
   ```

Variable definitions

The following table describes the parameters for the **`show spanning-tree rstp port config`** command.

Variable	Value
<portlist>	Specify the port for which you want to display RSTP configuration details.

Displaying RSTP port role using ACLI

Display RSTP related port-level role information.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   show spanning-tree rstp port role [<portlist>]
   ```

Variable definitions

The following table describes the parameters for the **`show spanning-tree rstp port role`** command.

Variable	Value
<portlist>	Specifies the port for which you want to display RSTP port role.

Displaying RSTP port statistics using ACLI

Display RSTP related port-level statistics.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

```
show spanning-tree rstp port statistics <portlist>
```

Variable definitions

The following table describes the parameters for the **`show spanning-tree rstp port statistics`** command.

Variable	Value
<portlist>	Specifies the port or ports for which you want to display RSTP statistics.

Displaying RSTP status per port using ACLI

Display the RSTP related status information for the selected port.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

```
show spanning-tree rstp port status [<portlist>]
```

Variable definitions

The following table describes the parameters for the **show spanning-tree rstp port status** command.

Variable	Value
<portlist>	Specifies the port for which you want to display RSTP status.

Configuring RSTP parameters using ACLI

Set the RSTP parameters, which include forward delay, hello time, maximum age time, default pathcost version, bridge priority, transmit hold count, and version for the bridge.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
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

The following table describes the parameters for the **spanning-tree rstp** command.

Variable	Value
port *<portlist>*	Filters on the list of ports.
cost *<1 — 200000000>*	Sets the RSTP pathcost on the single or multiple ports. DEFAULT: 200000.
edge-port *{false|true}*	Indicates whether the single or multiple ports should be assumed to be edge port. This parameter sets the Admin value of edge port status.

Variable	Value
	DEFAULT: false
learning *{disable* | *enable}*	Enables or disables RSTP on the single or multiple ports. DEFAULT: enable
p2p *{auto*|*force-false* | *force-true}*	Indicates whether the single or multiple port should be treated as a point-to-point link or not. This command sets the Admin value of P2P status. DEFAULT: force-true
priority *{00*|*10*|*...*|*F0}*	Sets the RSTP port priority on the single or multiple port. DEFAULT: 80
protocol-migration *{false*|*true}*	Forces the single or multiple ports to transmit RSTP BPDUs when set true, while operating in RSTP mode. DEFAULT: false

Displaying MSTP related information using ACLI

Display the MSTP related bridge-level, VLAN and region information.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

```
show spanning-tree mstp config
```

Displaying MSTP status information using ACLI

Display the MSTP related status information known by the selected bridge.

Procedure

1. Log on to ACLI in command mode.
2. At the command prompt, enter the following command:

```
show spanning-tree mstp status
```

Displaying MSTP related statistics using ACLI

Display MSTP related bridge-level statistics.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show spanning-tree mstp statistics
   ```

Displaying MSTP Cist port information using ACLI

Display the Multi Spanning Tree protocol (MSTP) Cist Port information maintained by every port of the Common Spanning Tree.

Before you begin

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show spanning-tree mstp port config [<portlist>]
   ```

   Important:

   In MSTP, if the Regional Root changes, the change does not display correctly when entering the **`show spanning-tree mstp port config`** command. In the command output, the Cist Port Regional Root field does not display the correct Regional Root.

Variable definitions

The following table describes the parameters for the **`show spanning-tree mstp port config`** command.

Variable	Value
<portlist>	Enter a list or range of port numbers.

Displaying MSTP Cist port role using ACLI

Display MSTP Cist port role information.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show spanning-tree mstp port role [<portlist>]
   ```

Variable definitions

The following table describes the parameters for the **`show spanning-tree mstp port role`** command.

Variable	Value
<portlist>	Specifies the port for which you want to display the MSTP port role.

Displaying MSTP Cist port statistics using ACLI

Display the Multi Spanning Tree Protocol (MSTP) Cist Port statistics that are maintained by every port.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show spanning-tree mstp port statistics [<portlist>]
   ```

Variable definitions

The following table describes the parameters for the **`show spanning-tree mstp port statistics`**command.

Variable	Value
<portlist>	Enter a list or range of port numbers.

Displaying MSTP bridge and VLAN information using ACLI

Display the Multi Spanning Tree Protocol (MSTP) instance-specific bridge and VLAN information.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   show spanning–tree mstp msti config <1 –7>
   ```

Variable definitions

The following table describes the parameters for the **`show spanning-tree mstp msti config`** command.

Variable	Value
<1–7>	Filters on MSTP instance.

Displaying MSTP bridge statistics using ACLI

Display the Multi Spanning Tree Protocol (MSTP) instance-specific bridge statistics.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   show spanning-tree mstp msti statistics <1 –7>
   ```

Variable definitions

The following table describes the parameters for the **`show spanning-tree mstp msti statistics`** command.

Variable	Value
<1–7>	Filters on MSTP instance.

Displaying MSTP port information using ACLI

Display Multi Spanning Tree Protocol (MSTP) instance-specific to port information.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   show spanning-tree mstp msti port config <1–7> [<portlist>]
   ```

Variable definitions

The following table describes the parameters for the **`show spanning-tree mstp msti port config`** command.

Variable	Value
<1–7>	Filter on MSTP instance.
<portlist>	Enter a list or range of port numbers.

Displaying MSTP port role using ACLI

Display the Multi Spanning Tree Protocol (MSTP) instance-specific to port statistics.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

```
show spanning-tree mstp msti port role <1–7> [<portlist>]
```

Variable definitions

The following table describes the parameters for the **`show spanning-tree mstp msti port role`** command.

Variable	Value
<1–7>	Enter an MSTP instance from 1 to 7.
<portlist>	Enter a list or range of port numbers

Displaying MSTP port statistics using ACLI

Display the Multi Spanning Tree Protocol (MSTP) instance-specific to port statistics.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

```
show spanning-tree mstp msti port statistics <1 –7>
[<portlist>]
```

Variable definitions

The following table describes the parameters for the **`show spanning-tree mstp msti port statistics`** command.

Variable	Value
<1–7>	Filter on MSTP instance.
<portlist>	Enter a list or range of port numbers.

Configuring MSTP parameters for Cist bridge using ACLI

Configure the MSTP parameters which include maximum hop count, maximum number of instances allowed, forward delay time, hello time, maximum age time, default pathcost version, priority, transmit hold count, and version for the Cist Bridge.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   spanning-tree mstp [max-hop <600 - 4000>] [forward-time <4
   -30>] [max-age <6 - 40>] [pathcost-type {bits16 | bits32}]
   [priority {0000 | 10000 | 20000 | … | F0000}] [tx-hold count
   <1- 10>] [version {stp-compatible | rstp| mstp}] [add-
   vlanb<1-4094>] [remove-vlan <1-4094>] [msti <1-7>] [region
   {config-id-sel|region-name|region-version}]
   ```

Variable definitions

The following table describes the parameters for the **`spanning-tree mstp`** command.

Variable	Value
max-hop *<600–4000>*	Sets the MSTP maximum hop count. DEFAULT: 2000
forward-time *<4–30>*	Sets the MSTP forward delay for the Cist Bridge in seconds. DEFAULT: 15 seconds
max-age *<6–40>*	Sets the MSTP maximum age time for the Cist Bridge in seconds. DEFAULT: 20 seconds
pathcost-type *{bits16* | *bits32}*	Sets the MSTP default pathcost version. DEFAULT: bits32
priority *{0000* | *10000* | *20000...*|*F000}*	Sets the MSTP bridge priority for the Cist Bridge. DEFAULT: 8000
tx-holdcount *<1–10>*	Sets the MSTP Transmit Hold Count. DEFAULT: 3
version *{stp-compatible* | *rstp*| *mstp}*	Sets the MSTP version for he Cist Bridge. DEFAULT: mstp
add-vlan	Adds a VLAN to the CIST bridge.
remove-vlan	Removes a VLAN from the CIST bridge.
msti	Changes MSTP instance-specific configuration.
region	Changes MSTP region configuration.

Configuring MSTP parameters for Common Spanning Tree using ACLI

Configure the MSTP parameters which include pathcost, hello time, edge-port indicator, learning mode, point-to-point indicator, priority, and protocol migration indicator on the single or multiple port for the Common Spanning Tree.

Before you begin

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
spanning-tree mstp [port <portlist>] [cost <1 - 200000000>]
[edge-port {false | true}][hello-time <1 - 10>] [learning
{disable | enable}][p2p {auto | force-false | force-true}]
[priority {00 | 10 | ... | F0}] [protocol-migration {false |
true}]
```

Variable definitions

The following table describes the parameters for the **`spanning-tree mstp`** command.

Variable	Value
port *<portlist>*	Specifies a list or range of port numbers.
cost *<1 — 2000000000>*	Sets the MSTP pathcost on the single or multiple port. DEFAULT: 200000
hello-time *<1–10>*	Sets the MSTP hello time on the single or multiple port for the Common Spanning Tree. DEFAULT: 2
edge-port *{false* | *true}*	Indicates whether the single or multiple port should be assumed to be edge port or not. This parameter sets the Admin value of edge port status. DEFAULT: false
learning *{disable* | *enable}*	Enables or disables MSTP on the single or multiple port. DEFAULT: enable

Variable	Value
p2p *{auto* | *force-false* | *force-true}*	Indicates whether the single or multiple port should be treated as a point-to-point link or not. This command sets the Admin value of P2P Status. DEFAULT: force-true
priority *{00* | *10* | *...*|*F0}*	Sets the MSTP port priority on the single or multiple port. DEFAULT: 80
protocol-migration *{false* | *true}*	Forces the single or multiple port to transmit MSTP BPDUs when set true, while operating in MSTP mode. DEFAULT: false

Configuring MSTP region parameters using ACLI

Configure the MSTP parameters including config ID selector, region name and region version.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
spanning-tree mstp region [config-id-sell <0 - 255>] [region-
name <1 - 32 chars>][region-version <0 - 65535>]
```

Variable definitions

The following table describes the parameters for the **`spanning-tree mstp region`** command.

Variable	Value
[config-id-sel *<0–255>]*	Sets the MSTP config ID selector. DEFAULT: 0
[region-name *<1–32 chars>]*	Sets the MSTP region name. DEFAULT: the MAC address of the switch
[region-version *<0–65535>]*	Sets the MSTP region version. DEFAULT: 0

Configuring MSTP MSTI bridge parameters using ACLI

Configure the MSTP parameters which include forward delay time, hello-time, max hop count, priority, and VLAN mapping for the bridge instance.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
spanning-tree mstp msti <1 - 7>[priority{0000|1000|…|F000}]
[add-vlan <vid>][remove-vlan <vid>][enable]
```

Variable definitions

The following table describes the parameters for the **`spanning-tree mstp msti`** command.

Variable	Value
<1–7>	Filter on MSTP instance.
priority *{0000* | *1000* | *...* | *F000}*	Sets the MSTP priority for the bridge instance. DEFAULT: 8000
add-vlan *<1–4094>*	Maps the specified vlan and MSTP bridge instance.
remove-vlan *<1–4094>*	Unmaps the specified vlan and MSTP bridge instance.
enable	Enables the MSTP bridge instances.

Configuring MSTP MSTI port parameters using ACLI

Configure the MSTP parameters including MSTP port pathcost, learning mode, and priority on the single or multiple port for the bridge instance.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
spanning-tree mstp msti <1 - 7> [port <portlist>] [cost <1
-200000000>][learning {disable | enable}][priority {00 | 10 |
…| F0}]
```

Variable definitions

The following table describes the parameters for the **`spanning-tree mstp msti`** command.

Variable	Value
<1–7>	Filter on MSTP instance.
port <*portlist*>	Enter a list or range of port numbers.
cost *<1 — 200000000>*	Set the MSTP port pathcost on the single or multiple port for the bridge instance. DEFAULT: 200000
learning *{disable* | *enable}*	Enable or disable MSTP on the single or multiple port for the bridge instance. DEFAULT: enable
priority *{00* | *10*| *...*|*F0}*	Set the MSTP port priority on the single or multiple port for the bridge instance. DEFAULT: 80

Deleting an MSTP bridge using ACLI

Delete an MSTP bridge-instance.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   no spanning-tree mstp msti <1–7>
   ```

Variable definitions

The following table describes the parameters for the **no spanning tree mstp msti** command.

Variable	Value
<1 —7>	Filter on MSTP instance.

Enabling or disabling an MSTP bridge using ACLI

Enable or disable an MSTP bridge instance.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
[no] spanning-tree mstp msti <1 —7> enable
```

Variable definitions

The following table describes the parameters for the **spanning-tree mstp msti enable** command.

Variable	Value
<1 —7>	Filters on MSTP instance.
no	Disables an MSTP bridge.

Configuring STP BPDU filtering using ACLI

Configure STP BPDU filtering on a port. This procedure can be used in all STP modes (STPG, RSTP, and MSTP).

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

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

3. To return to default values, use the following command:

```
default spanning-tree bpdu-filtering [port <portlist>]
[enable] [timeout]
```

4. To disable, use the following command:

```
no spanning-tree bpdu-filtering [port <portlist>] [enable]
```

5. To display the status of parameters, use the following command:

```
show spanning-tree bpdu-filtering fastEthernet [port
<portlist>]
```

Variable definitions

The following table describes the parameters for the **`spanning-tree bpdu-filtering`** command.

Variable	Value
port <*portlist*>	Specifies the ports affected by the command.
enable	Enables STP BPDU Filtering on the specified ports. DEFAULT: Disabled
no	Disables STP BPDU Filtering on the specified ports.
default	Returns STP BPDU Filtering to the default value on the specified ports. DEFAULT: 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. DEFAULT: 120 seconds

Chapter 12: Multi-Link Trunking configuration using ACLI

Configuring Multi-Link Trunking using ACLI

Displaying MLT configuration using ACLI

Display Multi-Link Trunking (MLT) configuration and utilization.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   show mlt [<1–6> | spanning-tree <1–6>]
   ```

Variable definitions

The following table describes the parameters for the **`show mlt`** command.

Variable	Value
<1–6>	Displays the MLT/spanning tree utilization in percentages.

Configuring a Multi-Link Trunk using ACLI

Configure a multi-link trunk.

Important:

An MLT must be disabled when you are adding ports.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   mlt <id> [name <trunkname>][enable|disable] [member
   <portlist>][learning {disable|fast|normal}] [loadbalance
   <advance|basic>][bpdu{all-ports|single-port}]
   ```

Variable definitions

The following table describes the parameters for the **mlt** command.

Variable	Value
id	Specifies the trunk ID. RANGE: 1 to 6
name *<trunkname>*	Specifies a text name for the trunk. Enter up to 16 alphanumeric characters.
enable | disable	Enables or disables the trunk.
member *<portlist>*	Enter the ports that you want as members of the trunk.
learning *<disable*|*fast*|*normal>*	Sets STP learning mode.
loadbalance *<advance* | *basic>*	Specifies MLT load balancing mode. Advance mode uses IP based load balancing. Basic mode uses MAC based load balancing.
bpdu *{all-ports*|*single-port}*	Sets BPDU send/received mode.

Deleting a Multi-Link Trunk using ACLI

Delete a specific Multi-Link Trunk (MLT) or all configured MLTs.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command to delete a specific MLT:
   ```
   no mlt [<id>]
   ```
3. To delete all configured MLTs, enter the following command:

no mlt

Variable definitions

The following table describes the parameters for the **`no mlt`** command.

Variable	Value
<*id*>	Specifies the ID of the MLT you want to delete.

Configuring MLT whole trunk using ACLI

Configure the shutdown of all ports in the MLT. This procedure enables or disables the MLT whole trunk feature.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   [no] mlt shutdown-ports-on-disable enable
   ```

Variable definitions

The following table describes the parameters for the **`mlt shutdown-ports-on-disable enable`** command.

Variable	Value
no	Disables the MLT whole trunk feature.

Displaying the MLT whole trunk status using ACLI

Display the current MLT whole trunk mode.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

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

Example

The following shows example outputs for the **`show mlt shutdown-ports-on-disable`** command.

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

`Trunk loop prevention is disabled`— MLT whole trunk feature is disabled (default).

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

`Trunk loop prevention is enabled`— MLT whole trunk feature is enabled.

Configuring Link Aggregation Group using ACLI

Configuring LACP system priority using ACLI

Set a system priority for LACP.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   lacp system-priority [0–65535]
   ```

Variable definitions

The following table describes the parameters for the **`lacp system-priority`** command.

Variable	Value
[0-65535]	Specifies a system priority for LACP. RANGE: 0 to 65535
default	Resets the system priority for LACP to the default value of 32768.

Configuring LACP port mode using ACLI

Set the mode for an LACP port.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   lacp mode [port <portlist>] {off|passive}active}
   ```

Variable definitions

The following table describes the parameters for the **lacp mode** command.

Variable	Value
port <*portlist*>	Specifies the ports for which you want to set the LACP mode.
port *[off*|*passive*|*active]*	Sets the LACP mode for the specified port of off, passive, or active. If port mode is selected as Passive or Active, port is ready to participate in LACP. DEFAULT: off

Resetting LACP port mode to default

Place an LACP port in the default mode.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   default lacp mode [port <portlist>]
   ```

Variable definitions

The following table describes the parameters for the **`default lacp mode`** command.

Variable	Value
port <*portlist*>	Enter the ports that you want to set in the LACP default mode of OFF.

Enabling or removing LACP aggregation for ports using ACLI

Enable or remove LACP aggregation on the specified port(s).

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   [no] [default] lacp aggregation [port <portlist>] enable
   ```

Variable definitions

The following table describes the parameters for the **`lacp aggregation`** command.

Variable	Value
port <*portlist*>	Specifies the port(s) you want to enable LACP aggregation.
no	Removes LACP aggregation for the specified port(s)
default	Disables LACP aggregation by default.

Assigning a key value to a port using ACLI

Assign a key value for the specified port(s).

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command to assign a key value :

```
lacp key [port <portlist>] <1–4095>
```

3. To set the LACP key to the default value (1) , enter the following command:

```
default lacp key [port<portlist>]
```

Variable definitions

The following table describes the parameters for the **`lacp key`** command.

Variable	Value
port <*portlist*>	Specifies the ports for which you want to assign an LACP key value.
default	Sets the key value for the specified port to the default value. DEFAULT: 1
<*1–4095*>	Specifies an LACP key value for the port. RANGE: 1 to 4095

Assigning LACP priority for ports using ACLI

Set an LACP priority for the specified port(s).

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
[default] lacp priority [port <portlist>] <0–65535>
```

Variable definitions

The following table describes the parameters for the **`lacp priority`** command.

Variable	Value
port <*portlist*>	Specifies the ports for which you want to set LACP priority.
<*0–65535*>	Specifies a priority number for the port. RANGE: 0 to 65535 DEFAULT: 32768

Variable	Value
default	Sets the LACP priority for the specified port(s) to the default value of 32768.

Configuring LACP timeout using ACLI

Set an LACP timeout for the specified port(s).

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   lacp timeout-time [port <portlist>] {short | long}
   ```

Variable definitions

The following table describes the parameters for the **`lacp timeout-time`** command.

Variable	Value
port <*portlist*>	Specifies the ports for which you want to set an LACP timeout.
port {*short* | *long*}	Sets a short or long LACP timeout for the port. The long timeout is 90 seconds and the short timeout is 3 seconds.

Displaying LACP information using ACLI

Display LACP information for the entire system.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   show lacp system
   ```

Displaying LACP aggregator information using ACLI

Display LACP aggregator information.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   show lacp aggr [<1–65535>]
   ```

Variable definitions

The following table describes the parameters for the **show lacp aggr** command.

Variable	Value
<1–65535>	Enter the aggregator ID.

Displaying LACP port information using ACLI

Display LACP port information.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   show lacp port [<portlist>]
   ```

   Important:

   The output of the **show vlacp port** command will display “A” or “I” for port type. A=Aggregatable and I=Individual.

Variable definitions

The following table describes the parameters for the **`show lacp port`** command.

Variable	Value
port <*portlist*>	Specifies the ports for which you want information.

Displaying LACP port debug information using ACLI

Display LACP port debug information.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   show lacp debug member [port <portlist>]
   ```

   The command can display the following terms:

   LACP Receiving State:

   - Current: Rx information is valid
   - Expired: Rx information is invalid
   - Defaulted: Rx machine is defaulted
   - Initialized: Rx machine is initializing
   - LacpDisabled: LACP is disabled on this port
   - PortDisabled: Port is disabled.

   Selection State:

   - Detached: Port is not attached to any aggregator
   - Waiting: Port is waiting to attach to an aggregator
   - Attached: Port is attached to an aggregator
   - Ready: Port is ready to Tx and Rx

Variable definitions

The following table describes the parameters for the **`show lacp debug member`** command.

Variable	Value
port <*portlist*>	Specifies the port(s) for which you want debug information.

Displaying LACP port statistics using ACLI

Display LACP port statistics.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   show lacp stats [port <portlist>]
   ```

Variable definitions

The following table describes the parameters for the **`show lacp stats`** command.

Variable	Value
port <*portlist*>	Specifies the port(s) for which you want statistics.

Clearing LACP port statistics using ACLI

Clear LACP port statistics.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   lacp clear-stats [port <portlist>]
   ```

Variable definitions

The following table describes the parameters for the **`lacp clear-stats`** command.

Variable	Value
port <*portlist*>	Specifies the port(s) for which you want to clear statistics.

Configuring VLACP using ACLI

You can use the ACLI to configure Virtual Link Aggregation Control Protocol (VLACP) parameters.

✱ **Note:**

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

Enabling or disabling VLACP globally using ACLI

Enable or disable VLACP globally for the device using this procedure.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   [no] vlacp enable
   ```

Variable definitions

The following table describes the parameters for the **`vlacp enable`** command.

Variable	Value
no	Disables VLACP globally for the device.

Configuring multicast MAC address for VLACP using ACLI

Set the multicast MAC address used by the device VLACPDUs.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   vlacp macaddress <macaddress>
   ```

Variable definitions

The following table describes the parameters for the **`vlacp macaddress`** command.

Variable	Value
<macaddress>	Specifies MAC address in the format 00:00:00:00:00:00.

Configuring VLACP on a port using ACLI

Configure VLACP parameters on a port.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   vlacp port <slot/port> [enable | disable] [timeout <long/
   short>][fast-periodic-time <integer>] [slow-periodic-time
   <integer>] [timeout-scale <integer>] [funcmac-addr
   <macaddress>][ethertype <hex>]
   ```

Variable definitions

The following table describes the parameters for the **`vlacp port`** command.

Variable	Value
<slot/port>	Specifies the slot and port number.

Variable	Value
enable|disable	Enables or disables 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) x (slow-periodic-time value). • short sets the port's timeout to: (timeout-scale value) x (fast-periodic-time value). For example, if the timeout is set to short while the timeout-scale value is 3 and the fast-periodic-time value is 400 ms, the timer expires after 1200 ms. DEFAULT: long
fast-periodic-time <*integer*>	Specifies the number of milliseconds between periodic VLACPDU transmissions using short timeouts. RANGE: 400 to 20000 ms DEFAULT: 500 ms
slow-periodic-time <*integer*>	Specifies the number of milliseconds between periodic VLACPDU transmissions using long timeouts. RANGE: 10000 to 30000 ms DEFAULT: 30000 ms
timeout-scale <*integer*>	Sets a timeout scale for the port, where timeout = (periodic time) x (timeout scale). RANGE: 1 to 10 DEFAULT: 3 **Note:** With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. However, if the timeout-scale is set to 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 after the packet arrives. To prevent this scenario from happening, set the timeout-scale toa value larger than 1.
funcmac-addr <*macaddress*>	Specifies the address of the far-end switch configured to be the partner of this switch. If none is configured, any VLACP-enabled

Variable	Value
	switch communicating with the local switch through VLACP PDUs is considered to be the partner switch. **Note:** VLACP has only one multicast MA C 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 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. 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. RANGE: 8101–81FF DEFAULT: 8103

Resetting VLACP MAC address value using ACLI

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

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
no vlacp macaddress
```

Disabling VLACP on a port using ACLI

Disable VLACP on the port.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   no vlacp <slot/port> [enable] [funcmac-addr]
   ```

Variable definitions

The following table describes the parameters for the **no vlacp** command.

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

Displaying VLACP status using ACLI

Display the status of VLACP on the switch.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   show vlacp
   ```

Displaying VLACP configuration for a port using ACLI

Display VLACP configuration details for a port or list of ports.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   `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 receive any VLACPDUs yet.

   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.

   As long as the VLACP functional address for a specific interface is not changed when using the command (config-if)#vlacp port x funcmac-addr H.H.H/ xx.xx.xx.xx.xx.xx, 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 specified 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.

Variable definitions

The following table describes the parameters for the **`show vlacp interface`** command.

Variable	Value
<slot/port>	Specifies a port or list of ports.

Chapter 13: Configuring ADAC for Avaya IP Phones using ACLI

Configuring global ADAC settings using ACLI

Enable global settings for Auto-Detection Auto-Correction (ADAC) on the device.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command to enable global settings for ADAC:

   ```
   adac [enable] [op-mode {untagged-frames-basic|untagged-
   frames-advanced|tagged-frames}] [voice-vlan <1–4094>]
   [uplink-port <portlist>][call-server-port <portlist>] [mac-
   range-table {low-end} {0123.4567.89ab} {high-end}
   (0123.4567.89ff}]}
   ```

Variable definitions

The following table describes the parameters for the **adac** command.

Variable	Value
enable	Enables ADAC on the device.

Variable	Value
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, and the Voice VLAN is created
voice-vlan *<1–4094>*	Configures the Voice VLAN ID. The assigned VLAN ID must not previously exist.
uplink-port *<portlist>*	Configures a maximum of 8 ports as uplink ports.
call-server-port *<portlist>*	Configures a maximum of 8 ports as Call Server ports.
mac-range-table *{low-end}{0123.4567.89ab}{high-end}{0123.4567.89ff}*	Adds new supported MAC address range. ❗ **Important:** MAC address must be entered in Hexadecimal format. ❗ **Important:** Specify the low-end parameter first to set the high-end parameter (H.H.H/xx.xx.xx.xx.xx.xx) for mac-range-table.

Disabling or clearing ADAC settings using ACLI

Disable or clear ADAC settings on the device.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
no adac {[enable] [voice-vlan] [uplink-port] [call-server-
port][mac-range-table {low-end}{0123.4567.89ab}{high-end}
{0123.4567.89ff}]}
```

Variable definitions

The following table describes the parameters for the **`no adac`** command.

Variable	Value
enable	Disables ADAC on the device
voice-vlan	Clears Voice-VLAN ID
uplink-port	Clears the uplink ports
call-server-port	Clears the Call Server ports
mac-range-table *{low-end}* *{0123.4567.89ab}{high-end}* *{0123.4567.89ff}*	Deletes the supported MAC address range ❗ **Important:** Specify the low-end parameter first to set the high-end parameter (H.H.H/ xx.xx.xx.xx.xx.xx) for mac-range-table.

Resetting ADAC settings to default using ACLI

Restore default ADAC settings on the device.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
default adac {[enable][op-mode][voice-vlan][uplink-port]
[call-server-port][mac-range-table]
```

Variable definitions

The following table describes the parameters for the **`default adac`** command.

Variable	Value
enable	Restores the default state of ADAC
op-mode	Restores the default ADAC operation mode
voice-vlan	Restores the default Voice-VLAN Id

Variable	Value
uplink-port	Restores the default Uplink port
call-server-port	Restores the default Call Server port
mac-range-table	Restores the MAC address ranges supported by default

Configuring ADAC MAC address ranges using ACLI

Add or delete a specified range to the table of MAC addresses recognized as Avaya IP Phones by the Auto-Detection process.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
[no] adac mac-range-table low-end <0123.4567.89aa> high-end
<0123.4567.89aff>
```

Variable definitions

The following table describes the parameters for the **`adac mac-range-table`** command.

Variable	Value
no	Deletes a range in the table of MAC addresses recognized by Avaya IP Phones by the Auto-Detection process.
low-end*<0123.4567.89aa>*	Specifies the low-end of the MAC address range to be added or deleted
high-end *<0123.4567.89aff>*	Specifies the high-end of the MAC address range to be added or deleted

Resetting MAC address ranges using ACLI

Restores all supported MAC address ranges on the switch their default values.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   default adac mac-range-table
   ```

Configuring ADAC device settings per port using ACLI

Set Auto-Detection Auto-Correction (ADAC) settings for the device on a specific port.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   adac [port <portlist>] {[enable][tagged-frames-pvid {1–4094>
   |no-change}] [tagged-frames-tagging {tagAll| tagPvidOnly|
   untagPvidOnly| no-change}] [detection {[mac][lldp]}]}
   ```

Variable definitions

The following table describes the parameters for the **adac** command.

Variable	Value
enable	Enables auto-detection on ports
port *<portlist>*	Specifies the port number for which settings are to be changed
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.

Variable	Value
detection*{[mac][lldp]}*	Enables detection mechanisms on ports; either mac or lldp.

Setting ADAC detection method using ACLI

Set the detection method, by MAC address or using LLDP (IEEEE 802.1AB) for a device on a port.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   [no] adac detection [port <portlist>] {[mac][lldp]}
   ```

Variable definitions

The following table describes the parameters for the **`adac detection`** command.

Variable	Value
no	Disables ADAC detection.
mac	Enables MAC-based detection on ports
lldp	Enables 802.1AB-based detection on ports
port <*portlist*>	Specifies the port or ports for which to set the detection mode.

Disabling ADAC per port using ACLI

Disable ADAC settings for the device on a specific port.

Procedure

1. Log on to ACLI Interface Configuration command mode.
2. At the command prompt, enter the following command:

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

Variable definitions

The following table describes the parameters for the **`no adac`** command.

Variable	Value
port <*portlist*>	Specifies the port numbers for which to change the settings
enable	Disables auto detection on ports

Resetting ADAC port settings to default using ACLI

Restore the per port ADAC settings to defaults for the specified ports.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
default adac [port <portlist>] {[enable] [tagged-frames-pvid]
[tagged-frames-tagging]}
```

Variable definitions

The following table describes the parameters for the **`default adac`** command.

Variable	Value
port <*portlist*>	Specifies the port numbers for which to change the settings
enable	Restores default auto-detection on ports
tagged-frames-pvid	Restores default PVID to be configured for telephony ports in Tagged Frames operating mode

Variable	Value
tagged-frames-tagging	Restores default tagging to be configured for telephony ports in Tagged Frames operating mode

Restoring ADAC detection method to default using ACLI

Restore the ADAC auto-detection method by either MAC address or LLDP for a device on a port.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   adac detection [port <portlist>] {[mac] [lldp]|}
   ```

Variable definitions

The following table describes the parameters for the **default adac detection** command.

Variable	Value
port *<portlist>*	Specifies the port numbers for which to change the settings
mac	Restores default MAC-based detection on ports.
lldp	Restores default 802.1AB-based detection on ports.

Displaying ADAC settings per port using ACLI

Display ADAC settings for the device on a specific port.

Procedure

1. Log on to ACLI in Global Configuration command mode.

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

```
show adac interface <Type> <Auto-Detection> <Oper State>
<Auto-Configuration> <Tagged-Frames PVID> <Tagged-
FramesTagging>
```

Variable definitions

The following table describes the parameters for the **show adac interface** command.

Variable	Value
Type	Specifies how ADAC classifies this port: • T: Telephony port • CS: Call Server port • U: Uplink port or part of the same trunk as the current set uplink port
Auto-Detection	Controls whether the interface should auto-detect; if there is any Avaya IP Phone connected to it (and implicitly apply auto-configuration for it)
Oper State	Indicates whether ADAC is enabled or disabled on that port
Auto-Configuration	Specifies if the auto-configuration is applied on a port or not
Tagged-Frames PVID	Specifies the PVID value that Auto-Configuration apply for ports having Auto-Detection enabled and running in Tagged-Frames operational mode. A value of 0 indicates that Auto-Configuration cannot change the PVID for the respective port. If the VLAN with the ID equal with this PVID does not exist when Auto-Configuration is applied to a port, then Auto-Configuration won't change the port's PVID (it will ignore the current value of this parameter, and treat it as if its value is currently 0);
Tagged-FramesTagging	Specifies the tagging value that Auto-Configuration apply for ports having Auto-Detection enabled and running in Tagged-Frames operational mode.

Displaying ADAC MAC range using ACLI

Display the range of MAC addresses used by ADAC to identify an IP Phone with the MAC detection mechanism.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   show adac mac-range-table
   ```

Displaying ADAC detection method status using ACLI

Display the status of detection mechanism for the device on a specific port.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   show adac detection interface
   ```

Chapter 14: Configuring Link Layer Discovery Protocol (LLDP) using ACLI

This section describes the procedures that are used to configure and display LLDP parameters using ACLI.

Configuring LLDP using ACLI

This section describes how to enable the Link Layer Discovery Protocol (LLDP) with ACLI.

Setting LLDP transmission parameters using ACLI

Configure the LLDP transmission parameters or return the parameters to their default values.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
[default] lldp [tx-interval <5-32768>] [tx-hold-multiplier
<2-10>] [reinitdelay <1-10>] [tx-delay <1-8192>]
[notification-interval <5-3600>] [med-fast-start <1-10>]
```

Variable definitions

The following table describes the parameters for the **`lldp`** command.

Variable	Value
default	Specifies which LLDP parameters you would like to return to their default values when you

Variable	Value
	add one or more of these parameters after the **`default lldp`** command: • tx-interval • tx-hold-multiplier • reinit-delay • tx-delay • notification-interval • med-fast-start If no parameters are specified, the **`default lldp`** command sets all parameters to their default values.
tx-interval *<5–32768*	Sets the interval between successive transmission cycles. DEFAULT: 30
tx-hold-multiplier *<2–10>*	Sets the multiplier for tx-interval used to compute the Time To Live value for the TTL TLV. DEFAULT: 4
reinit-delay *<1–10>*	Sets the delay for re-initialization attempt if the adminStatus is disabled. DEFAULT: 2
tx-delay *<1–8192>*	Sets the minimum delay between successive LLDP frame transmissions. DEFAULT: 2
notification-interval *<5–3600>*	Sets the interval between successive transmissions of LLDP notifications. DEFAULT: 5
med-fast-start *<1–10>*	Sets the vale for MED-Fast-Start. DEFAULT: MED Fast Start repeat count

Enabling or disabling LLDP config notification using ACLI

Enable or disable notification when new neighbor information is stored or when existing information is removed.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
[no] [default] llpd [port <portlist>]config-notification
```

Note:

The command **`lldp config-notification`** is enabled on the switch by default.

Variable definitions

The following table describes the parameters for the **`lldp config-notification`** command.

Variable	Value
no	Disables config notification.
default	Returns config notification to its default value. DEFAULT: Enabled
port <*portlist*>	Specifies the ports affected by the command.

Configuring Optional Management TLVs using ACLI

Sets the optional Management TLVs to be included in the transmitted LLDPDUs

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
[no] [default] lldp tx-tlv [port <portlist>] [local-mgmt-addr] [port-desc] [sys-cap] [sys-desc] [sys-name]
```

Note:

The command **`lldp tx-tlv local-mgmt-addr port-desc sys-desc sys-name`** is enabled on the switch by default.

Variable definitions

The following table describes the parameters for the **`lldp tx-tlv`** command.

Variable	Value
[no]	Specifies the optional TLVs not to include in the transmitted LLDPDUs. The following parameters can be specified: • local-mgmt-addr • port-desc • sys-cap • sys-desc • sys-name
[default]	Sets the LLDP Management TLVs to their default values
port <*portlist*>	Specifies the ports affected by the command
local-mgmt-addr	Local management address TLV DEFAULT: enable— not included
port-desc	Port description TLV DEFAULT: enable — not included
sys-cap	System capabilities TLV DEFAULT: enable — not included
sys-desc	System description TLV DEFAULT: enable — not included
sys-name	System name TLV DEFAULT: enable — not included

Configuring the IEEE 802.3 organizationally-specific TLVs using ACLI

Specify the optional IEEE 802.3 organizationally-specific TLVs to be included in the transmitted LLDPDUs.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
[no] [default] lldp tx-tlv [port <portlist>] dot 3 [link-
aggregation] [mac-phy-config-status] [maximum-frame-size]
[mdi-power-support]
```

Variable definitions

The following table describes the parameters for the **`lldp tx-tlv dot3`** command.

Variable	Value
no	Specifies that the optional IEEE 802.3 organizationally-specific TLVs should not be included in the transmitted LLDPDUs.
default	Sets the optional IEEE 802.3 organizationally-specific TLVs to their default values.
port <*portlist*>	Specifies the port affected by the command
link-aggregation	Sets the link aggregation TLV. DEFAULT: false (not included)
mac-phy-config-size	Sets the MAC/PHY configuration or status TLV DEFAULT: false (not included)
maximum-frame-size	Set the Maximum Frame Size TLV DEFAULT: false (not included)
mdi-power-support	Sets the Power via MDI TLV. Transmission of this TLV is enabled by default only on PoE switch ports. DEFAULT: Enabled

Configuring Optional TLVs for MED Devices using ALCI

Sets the optional organizationally-specific TLVs for use by MED devices to be included in the transmitted LLDPDUs.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
lldp tx-tlv [port <portlist>] med [med-capabilities]
[extendedPSE] [inventory] [location] [network-policy]
```

Note:

The command **`lldp tx-tlv med extendedPSE inventory location med-capabilities network-policy`** is enabled on the switch by default.

Variable definitions

The following table describes the parameters for the **`lldp tx-tlv med`** command.

Variable	Value
port <*portlist*>	Specifies the ports affected by the command
med-capabilities	MED Capabilities TLV (MED TLVs are transmitted only if MED Capabilities TLVs are transmitted). DEFAULT: enabled
extendedPSE	Extended PSE TLV. DEFAULT: enabled
inventory	Inventory TLVs DEFAULT: enabled
location	Location Identification TLV DEFAULT: enabled
network-policy	Network Policy TLV DEFAULT: enabled

Configuring LLDPU Transmit and Receive Status using ACLI

Sets the LLDPU transmit and receive status on ports.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
[no] [default] lldp [port <portlist>] status [rxOnly |
txAndRx | txOnly][config-notification]
```

Note:

The command **`lldp status txAndRx config-notification`** is enabled on the switch by default.

Variable definitions

The following table describes the parameters for the **`lldp status`** command.

Variable	Value
[no]	Disables 802.1AB on ports
[default]	Sets the LLDPU transmit and receive status on specified ports to its default value (txAndRx).
port <*portlist*>	Specifies the ports affected by the command.
rxOnly	Enables LLDPU receive only
txAndRx	Enables LLDPU transmit and receive
txOnly	Enables LLDPU transmit only
config-notification	Enables notification when a new neighbor information is stored or when existing information is removed. DEFAULT: enabled

Displaying Configuration Data for LLDP using ACLI

Displays configuration data for LLDP.

Procedure

1. Log on to ACLI in User Exec command mode.
2. At the command prompt, enter the following command:
   ```
   show lldp [local-sys-data] [mgmt-sys-data] [pdu-tlv-size]
   [stats] [rx-stats] [tx-stats] [tx-tlv] [neighbor] [neighbor-
   mgmt-addr]
   ```

Variable definitions

The following table describes the parameters for the **`show lldp`** command.

Variable	Value
local-sys-data	Displays 802.1AB local system data

Variable	Value
mgmt-sys-data	Displays 802.1AB management data
neighbor	Displays 802.1AB neighbors
neighbor-mgmt-addr	Displays 802.1AB neighbors management addresses
pdu-tlv-size	Displays 802.1AB tlv in pdu
port<*portlist*>	Specifies the ports affected by the command
rx-stats	Displays 802.1AB RX statistics
stats	Displays LLDP statistics
tx-stats	Displays 802.1AB TX statistics
tx-tlv	Displays 802.1AB TLVs

Displaying Configuration Data for LLDP Ports using ACLI

Display configuration data for LLDP ports.

Procedure

1. Log on to ACLI in User Exec command mode.
2. At the command prompt, enter the following command:
   ```
   show lldp [port <portlist>] [neighbor] [neighbor-mgmt-addr]
   [local-sys-data] [rx-stats] [tx-stats] [tx-tlv]
   ```

Example

The following figure provides a sample output from the **`show lldp port neighbor`** command showing ALL ports.

```
3524GT-PWR+>show lldp port ALL neighbor
-----------------------------------------------------------------------
                      LLDP neighbor
-----------------------------------------------------------------------
Port: 2   Index: 2                Time: 0 days, 00:00:58
     ChassisId : MAC address      00:16:ca:da:c4:00
     PortId:     MAC address      00:16:ca:da:c4:30
     SysCap:     rB / B           <Supported/Enabled>
     PortDesc:   Port 48
     SysDescr:
Ethernet Routing Switch 4548GT-PWR   HW:0B  FW:5.3.0.0  SW:v5.6.0.0.009
------------------------------------------------------------------------
Port: 2   Index: 3                Time: 0 days, 00:01:02
     ChassisId : MAC address      00:16:ca:da:c4:00
     PortId:     MAC address      00:16:ca:da:c4:0d
     SysCap:     rB / B           <Supported/Enabled>
     PortDesc:   Port 13
     SysDescr:
Ethernet Routing Switch 4548GT-PWR   HW:0B  FW:5.3.0.0  SW:v5.6.0.0.009
```

```
------------------------------------------------------------------------
Port: 2   Index: 4                Time: 0 days, 00:01:03
     ChassisId : MAC address      00:16:0e:9d:28:01
     PortId:     MAC address      00:16:0e:9d:28:19
     SysCap:     rB / B           <Supported/Enabled>
     PortDesc:   Unit 1 Port 24
     SysDescr:
Ethernet Routing Switch 2526T       HW:02  FW:1.0.0.15  SW:v4.4.0.010
------------------------------------------------------------------------
------More   (q=Quit, space/return=Continue)----
```

The following figure provides a sample output from the **show lldp port neighbor-mgmt-addr** command using Ports 1–3.

```
3524GT-PWR+>show lldp port 1-3 neighbor
-----------------------------------------------------------------------
                      LLDP neighbor-mgmt-addr
-----------------------------------------------------------------------
Port: 2   Index: 2                Time: 0 days, 00:00:58
     ChassisId : MAC address      00:16:ca:da:c4:00
     PortId:     MAC address      00:16:ca:da:c4:30
     MgmtAddr:   IPv4 172.16.120.67
     MgmtOID:    1.3.6.1.4.1.45.3.71.2
     Interface:  type-unknown, number:0
------------------------------------------------------------------------
Port: 2   Index: 3                Time: 0 days, 00:01:02
     ChassisId : MAC address      00:16:ca:da:c4:00
     PortId:     MAC address      00:16:ca:da:c4:0d
     MgmtAddr:   IPv4 172.16.120.67
     MgmtOID:    1.3.6.1.4.1.45.3.71.2
     Interface:  type-unknown, number:0

------------------------------------------------------------------------
Port: 2   Index: 4                Time: 0 days, 00:01:03
     ChassisId : MAC address      00:16:0e:9d:28:01
     PortId:     MAC address      00:16:0e:9d:28:19
    MgmtAddr:   IPv4 192.167.130.230
------More   (q=Quit, space/return=Continue)----
```

Important:

To display the neighbor management addresses using the **show lldp port neighbor-mgmt-addr** command, you must configure the connected port of the neighbor to transmit local management address **(lldp tx-tlv [port <portlist>] local-mgmt-addr).**

The following figure provides a sample output from the **show lldp rx-stats** command.

```
3524GT-PWR+>show lldp rx-stats
------------------------------------------------------------------------
                            LLDP rx-stats
------------------------------------------------------------------------
------------------------------------------------------------------------
Port    Frames        Frames     Frames  TLVs      TLVs           AgeOuts
Num     Discarded     Errors      Total  Discarded Unrecognized
------------------------------------------------------------------------
1               0          0          0          0          0           0
2               0          0       2944          0       1105           0
3               0          0          0          0          0           0
4               0          0          0          0          0           0
5               0          0          0          0          0           0
6               0          0          0          0          0           0
```

```
7               0          0          0          0          0           0
8               0          0          0          0          0           0
9               0          0          0          0          0           0
10              0          0          0          0          0           0
11              0          0          0          0                      0
12              0          0          0          0          0           0
13              0          0          0          0          0           0
14              0          0          0          0          0           0
15              0          0          0          0          0           0
----More (q=Quit, space/return=Continue)----
```

The following figure provides a sample output from the **show lldp tx-stats** command.

```
3524GT-PWR+>show lldp tx-stats
------------------------------------------------------------------------
                            LLDP tx-stats
------------------------------------------------------------------------
------------------------------------------------------------------------
Port        Frames
------------------------------------------------------------------------
1                0
2              378
3                0
4                0
5                0
6                0
7                0
8                0
9                0
10               0
11               0
12               0
13               0
14               0
15               0
16               0
----More (q=Quit, space/return=Continue)----
```

The following figure provides a sample output from the **show lldp tx-tlv** command.

```
3524GT-PWR+>show lldp tx-tlv
------------------------------------------------------------------------
                            LLDP port tlvs
------------------------------------------------------------------------
------------------------------------------------------------------------
Port  PortDesc SysName  SysDesc  SysCap   MgmtAddr
------------------------------------------------------------------------
1      true     true     true     true     true
2      true     true     true     true     true
3      true     true     true     true     true
4      true     true     true     true     true
5      true     true     true     true     true
6      true     true     true     true     true
7      true     true     true     true     true
8      true     true     true     true     true
9      true     true     true     true     true
10     true     true     true     true     true
11     true     true     true     true     true
12     true     true     true     true     true
13     true     true     true     true     true
14     true     true     true     true     true
15     true     true     true     true     true
16     true     true     true     true     true
----More (q=Quit, space/return=Continue)----
```

Variable definitions

The following table describes the parameters for the **`show lldp`** command.

Variable	Value
port <*portlist*>	Specifies the ports affected by the command
neighbor	Displays LLDP neighbors
neighbor-mgmt-addr	Displays LLDP management addresses for neighbors
local-sys-data	Displays 802.1AB management data
rx-stats	Displays LLDP receive statistics
tx-stats	Displays LLDP transmit statistics
tx-tlv	Displays LLDP transmit TLVs

Configuring Autotopology

This section describes how to configure and display Autotopology using ACLI.

Configuring Autotopology using ACLI

You can configure the Optivitiiy* Autotopology* protocol with ACLI.

Procedure

1. Log on to ACLI in Global Configuraiton command mode.
2. At the command prompt, enter the following command:

```
[no] [default] autotopology
```

Variable definitions

The following table describes the parameters for the **`autotopology`** command.

Variable	Value
no	Disables Autotopology on the switch

Variable	Value
default	Returns Autotopology setting on the switch to the default setting. DEFAULT: Enabled

Displaying Autotopology settings using ACLI

Display information about the Autotopology configuration.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show autotopology settings
   ```

Example

The following figure provides a sample output of the **show autotopology settings** command.

```
3524GT-PWR+#show autotopology settings
Autotopology:  Enabled
Last NMM Table Change:  0 days, 03:11:08
Maximum NMM Table Entries:  100
Current NMM Table Entries:  2
3524GT-PWR+#
```

Configuring the PoE conservation level request TLV using ACLI

Request a specific power conservation level for an Avaya IP phone connected to a switch port.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   lldp [port <portlist>] vendor-specific avaya poe-conservation-request-level <0–255>
   ```

3. To reset the PoE conservation level TLVs for connected Avaya IP phones to the default value, enter the following command:

```
[default] [port <portlist>] lldp vendor-specific avaya poe-
conservation-request-level
```

Important:

Only Ethernet ports on switches that support PoE can request a specific power conservation level for an Avaya IP phone.

Variable definitions

The following table describes the parameters for the **`lldp vendor-specific avaya poe – conservation- request-level`** command.

Variable	Value
<0–255>	Specifies the power conservation level to request for a vendor specific PD. With the default value, the switch does not request a power conversation level for an Avaya IP phone connected to the port. RANGE: 0 to 255 DEFAULT: 0
port <*portlist*>	Specifies a port or list of ports

Displaying the Switch PoE Conservation Level Request TLV Configuration using ACLI

Display PoE conservation level request configuration for local switch ports.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show lldp [port <portlist>] vendor-specific avaya poe-
   conservation-request-level
   ```

Example

The following figure provides a sample of the **`show lldp vendor-specific avaya poe-conservation-request-level`** command.

```
3524GT-PWR+#show lldp vendor-specific avaya poe-conservation-request-level
------------------------------------------------------------------------
```

```
              LLDP vendor-specific Avaya POE Request Conservation Level
------------------------------------------------------------------------
------------------------------------------------------------------------
      Unit/       POE Request
      Port          Level
------------------------------------------------------------------------
      1             0
      2             0
      3             0
      4             0
      5             0
      6             0
      7             0
      8             0
      9             0
      10            0
      11            0
      12            0
      13            0
      14            0
      15            0
----More (q=Quit, space/return=Continue)----
```

Variable definitions

The following table describes the parameters for the **show lldp** command.

Variable	Value
port <*portlist*>	Specifies a port or list of ports

Displaying PoE Conservation Level Support TLV Information using ACLI

Display PoE conservation level information received on switch ports from an Avaya IP phone.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   show lldp [port <portlist>] neighbor vendor-specific avaya
   poe-conservation
   ```

Configuring the Switch Call Server IP Address TLV using ACLI

Define the local call server IP addresses that switch ports advertise to Avaya IP phones.

You can define IP addresses for a maximum of 8 local call servers.

Important:

The switch does not support the advertisement of IPv6 addresses to Avaya IP phones

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   lldp vendor-specific avaya call-server [<1-8>] <A.B.C.D>
   [[<1-8>] <A.B.C.D>] [[<1–8>] <A.B.C.D>]
   ```
3. Delete call server IPv4 addresses configured on the switch by using the following command:
   ```
   default lldp vendor-specific avaya call server <1–8>
   ```

Variable definitions

The following table describes the parameters for the **`lldp vendor-specific avaya call-server`** command.

Variable	Value
<1–8>	Specifies the call server number. **Note:** When you advertise the IPv4 address of call server 1 only, you do not have to enter a call server number before you enter the IP address.
<A.B.C.D>	Specifies the call server IPv4 address

Displaying the Switch Call Server IP Address TLV Configuration using ACLI

Display information about the defined local call server IP address that switch ports advertise to connected Avaya IP phones.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   `show lldp vendor-specific avaya call-server`

Example

The following figure provides a sample of the **`show lldp vendor-specific avaya call-server`** command.

```
3524GT-PWR+>enable
3524GT-PWR+#show lldp vendor-specific avaya call-server
------------------------------------------------------------------------
                     LLDP Avaya Call Servers IP addresses
------------------------------------------------------------------------
------------------------------------------------------------------------
 Avaya Configured Call Server 1: 10.10.10.4
 Avaya Configured Call Server 2: 10.10.10.1
 Avaya Configured Call Server 3: 10.10.10.2
 ------------------------------------------------------------------------
3524GT-PWR+#
```

Displaying Avaya IP Phone Call Server IP Address TLV Information using ACLI

Display call server IP address information received on switch ports from an Avaya IP phone.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   `show lldp [port <portlist>] neighbor vendor-specific avaya call-server`

Variable definitions

The following table describes the parameters for the **`show lldp neighbor vendor-specific avaya call-server`** command.

Variable	Value
port <*portlist*>	Specifies a port or list of ports

Configuring the Switch File Server IP Address TLV using ACLI

Define the local file server IP addresses that switch ports advertise to Avaya IP phones.

You can define IP addresses for a maximum of 4 local file servers.

Note:

If your Avaya IP Handset uses SIP, 802.1AB (LLDP) TLVs do not provide all information for the IP Phone. You must specify a file server IP address TLV so the IP phone can download the SIP configuration information, because the IP Phone retrieves information related to the SIP domain, port number and transport protocol from the file server.

Important:

The switch does not support the advertisement of IPv6 addresses to Avaya IP phones.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   lldp vendor-specific avaya file-server [<1–4>] <A.B.C.D>
   [[<1–4>] <A.B.C.D>] [[<1–4>] <A.B.C.D>]
   ```
3. Delete file server IPv4 addresses configured on the switch by using the following command:
   ```
   default lldp vendor-specific avaya file server <1–4>
   ```

Variable definitions

The following table describes the parameters for the **`lldp vendor-specific avaya file-server`** command.

Variable	Value
<1–4>	Specifies the file server number **Note:** When you advertise the IPv4 address of file server 1 only, you do not have to enter a file server number before you enter the IP address.
<A.B.C.D>	Specifies the file server IPv4 address

Displaying the Switch File Server IP Address TLV Configuration using ACLI

Display information about the defined local file server IP address that switch ports advertise to connected Avaya IP phones.

You can define IP addresses for a maximum of 4 local servers.

Important:

The switch does not support the advertisement of IPv6 addresses to Avaya IP phones.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

```
show lldp vendor-specific avaya file-server
```

Displaying Avaya IP Phone File Server IP Address TLV Information using ACLI

Display information about file server IP address received on switch ports from Avaya IP phones.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show lldp [port <portlist>] neighbor vendor-specific avaya
   file-server
   ```

Variable definitions

The following table describes the parameters for the **show lldp neighbor vendor-specific avaya file-server** command.

Variable	Value
port <*portlist*>	Specifies a port or list of ports

Configuring the 802.1Q Framing TLV using ACLI

Configure the frame tagging mode for exchanging Layer 2 priority tagging information between the switch and an Avaya IP phone.

Before you begin

- Enable LLDP MED capabilities.
- Enable LLDP MED network policies.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
lldp {port <portlist>] vendor-specific avaya dotlq-framing
[tagged | non-tagged | auto]
```

3. Set the Layer 2 frame tagging mode to default by using the following command:

```
default lldp [port <portlist>] vendor-specific avaya dotlq-
framing
```

Variable definitions

The following table describes the parameters for the **`lldp vendor-specific avaya dotlq-framing`** command.

Variable	Value
port *<portlist>*	Specifies a port or list of ports
[tagged | non-tagged | auto]	Specifies the frame tagging mode. Values include: • tagged — frames are tagged based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. • non-tagged — frames are not tagged with 802.1Q priority. • auto — an attempt is made to tag frames based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. If there is no LLDP-MED Network Policy information available, an attempt is made to tag frames based on server configuration. If that fails, traffic is transmitted untagged. DEFAULT: auto

Displaying the Switch 802.1Q Framing TLV Configuration using ACLI

Display the configured Layer 2 frame tagging mode for switch ports.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.

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

   ```
   show lldp [port <portlist>] vendor-specific avaya dotlq-framing
   ```

Variable definitions

The following table describes the parameters for the **`show lldp vendor-specific avaya dotlq-framing`** command.

Variable	Value
port <*portlist*>	Specifies a port or list of ports

Displaying Avaya IP Phone 802.1Q Framing TLV Information using ACLI

Display Layer 2 frame tagging mode information received on switch ports from connected Avaya IP phones.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show lldp [port <portlist>] neighbor vendor-specific avaya dotlq-framing
   ```

Variable definitions

The following table describes the parameters for the **`show lldp neighbor vendor-specific avaya dotlq-framing`** command.

Variable	Value
port <*portlist*>	Specifies a port or list of ports

Enabling Or Disabling Avaya Transmit Flag Status using ACLI

Enable or disable the transmission of optional proprietary Avaya TLVs from switch ports to Avaya IP phones.

Important:

The switch transmits configured Avaya TLVs only on ports with the TLV transmit flag enabled.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
[no] [default] lldp tx-tlv [port <portlist>] vendor-specific
avaya {[poe—conservation] [call-server] [file-server]
[dotlq-framing]}
```

Variable definitions

The following table describes the parameters for the **lldp tx-tlv vendor-specific avaya** command.

Variable	Value
[no]	Disables the transmission of optional proprietary Avaya TLVs from switch ports to Avaya IP phones.
[default]	Sets the TLV transmit flag to the default value of true. DEFAULT: enabled
call-server	Enables the call server TLV transmit flag
dot1q-framing	Enables the Layer 2 priority tagging TLV transmit flag
file-server	Enables the file server TLV transmit flag
poe-conservation	Enables the PoE conservation request TLV transmit flag

Variable	Value
port <*portlist*>	Specifies a port or list of ports

Displaying Avaya TLV Transmit Flag Status using ACLI

Display the status of transmit flags for switch ports on which Avaya IP phone support TLVs are configured.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   `show lldp [port <portlist>] tx-tlv vendor-specific avaya`

Example

The following figure provides a sample of the **`show lldp tx-tlv vendor-specific avaya`** command.

```
3524GT-PWR+#show lldp tx-tlv vendor-specific avaya
------------------------------------------------------------------------
                 LLDP port Avaya Vendor-Specific TLVs
------------------------------------------------------------------------
------------------------------------------------------------------------
      Unit/    POE Conservation   Call-Server   File-Server Dot1Q-Framing
      Port        Request
------------------------------------------------------------------------
      1           true           true           true           true
      2           true           true           true           true
      3           true           true           true           true
      4           true           true           true           true
      5           true           true           true           true
      6           true           true           true           true
      7           true           true           true           true
      8           true           true           true           true
      9           true           true           true           true
      10          true           true           true           true
      11          true           true           true           true
      12          true           true           true           true
      13          true           true           true           true
      14          true           true           true           true
      15          true           true           true           true
----More (q=Quit, space/return=Continue)----
```

Variable definitions

The following table describes the parameters for the **`show lldp tx-tlv vendor-specific avaya`** command.

Variable	Value
port <*portlist*>	Specifies a port or list of ports

Displaying Avaya IP Phone IP TLV Configuration using ACLI

Displays IP address configuration information received on switch ports from connected Avaya IP phones.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   `show lldp [port <portlist>] neighbor vendor-specific avaya phone-ip`

Example

The following figure provides a sample output from the **`show lldp port neighbor vendor-specific avaya phone-ip`** command.

```
3526T-PWR+(config)#show lldp port 5 neighbor vendor-specific avaya phone-ip
-------------------------------------------------------------------------------
                       Neighbors LLDP info - Avaya TLVs
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Port: 5
   Avaya Phone IP:
      Address: 192.168.70.35
      Netmask: 255.255.255.0
      Gateway: 0.0.0.0
```

Variable definitions

The following table describes the parameters for the **`show lldp neighbor vendor-specific avaya phone-ip`** command.

Variable	Value
port <*portlist*>	Specifies a port or list of ports

Chapter 15: Configuring VLANs using Enterprise Device Manager

This chapter describes how to use Enterprise Device Manager (EDM) to manage VLANs on your Ethernet Routing Switch 3500 Series. This chapter covers creating, editing, and deleting VLANs.

Use Enterprise Device Manager to manage VLANs on your Ethernet Routing Switch 3500 Series.

VLANs

A VLAN is a collection of ports on one or more switches that define a broadcast domain. The Ethernet Routing Switch 3500 Series supports port-based and IPv6 protocol-based VLANs.

When you create VLANs using Enterprise Device Manager, observe the following rules:

- The ports in a VLAN or Multi-Link trunk must be a subset of a Single Spanning Tree Group.
- VLANs must have unique VLAN IDs and names.

VLAN management using EDM

Use procedures in this section to view, create, and manage VLAN configuration for a switch.

Displaying VLAN information using EDM

Use this procedure to view the VLAN configuration information for a switch.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To display IP address information for a VLAN, click the **VLAN ID**.
5. Click the **IP** button.
6. To display IPv6 address information for a VLAN, click the **VLAN ID**.
7. Click the **IPv6** button.

VLAN display field descriptions

The following table describes the fields in the VLAN display.

Name	Description
Id	Indicates the VLAN ID for the VLAN.
Name	Indicates the name of the VLAN.
Ifindex	Indicates the interface index. This is a read-only value.
Type	Indicates the type of VLAN. Values include: • **byPort**: VLAN by port • **byProtocolId**: VLAN by protocol ID
PortMembers	Indicates the ports that are members of the VLAN.
StgId	Indicates the Spanning Tree Group to which the selected port(s) belongs. ❗ **Important:** This column is available only when the switch is operating in STPG mode. Ethernet Routing Switch 3500 Series does not support multiple STGs when operating in the STPG mode.
ProtocolId	Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is byProtocolId; otherwise the protocol ID value is none (0). Values include: • 0 • ipV6
UserDefinedPid	Indicates the user defined protocol identifier for a protocol-based VLAN.
MstpInstance	Indicates the MSTP instance associated with the VLAN. Values include: • none • cist • msti 1–7

Name	Description
	❗ **Important:** This column is available only when the switch is operating in the MSTP mode.
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 STPG mode using EDM

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

Procedure

1. In 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. On the toolbar, click **Apply**.

VLAN in STPG mode field descriptions

The following table describes the fields on the VLAN in STPG mode tab.

Name	Description
Id	Indicates the VLAN 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. Values include: • **byPort**: VLAN by port • **byProtocolId**: VLAN by protocol ID This is a read-only value.
PortMembers	Specifies the ports that are members of the VLAN.
StgId	Indicates the Spanning Tree Group to which the selected port or ports belong. This is a read-only value. **Important:** This column is available only when the Spanning Tree administration operating mode is avayaStpg. The switch does not support multiple STGs when operating in the STPG mode. **Important:** When the Spanning Tree administration operating mode is RSTP, this column is not available.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Indicates 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.

Procedure

1. In 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. On the toolbar, click **Apply**.

VLAN in RSTP mode field descriptions

The following table describes the fields for VLAN in RSTP mode..

Name	Description
Id	Indicates the VLAN 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.

Name	Description
Type	Indicates the type of VLAN. Values include: • **byPort**: VLAN by port • **byProtocolId**: VLAN by protocol ID This is a read-only value.
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.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Indicates 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.

Procedure

1. In 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. On the toolbar, click **Apply**.

VLAN in MSTP mode field descriptions

The following table describes the fields for VLAN in MSTP mode.

Name	Description
Id	Indicates the VLAN 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. Values include: • **byPort**: VLAN by port • **byProtocolId**: VLAN by protocol ID This is a read-only value.
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	Indicates 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.

Name	Description
	Important: When the Spanning Tree administration operating mode is RSTP, this column is not available.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Indicates whether routing is enabled (true) or disabled (false) for the VLAN.

Creating a VLAN in STP mode using EDM

Use this procedure to create a new VLAN when the switch is in STP mode.

Before you begin

Select avayaStpg for the Spanning Tree administration mode.

Procedure

1. In 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 **VLAN ID** field, type a value.
   OR

   Accept the default ID for the VLAN.
6. In the **Name** field, type a value.
   OR

   Accept the default name for the VLAN.
7. In the **Type** field, select **byPort** or **byProtocolId**.
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 **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. On the toolbar, click **Apply**.

VLAN in STP mode field descriptions

The following table describes the fields to create VLANs in STP mode.

Name	Description
Id	Specifies the VLAN 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 protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is by ProtocolID. The only supported value is ipv6.
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	Indicates the Spanning Tree Group to which the selected port or ports belong. This is a read-only value. **Important:** This column is available only when the Spanning Tree administration operating mode is avayaStpg. The switch does not support multiple STGs when operating in the STPG mode. **Important:** When the Spanning Tree administration operating mode is RSTP, this column is not available.

Name	Description
ProtocolId	Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is byProtocolId; otherwise the protocol ID value is none (0). Values include: • 0 • ipV6
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Indicates whether routing is enabled (true) or disabled (false) for the VLAN.

Creating a VLAN in RSTP mode using EDM

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

Before you begin

Select RSTP for the Spanning Tree administration mode.

Procedure

1. In 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** field, type a value.

   OR

   Accept the default ID for the VLAN.
6. In the **Name** field, type a value.

   OR

   Accept the default name for the VLAN.
7. In the **Type** field, select **byPort** or **byProtocolId**.
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 **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. On the toolbar, click **Apply**.

VLAN in RSTP mode field descriptions

The following table describes the fields to create a VLAN in RSTP mode.

Name	Description
Id	Specifies the VLAN 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 protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is by ProtocolID. The only supported value is ipv6.
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	Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is byProtocolId; otherwise the protocol ID value is none (0). Values include: • 0 • ipV6
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN.

Name	Description
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Indicates whether routing is enabled (true) or disabled (false) for the VLAN.

Creating a VLAN in MSTP mode using EDM

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

Before you begin

Select MSTP for the Spanning Tree administration mode.

Procedure

1. In 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** field, select **byPort** or **byProtocolId**.
8. Click the **MstpInstance** box arrow.
9. Select a value from the list.
10. Click **Insert**.
11. In the VLAN row, double-click the cell in the **PortMembers** column.
12. Select ports to add to the VLAN.
    OR

    Deselect ports to remove them from the VLAN.
13. Click **Ok**.
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. On the toolbar, click **Apply**.

VLAN in MSTP mode field descriptions

The following table describes the fields to create a VLAN in MSTP mode.

Name	Description
Id	Indicates 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 protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is byProtocolId. The only supported value is ipv6.
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	Indicates theprotocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is byProtocolId; otherwise the protocol ID value is none (0). Values include: • 0 • ipv6
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN.
MstpInstance	The MSTP instance associated with the VLAN. Values include: • none • cist • msti 1–7

Name	Description
	Important: This column is available only when the Spanning Tree administration operating mode is MSTP. **Important:** When the Spanning Tree administration operating mode is RSTP, this column is not available.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Indicates whether routing is enabled (true) or disabled (false) for the VLAN.

Deleting a VLAN using EDM

Use this procedure to delete a VLAN.

Procedure

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

VLAN configuration for ports using EDM

Use the information in this section to view and configure VLAN membership for specific ports.

Displaying VLAN membership port information using EDM

Use this procedure to display the VLAN membership information for switch ports.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **VLANs**.
3. Click the **Ports** tab.

VLAN port membership field descriptions

The following table describes the fields to help you understand the VLAN port membership.

Name	Description
Index	Indicates the switch position in the stack and the port number. This is read-only value. ✱ **Note:** Stacking is not available in Release 5.0.
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.
FilterUnregisteredFrames	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. RANGE: 0 to 7

Name	Description
Tagging	Indicates 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.

Configuring VLAN membership ports using EDM

Use this procedure to configure VLAN membership for one or more switch ports.

Procedure

1. In 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 **FIlterUnregisteredFrames** 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. Repeat steps 5 through 15 to configure VLAN memberships for additional ports.

16. On the toolbar, click **Apply**.

VLAN Membership ports field descriptions

The following table describes the fields to configure VLAN membership ports.

Name	Description
Index	Indicates the switch position in the stack and the port number. This is read-only value. ✱ **Note:** Stacking is not available in Release 5.0.
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.
FilterUnregisteredFrames	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. RANGE: 0 to 7
Tagging	Indicates the type of VLAN port. Possible values are: • **untagAll (access)** • **tagAll (trunk)** • **untagPvidOnly** • **tagPvidOnly**

Name	Description
	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 this procedure to select configuration control for a VLAN.

Procedure

1. In 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**.

VLAN configuration control field descriptions

The following table describes the fields used to set VLAN configuration control.

Name	Description
ManagementVlanID	Specifies the identifier of the management VLAN. RANGE: 1 to 4094.
VlanConfigControl	VlanConfigControl presents four selections: • **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 new 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

Name	Description
	involved are in the same Spanning Tree Group • **autopvid**: When an untagged port is added to a new VLAN, the port is added to the new VLAN and the PVID is 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. Any new additions of an untagged port to a new VLAN do 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 a new VLAN. The PVID of the port is changed to the new VID to which it was added.

Port configuration for VLANs using EDM

Use the information in this section to view and configure specific ports for VLAN membership.

Displaying port VLAN membership information using EDM

Use this procedure to display the VLAN membership information for switch ports.

Procedure

1. In 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.

Port VLAN membership information field descriptions

The following table describes the fields used to display VLAN membership information.

Name	Description
Index	Indicates the switch position in the stack and the port number. This is read-only value. ✱ **Note:** Stacking is not available in Release 5.0.
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.
FilterUnregisteredFrames	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. RANGE: 0 to 7
Tagging	Indicates the type of VLAN port. Possible values are: • **untagAll (access)** • **tagAll (trunk)**

Name	Description
	• **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 ports for VLAN membership using EDM

Use this procedure to configure one or more switch ports for VLAN membership.

Procedure

1. In 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.
5. To select a port to edit, click the port row.
6. In the port row, double-click the cell in the **DiscardUntaggedFrames** column.
7. Select a value from the list — **true** to discard untagged frames for the port, or **false** to accept untagged frames for the port.
8. In the port row, double-click the cell in the **FIlterUnregisteredFrames** column.
9. Select a value from the list — **true** to discard unregistered frames for the port, or **false** to process unregistered frames normally for the port.
10. In the port row, double-click the cell in the **DefaultVlanId** column.
11. Type a value for the default VLAN ID.
12. In the port row, double-click the cell in the **PortPriority** column.
13. Select a value from the list.
14. In the port row, double-click the cell in the **Tagging** column.
15. Select a value from the list.
16. Repeat steps 5 through 15 to configure VLAN memberships for additional ports.
17. On the toolbar, click **Apply**.

Configure ports for VLAN membership field descriptions

The following table describes the fields to configure ports for VLAN membership

Name	Description
Index	Indicates the switch position in the stack and the port number. This is read-only value. ✱ **Note:** Stacking is not available in Release 5.0.
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.
FilterUnregisteredFrames	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. RANGE: 0 to 7
Tagging	Indicates 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

Name	Description
	is an access port, the port can only be a member of one VLAN.

MAC address table management using EDM

This section describes how to manage the MAC address table by clearing entries.

Important:

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

Flushing the MAC address table using EDM

Use this procedure to flush the MAC address table to clear all addresses in the MAC address table.

Procedure

1. In the navigation tree, double-click **Edit** to open the Edit navigation tree.
2. Double-click **Bridge** to open the Bridge work area.
3. Select the **Mac Flush** tab.
4. To clear all MAC address table entries, select the **FlushMacAddrTableAll** check box.
5. On the toolbar, click **Apply**.

Flushing the MAC address table for a FastEthernet interface using EDM

Use this procedure to flush the MAC address table for a FastEthernet interface to clear the MAC address table for specified interface ports.

Procedure

1. In the navigation tree, double-click **Edit** to open the Edit navigation tree.
2. Double-click **Bridge** to open the Bridge work area.

3. Select the **Mac Flush** tab.
4. Click the **FlushMacAddrTableByPortList** elipsis (...).
5. Select interface ports for which to clear MAC address table entries.
6. Click **Ok**.
7. On the toolbar, click **Apply**.

Flushing the MAC address table for a VLAN using EDM

Use this procedure to flush the MAC address table for a VLAN to clear all MAC addresses for a specific VLAN.

Procedure

1. In the navigation tree, double-click **Edit** to open the Edit navigation tree.
2. Double-click **Bridge** to open the Bridge work area.
3. Select the **Mac Flush** tab.
4. Type a VLAN ID for which to clear the MAC address table in the **FlushMacAddrTableByVlan** box.
5. On the toolbar, click **Apply**.

MAC Flush tab field descriptions

The following table describes the fields on the MAC Flush tab.

Name	Description
FlushMacAddrTableByVlan	Specifies the VLAN ID. RANGE: 1 to 4094

Flushing the MAC address table for a trunk using EDM

Use this procedure to flush the MAC address table for a trunk to clear all MAC addresses for members of a multi-link trunk.

Procedure

1. In the navigation tree, double-click **Edit** to open the Edit navigation tree.

2. Double-click **Bridge** to open the Bridge work area.
3. Select the **Mac Flush** tab.
4. Type a trunk number for which to clear the MAC address table in the **FlushMacAddrTableByTrunk** box.
5. On the toolbar, click **Apply**.

MAC Flush field descriptions

The following table describes the fields on the MAC Flush tab.

Name	Description
FlushMacAddrTableByTrunk	Specifies the multi-link trunk. RANGE: 1 to 6

Flushing a single MAC address table entry using EDM

Use this procedure to flush a single MAC address table entry to clear one MAC address from the MAC address table.

Procedure

1. In the navigation tree, double-click **Edit** to open the Edit navigation tree.
2. Double-click **Bridge** to open the Bridge work area.
3. Select the **Mac Flush** tab.
4. Type a MAC address in the **FlushMacAddrTableByAddress** box.
5. On the toolbar, click **Apply**.

MAC Flush field descriptions

The following table describes the fields on the MAC Flush tab.

Name	Description
FlushMacAddrTableByAddress	Specifies a MAC address. DEFAULT: 00:00:00:00:00:00.

Chapter 16: Configuring Spanning Tree Groups using Enterprise Device Manager

This chapter describes using Enterprise Device Manager (EDM) to manage Spanning Tree Groups (STGs) on your Ethernet Routing Switch 3500 Series . It also discusses Rapid Spanning Tree Protocol (RSTP), and the Multiple Spanning Tree Protocol (MSTP).

Changing the Spanning Tree mode using EDM

Use this procedure to change the Spanning Tree mode for the Ethernet Routing Switch 3500 Series.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree navigation tree, double-click **Globals**.
4. In the **SpanningTreePortMode** section, click a radio button.
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. Reset the switch.

   For information about how to reset the switch, see Resetting the switch using EDM on page 198.
8. Rediscover the switch.

   For information about how to rediscover the switch, see Rediscovering the switch using EDM on page 198.

Resetting the switch using EDM

Use this procedure to reset the switch.

Procedure

1. In 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 ReBoot section, click the **reboot** radio button.
6. On the toolbar, click **Apply**.

Note:

The rebooting process can take several minutes.

Rediscovering the switch using EDM

Use this procedure to rediscover the switch after performing the switch reset procedure.

Procedure

1. In the navigation tree, double-click **Device**.
2. Double-click **Rediscover Device**.

Note:

The rediscover process can take several minutes.

Configuring STP BPDU Filtering using EDM

Use this procedure to configure STP BPDU Filtering.

Procedure

1. In 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. In the table, double-click a cell under the column heading for the parameter you want to change.
6. Select a parameter or value from the list.
7. Repeat the previous two steps until you have amended all of the parameters you want to change.
8. On the toolbar, click **Apply**.

STP BPDU-Filtering field descriptions

The following table describes the fields on the STP BPDU-Filtering tab.

Name	Description
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 • **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 time is disabled if this value is set to 0. DEFAULT: 12000 (120 seconds)
TimeCount	Displays the time remaining for the port to stay in the disabled state after receiving a BPDU.

Spanning Tree Group configuration using EDM

Use the information in this section to configure and manage a Spanning Tree Group (STG).

Configuring STG globally using EDM

Use this procedure to configure Spanning Tree Group (STG) globally to select the STG configuration for the switch.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **STG** to open the STG work area.
4. Select the **Globals** tab.
5. Select a **SpanningTreePathCostCalculationMode** radio button.
6. Select a **SpanningTreePortMode** radio button.
7. Select or clear the **port802dot1dLearning** check box as required.
8. On the toolbar, click **Apply**.

Globals field descriptions

The following table describes the fields on the Globals tab.

Name	Description
SpanningTreePathCostCalculationMode	Indicates the current spanning-tree path cost calculation mode. Values include: • ieee802dot1dCompatible • ieee802dot1tCompatible The value ieee802dot1dCompatible is valid only after the switch is running in Avaya STPG mode.

Name	Description
SpanningTreePortMode	Specifies the STP port mode. Values include: • normal • auto
SpanningTreeAdminCompatibility	Specifies the STP compatibility mode for various features. If port802dot1dLearning is selected, the port goes to a Disabled state when the port operational status fails. If port802dot1dLearning is not selected, the port remains in the Forwarding state when the port operational status fails.
SpanningTreeOperCompatibility	Indicates the STP compatibility mode for various features if applicable.

Displaying STG configuration general information using EDM

Use this procedure to view general information for the Spanning Tree Group.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **STG** to open the STG work area.
4. Select the **Configuration** tab.

Configuration field descriptions

The following table describes the fields on the Configuration tab.

Name	Description
Id	Identifies an STG in the device.
BridgeAddress	Identifies the MAC address used by a bridge. Avaya recommends that the number has to be the smallest MAC address of all ports belonging to the bridge. However, it is only required to be unique. When concatenated with Priority, a unique bridge identifier is formed that is used in the Spanning Tree Protocol.

Name	Description
NumPorts	Identifies the number of ports controlled by this bridging entity.
ProtocolISpecification	Specifies the version of the spanning tree protocol being run. Values include: • **decLb100**: Indicates the DEC LANbridge 100 Spanning Tree Protocol. • **ieee8021d**: IEEE802.1d implementations will return this entity. 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	Specifies the value of the writable portion of the bridge ID. That is, the first two octets of the (8–octet long) bridge ID. The last six octets of the bridge ID are given by the value of BridgeAddress.
BridgeMaxAge	Specifies the value, in units of hundredths of a second, that all bridges use for the maximum age of a bridge when it is acting as the root. **Important:** 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error can be returned if the value set is not a whole number.
BridgeHelloTime	Specifies the value, in units of hundredths of a second, that all bridges use for HelloTime when a bridge is acting as the root. **Important:** The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error can be returned if the value set is not a whole number.
BridgeForwardDelay	Specifies the value, in units of hundredths of a second, that all bridges use for ForwardDelay when this bridge is acting as the root.

Name	Description
	Important: 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error can be returned if the value set is not a whole number.

Displaying STG status information using EDM

Use this procedure to view STG status information.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **STG** to open the STG work area.
4. Select the **Status** tab.

Status field descriptions

The following table describes the fields on the Status tab.

Name	Description
Id	Identifies an STG in the device.
BridgeAddress	Identifies the MAC address used by a bridge. Avaya recommends that the number has to be the smallest MAC address of all ports belonging to the bridge. However, it is only required to be unique. When concatenated with Priority, a unique bridge identifier is formed that is used in the Spanning Tree Protocol.
NumPorts	Identifies the number of ports controlled by this bridging entity.

Name	Description
ProtocolSpecification	Specifies the version of the spanning tree protocol being run. Values include: • **decLb100**: Indicates the DEC LANbridge 100 Spanning Tree Protocol. • **ieee8021d**: IEEE802.1d implementations will return this entity. When future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version, a new value will be defined.
TimeSinceTopologyChange	Specifies the time (in hundredths of seconds) since the last topology change was detected by the bridge entity.
TopChanges	Specifies the number of topology changes detected by the bridge since the management entity was last reset or initialized.
DesignatedRoot	Specifies the bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol. The value is used as the root identifier parameter in all configuration bridge PDUs originated by this node.
RootCost	Indicates the cost of the path to the root as seen from the bridge.
RootPort	Identifies the port that has the lowest cost path from the bridge to the root bridge.
MaxAge	Specifies the maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in units of hundredths of a second. This is the actual value that this bridge is currently using.
HelloTime	Specifies the amount of time between the transmission of configuration bridge PDUs by this node on any port when it is the root of the spanning tree (in hundredths of a second). This is the actual value that this bridge is currently using.
HoldTime	Specifies the value of the interval length during which no more than two configuration bridge PDUs shall be transmitted by this node (in hundredths of a second).

Name	Description
ForwardDelay	Specifies the time value (in hundredths of a second) that controls how fast a port changes its spanning state when moving towards the forwarding state. Value determines how long the port stays in each of the listening and learning states, which precede the forwarding state. This is also used when a topology change has been detected and is underway, to age all dynamic entries in the forwarding database. **Important:** This value is the one that this bridge is currently using, in contrast to BridgeForwardDelay which is the value that this bridge and all other would start using if/when this bridge were to become the root.

Displaying STG port information using EDM

Use this procedure to view port information for the STG.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **STG** to open the STG work area.
4. Select the **Ports** tab.

Ports field descriptions

The following table describes the fields on the Ports tab.

Name	Description
Port	Indicates the switch position in a stack and port number. For a standalone switch, the default value of 1 is used for the switch position.

Name	Description
	Note: Stacking is not available is Release 5.0.
StgId	Specifies the STG identifier assigned to this port.
Priority	Indicates the value of the priority field contained in the first octet of the port ID. The other octet is given by the value of the “rcStgPort.”.
State	Specifies the current state of the port as defined by application of the Spanning Tree Protocol. These are the instructions the port takes on a frame when it is received. If the bridge detects a port is malfunctioning, it will list it as "broken(6)." For ports that are disabled, the value is "disabled(1).".
EnableStp	Enables (True) or disables (False) the spanning tree of the port.
FastStart	When enabled (True), the port moves to forwarding or blocking state in 4 seconds.
AdminPathCost	Specifies the administrative value of PathCost.
PathCost	Specifies the contribution of the port to the pathcost of paths towards the spanning tree root, including the current port. 802.1D-1990 specifications recommends that the default of this parameter be in inverse proportion to the speed of the attached LAN.
DesignatedRoot	Specifies the unique "Bridge Identifier." This is recorded as Root in the configuration bridge PDUs transmitted by the Designated Bridge for the segment to that the port is attached.
DesignatedCost	Specifies the path cost of the Designated Port of the segment connected to the port. The value is compared to the Root Path Cost field in received bridge PDUs.
DesignatedBridge	Identifies the Bridge identifier that this port considers to be the Designated Bridge for this port's segment.
DesignatedPort	Identifies the Port identifier of the port on the designated Bridge for this port's segment.

Name	Description
ForwardTransitions	Defines the number of times this port has transitioned from the learning state to the forwarding state.

Configuring STG for a single port using EDM

Use this procedure to view the status and modify the configuration of a port's spanning tree parameters.

Before you begin

The switch must be operating in STG mode to access the **STG** tab.

Procedure

1. From the Device Physical View, right click a port.
2. Double-click **Edit**.
3. In the Edit tree, double-click **Chassis**.
4. In the Chassis tree, click **Ports**.
5. To select an STG to edit, click the STG ID.
6. In the STG row, double-click the cell in the **Priority** row.
7. Type a priority value.
8. In the STG row, double-click the cell in the **EnableStp** column.
9. Select a value from the list — **true** to enable STP for the STG, or **false** to disable STP for the STG.
10. In the STG row, double-click the cell in the **FastStart** column.
11. Select a value from the list — **true** to enable fast start for the STG, or **false** to disable fast start for the STG.
12. In the STG row, double-click the cell in the **AdminPathCost** column.
13. Type an administrative path cost value.
14. In the STG row, double-click the cell in the **PathCost** column.
15. Type a path cost value.
16. On the toolbar, click **Apply**.

STG field descriptions

The following table describes the fields on the STG tab.

Name	Description
StgId	Indicates the STG identifier assigned to this port. This is a read-only value.
Priority	Specifies the value of the priority contained in the first octet of the port ID. The other octet is given by the value of the “rcStgPort.”
State	Indicates the current port state as defined by application of the Spanning Tree Protocol. This state controls the action a port takes after it receives a frame. If the bridge detects a port that is malfunctioning, it places that port into the broken state. For ports that are disabled (see EnableStp), this object has a value of disabled. This is a read-only value.
EnableStp	Enables (true) or disables (false) STP for the port.
FastStart	Enables (true) or disables (false) fast start for the port.
AdminPathCost	Specifies the administrative value of PathCost.
PathCost	Specifies the contribution of this port to the cost of paths toward the spanning tree root, which include this port. The IEEE802.1D-1990 standard recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN.
DesignatedRoot	Specifies the unique Bridge Identifier of the bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached. This is a read-only value.
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 bridge PDUs. This is a read-only value.

Name	Description
DesignatedBridge	Specifies the Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port's segment. This is a read-only value.
DesignatedPort	Specifies the Port Identifier of the port on the Designated Bridge for this port's segment. This is a read-only value.
ForwardTransitions	Specifies the number of times this port has transitioned from the Learning state to the Forwarding state. This is a read-only value.

Rapid Spanning Tree Protocol

The current Spanning Tree implementation in Ethernet Routing Switch 3500 Series is based on IEEE 802.1d, which is slow to respond to a topology change in the network (such as a dysfunctional link in a network). The Rapid Spanning Tree Protocol (RSTP or IEEE 802.1w) reduces the recovery time after a network breakdown. In certain configurations the RSPT recovery time is less than 1 second. It also maintains a backward compatibility with the IEEE 802.1d, which was the Spanning Tree implementation prior to RSTP. The backward compatibility can be maintained by configuring a port to be in STP compatible mode. A port operating in the STP compatible mode transmits and receives only STP BPDUs and drops any RSTP BPDUs.

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

Rapid Spanning Tree Protocol

The Rapid Spanning Tree Protocol (RSTP or IEEE 802.1w) reduces the recovery time after a network break down. It also maintains a backward compatibility with the IEEE 802.1d which was the Spanning Tree implementation prior to RSTP. In certain configurations the recovery time of RSTP can be reduced to less than 1 second.

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

Important:

You can access the RSTP menu command only after the switch is operating in the RSTP mode.

Displaying RSTP general information using EDM

Use this procedure to .view general information about Rapid Spanning Tree Protocol (RSTP) when RSTP is in active mode.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **RSTP**.

RSTP field descriptions

The following table describes the fields on the RSTP tab.

Name	Description
PathCostDefault	Sets the version of the Spanning Tree default Path Costs that the Bridge uses: • The 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. RANGE: 1 to 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 Rapid Spanning Tree Protocol specified in IEEE 802.1w.
Priority	Specifies the value of the writable portion of the Bridge Identifier comprising of the first two octets. The values that are set for Priority must be in steps of 4096.

Name	Description
BridgeMaxAge	Specifies t he value that all bridges use for MaxAge when this bridge is acting as the root. The granularity of this timer is specified to be 1 second. An agent can return a badValue error if a set is attempted to a value which is not a whole number of seconds.
BridgeHelloTime	Specifies the value that all bridges use for HelloTime when this bridge is acting as the root. The granularity of this timer is specified by 802.1D-1990 to be 1 second. An agent can return a badValue error if a set is attempted to a value which is not a whole number of seconds. Reference IEEE 802.1D-1990: Section 4.5.3.9.
BridgeForwardDelay	Specifies the value that all bridges use for ForwardDelay when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of rcStgBridgeMaxAge. The granularity of this timer is specified by 802.1D-1990 to be 1 second. An agent can return a badValue error if a set is attempted to a value which is not a whole number of seconds.
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 which offers the lowest cost path from this bridge to the root bridge.
MaxAge	Specifies the maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded . The maximum age is specified in units of hundredths of a second. This is the actual value that bridge uses.
HelloTime	Sets 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.

Name	Description
	This is specified in units of hundredths of a second. This is the actual value that bridge uses.
ForwardDelay	Specifies the time (measured in units of hundredths of a second), which control 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. This value is also used when a topology change has been detected, and is underway to age all dynamic entries in the Forwarding Database.
RstpUpCount	Specifies the number of times the RSTP Module has been enabled. A Trap is generated on the occurrence of this event.
RstpDownCount	Specifies the number of time the RSTP Module has been 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 this event.
TimeSinceToplogyChange	Specifies the time (in hundredths of a second) since the TcWhile Timer for any port in this Bridge was non-zero for 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.

Displaying RSTP ports information using EDM

Use this procedure to view RSTP Ports information.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **RSTP**.

4. Select the **RSTP Ports** tab.

RSTP Ports field descriptions

The following table describes the fields on the RSTP Ports tab.

Name	Description
Port	Specifies the port number.
State	Every 2 bitfields identifies a port state in this STG. Port state is cataloged as non-stp(0), blocking(1), learning(2), and forwarding(3).
Priority	The value of the priority field is contained in the first (in network byte order) octet of the (2 octet long) Port ID.
PathCost	Specifies the contribution of this port to the path cost of paths towards the spanning tree root which include this port.
ProtocolMigration	Specifies the number of times this port has migrated from one STP protocol version to another. The relevant protocols are: • STP-COMPATIBLE • RSTP A Trap is generated on the occurrence of this event.
AdminEdgePort	Specifies the administrative value of the Edge Port parameter. A value of TRUE(1) indicates that this port should be assumed as an edge-port and a value of FALSE(2) indicates that this port should be assumed as a non-edge-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. A value of forceTrue(0) indicates that

Name	Description
	this port should always be treated as if it is connected to a point-to-point link. • A value of forceFalse or 1 indicates that this port should be treated as having a shared media connection. • A value of auto or 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.
OperPointToPoint	Specifies the operational point-to-point status of the LAN segment attached to this port. It indicates whether a port is considered to have a point-to-point connection or not. The value is determined by management or by auto-detection.
Participating	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's segment.
DesignatedPort	Specifies the Port Identifier for the port segment which is on the Designated Bridge for this port's segment.
ForwardTransitions	Specifies the number of times this port has transitioned from the Learning state to the Forwarding state.

Displaying RSTP status using EDM

Use this procedure to view RSTP status.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **RSTP**.
4. Select the **RSTP Status** tab.

RSTP Status field descriptions

The following table describes the fields on the RSTP Status tab.

Name	Description
Port	Specifies the port number.
Role	Specifies the 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 for example, whether the Port is transmitting RST BPDUs or Config/TCN BPDUs.
EffectivePortState	Specifies the effective Operational state of the port. This object will be set to TRUE only when the port is operationally up in the interface manager and the force Port State for this port and specified port state is enabled. Otherwise this object is set to FALSE

Graphing RSTP port statistics using EDM

Use this procedure to display RSTP port statistics.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **RSTP**.
4. Select the **RSTP Status** tab.

5. Select a port and click on **Graph** to get the statistics for the selected port.

RSTP Status Graph field descriptions

The following table describes the fields on the RSTP Status Graph tab.

Name	Description
RxRstBpduCount	Displays the number of RST BPDUs that were received on this port.
RxConfigBpduCount	Displays the number of Configuration BPDUs that were received on this port.
RxTcnBpduCount	Displays the number of TCN BPDUs that were received on this port.
TxRstBpduCount	Displays the number of RST BPDUs transmitted from this port.
TxConfigBpduCount	Displays the number of Configuration BPDUs transmitted from this port.
TxTcnBpduCount	Displays the number of TCN BPDUs transmitted from this port.
InvalidRstBpduRxCount	Displays the number of invalid RST BPDUs received on this port.
InvalidConfigBpduRxCount	Displays the number of invalid Configuration BPDUs received on this port.
InvalidTcnBpduRxCount	Displays the number of invalid TCN BPDUs received on this port.
ProtocolMigrationCount	Displays the number of times this port has 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.

Multiple Spanning Tree Protocol

With Multiple Spanning Tree Protocol (MSTP or IEEE 802.1s), you can 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 Ethernet Routing Switch 3500 Series use RSTP and MSTP to achieve the following:

- Reduce converging time from 30 seconds to less than 1 or 2 seconds when there is topology change in the network (such as, a port in or out of service).
- Eliminate unnecessary flushing of the MAC database and flooding of traffic to the network, using new Topology Change mechanism.
- Backward compatibility with other switches that run legacy 802.1d STP.
- Under MSTP mode, eight instances of RSTP can be supported simultaneously. Instance 0 or CIST is the default group, which includes default VLAN 1. Instances 1 to 7 are called MSTIs 1 to 7.
- You can configure the switch to run avayaStpg, RSTP, or MSTP configuration.

Multiple Spanning Tree Protocol

With Multiple Spanning Tree Protocol (MSTP or IEEE 802.1s), the user can 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 STG.

In the MSTP mode, the Ethernet Routing Switch 3500 Series supports a maximum of one Common and Internal Spanning Tree (CIST) and seven Multiple Spanning Tree Instances (MSTI).

Important:

You can access the MSTP menu command only when the switch is operating in the MSTP mode.

Displaying MSTP general information using EDM

Use this procedure to view MSTP information.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **MSTP**.
   The MSTP dialog box with the **Globals** tab is displayed.

MSTP Globals field descriptions

The following table describes the fields on the MSTP Globals tab.

Name	Description
PathCostDefaultType	Specifies the version of the Spanning Tree default Path Costs that are to be 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.
MaxHopCount	Specifies the Maximum Hop Count value. The granularity of this timer is specified to be 1 second. An agent can return a badValue error if a set is attempted to a value which is not a whole number of seconds.
NoOfInstancesSupported	Indicates maximum number of spanning tree instances supported.
MstpUpCount	Specifies the number of times the MSTP Module has been enabled. A Trap is generated on the occurrence of this event.
MstpDownCount	Specifies the number of times the MSTP Module has been 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.

Name	Description
BrgAddress	The bridge address is generated when events like protocol up or protocol down occurs.
Root	The bridge identifier of the Root of the common spanning tree as determined by the Spanning Tree Protocol as executed by this node. This value is used as the CIST Root Identifier parameter in all Configuration BPDUs originated by this node.
RegionalRoot	The bridge identifier of the root of the Multiple spanning tree region as determined by the Spanning Tree Protocol as executed by this node. This value is used as the CIST Regional Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
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	Indicatest he port number of the port which offers the lowest path cost from the bridge to the CIST Root Bridge.
BridgePriority	Indicates the value of the writable portion of the Bridge Identifier comprising of the first two octets. The values that are set for Bridge Priority must be in steps of 4096.
BridgeMaxAge	Specifies the value that all bridges use for MaxAge when this bridge is acting as the root. The granularity of this timer is specified to be 1 second. An agent can return a badValue error if a set is attempted to a value which is not a whole number of seconds.
BridgeForwardDelay	Specifies the value that all bridges use for ForwardDelay when this bridge is acting as the root. IEEE 802.1D specifies that the range for this parameter is related to the value of BridgeMaxAge. The granularity of this timer is specified to be 1 second. An agent can return a badValue error if a set is attempted to a value which is not a whole number of seconds.
HoldTime	Determines the time interval during which no more than two Configuration BPDUs shall be

Name	Description
	transmitted by this node. This value is measured in units of hundredths of a second.
MaxAge	Specifies the maximum age of the Spanning Tree Protocol information learned from the network on any port before it is discarded. This value is measured in units of hundredths of a second.
ForwardDelay	Controls how fast a port changes its spanning state when moving towards the Forwarding state. This value determines how long the port stays in a particular state before moving to the next state. It is measured in units of hundredths of a second.
TimeSinceTopology Change	Specifies the value (measured in hundredths of a second) The time since the TcWhile Timer for any port in this Bridge was non-zero for Common Spanning Tree context.
TopChanges	Specifies the number of times that there have been at least one non-zero TcWhile Timer on this Bridge for the Common Spanning Tree context.
NewRootBridgeCount	Specifies the number of times this Bridge has detected a Root Bridge change for the Common Spanning Tree context. A Trap is generated when this event occurs.
RegionName	Signifies the name of the Region's configuration. By default, the Region Name is equal to the Bridge Mac Address.
RegionVersion	Denotes 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 is used to indicate RegionName, RegionVersion as specified in standard.
ConfigDigest	Signifies the Configuration Digest value for this Region. This is an MD5 digest value, and hence must always be 16octets long.
RegionConfigChangeCount	Specifies the number of times a Region Configuration Identifier Change was detected. A Trap is generated when this event occurs.

Displaying CIST port information using EDM

Use this procedure to display CIST port information.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **MSTP**.
4. Select the **CIST Port** tab.

CIST Port field descriptions

The following table describes the fields on the CIST Port tab.

Name	Description
Port	Identifies the port number of the port containing Spanning Tree information.
PathCost	Specifies the contribution of this port to the path cost of paths towards the CIST Root which include this port.
Priority	Displays 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. It is 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's segment.
DesignatedPort	Displays the Port identifier of the port on the Designated Bridge which is designated for the port's segment.
RegionalRoot	Displays the unique Bridge Identifier of the bridge. It is recorded as the CIST Regional

Name	Description
	Root Identifier in the configuration BPDUs which are transmitted.
RegionalPathCost	Displays the contribution of this port to the cost of paths. This value denotes the path of costs for the path towards the CIST Regional Root which include this port.
ProtocolMigration	Display is generated when port protocol migration happens in the port.
AdminEdgeStatus	Specifies the administrative value of the Edge Port parameter. A value of TRUE indicates that this port to be assumed as an edge-port and a value of FALSE indicates that this port to be assumed as a non-edge-port.
OperEdgeStatus	Signifies the operational value of the Edge Port parameter. It is initialized to the value of AdminEdgeStatus and is set to FALSE when the port receives a BPDU.
AdminP2P	Displays the administrative point-to-point status of the LAN segment attached to this port. A value of 0 indicates that this port should always be treated as if it is connected to a point-to-point link. A value of 1 indicates that this port should be 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 aport is considered to have a point-to-point connection or not. The value is determined by management or by auto-detection, as described in the AdminP2P object
HelloTime	Displays the amount of time between the transmission of Configuration BPDUs transmitted by this node on the port. It is measured in units of hundredths of a second.

Name	Description
OperVersion	Indicates whether the port is operationally in the MSTPmode, RSTP mode or the STP-compatible mode for example, whether the port is transmitting MST BPDUs, RST BPDUs, or Config/TCN BPDUs.
EffectivePortState	Displays the effective operational state of the port for CIST. This will beset to TRUE only when the port is operationally up in the Interface level and Protocol level for CIST. This is will be set to FALSE for all other times.
State	Displays the current state of the port as defined by the Common Spanning Tree Protocol.
ForcePortState	Displays the current state of the port which can be changed to either Disabled or Enabled for the base Spanning Tree instance.
SelectedPortRole	Displays the elected port role of the port for the Spanning Tree instance.
CurrentPortRole	Displays the current port role of the port for the Spanning Tree instance.

Graphing CIST Port Statistics using EDM

Use this procedure to display CIST Port statistics.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **MSTP**.
4. Select the **CIST Port** tab.
5. Select a port and click on **Graph** to get the statistics for the CIST port.

CIST Port field descriptions

The following table describes the fields on the CIST Port tab.

Name	Description
ForwardTransitions	Displays the number of times this port has transitioned to the Forwarding State.
RxMstBpduCount	Displays the number of MST BPDUs that were received on this port.
TxRstBpduCount	Displays the number of RST BPDUs that were received on this port.
RxConfigBpduCount	Displays the number of Configuration BPDUs that were received on this port.
RxTcnBpduCount	Displays the number of TCN BPDUs that were received on this port.
TxMstBpduCount	Displays the number of MST BPDUs transmitted from this port.
TxRstBpduCount	Displays the number of RST BPDUs transmitted from this port.
TxConfigBpduCount	Displays the number of Configuration BPDUs transmitted from this port.
TxTcnBpduCount	Displays the number of TCN BPDUs transmitted from this port.
InvalidMstBpduRxCount	Displays the number of invalid MST BPDUs received on this port.
InvalidRstBpduRxCount	Displays the number of invalid RST BPDUs received on this port.
InvalidConfigBpduRxCount	Displays the number of invalid Configuration BPDUs received on this port.
InvalidTcnBpduRxCount	Displays the number of invalid TCN BPDUs received on this port.
ProtocolMigrationCount	Displays the number of times this port has 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.

Displaying MSTI Bridges using EDM

Use this procedure to view the MSTI Bridges information.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **MSTP**.
4. Select the **MSTI Bridges** tab.

MSTI Bridges field descriptions

The following table describes the fields on the MSTI Bridges tab.

Name	Description
Instance	Specifies the Spanning Tree Instance to which the information belongs.
RegionalRoot	Specifies 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 of 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 port number of the port which offers the lowest path cost from this bridge to the MSTI Region Root Bridge.
Enabled	Defines whether the bridge instance is enabled or disabled.
TimeSinceTopology Change	Specifies the time (measured in hundredths of a second) since theTcWhile Timer for any port in this bridge was non-zero for this Spanning Tree instance.

Name	Description
TopChanges	Specifies the number of times that there have been at least one non-zero TcWhile Timer on this Bridge for this Spanning Tree instance.
NewRootCount	Specifies the number of times that there have been at least one non-zero TcWhile Timer on this Bridge for this Spanning Tree instance.
InstanceUpCount	Specifies the number of times a new Spanning Tree instance has been created. A Trap is generated on the occurrence of this event.
InstanceDownCount	Specifies the number of times a Spanning Tree instance has been deleted. A Trap is generated on the occurrence of this event.

Inserting MSTI Bridges using EDM

Use this procedure to insert MSTI Bridges.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **MSTP**.
4. Select the **MSTI Bridges** tab.
5. Click **Insert**.
6. Type the instance id.
7. Click **Insert**.

Deleting MSTI Bridges using EDM

Use this procedure to delete MSTI Bridges.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **MSTP**.

4. Select the **MSTI Bridges** tab.
5. Click on one or multiple MSTI Bridges.
6. Click **Delete**.
7. To confirm you wish to delete the MSTI bridge, click **Yes**.

Displaying MSTI Port information using EDM

Use this procedure to view MSTI Port information.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **MSTP**.
4. Select the **MSTI Port** tab.

MSTI Port field descriptions

The following table describes the fields on the MSTI Port tab.

Name	Description
Port	Denotes the port number.
Instance	Specifies the number of times a Spanning Tree instance has been deleted. A Trap is generated when this event occurs.
State	Specifies the current state of the port as defined by application of the Multiple Spanning Tree Protocol. The state of a port can be Forwarding state in one instance, and Discarding (Blocking) state in another instance.
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 thecost of paths towards the MSTI root, including the current port.

Name	Description
Priority	Indicates the four most significant bits of the Port Identifier for a given Spanning Tree instance. It can be modified independently for each Spanning Tree instance supported by the bridge. The values that are set for Port Priority must be in steps of 16.
DesignatedRoot	Specifies the unique "Bridge Identifier." This is recorded as the MSTI Regional Root in the configuration BPDUs that are transmitted.
Designated Bridge	Identifies the Bridge Identifier of the bridge which this port considers to be the Designated Bridge for this port's segment.
DesignatedPort	Identifies the Port Identifier of the port on the designated Bridge for this port's segment.
DesignatedCost	Specifies the path cost of the Designated Port of the segment connected to the 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 specific instance. This is 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 MSTI port statistics.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **MSTP**.
4. Select the **MSTI Port** tab.
5. Select a port and click on **Graph** to get the statistics for the MSTI port.

MSTI Port field descriptions

The following table describes the fields on the MSTI Port tab.

Name	Description
ForwardTransitions	Specifies the number of times this port has transitioned to the Forwarding State for specific instance.
InvalidBPDUsRcvd	Specifies the number of Invalid BPDUs received on this Port for this Spanning Tree instance.
ReceivedBPDUs	Specifies the number of BPDUs received by this port for this Spanning Tree instance.
TransmittedBPDUs	Specifies the number of BPDUs transmitted on this port for this Spanning Tree instance.

Setting up bridging

The Bridge parameters allow you to configure the global Spanning Tree and to view MAC address table for an Ethernet Routing Switch 3500 Series. Bridge information also includes Spanning Tree Group (STG) information.

This section describes how to work with the Base, Transparent, and Forwarding tabs to view bridge parameters, and how to view port bridge statistics.

Viewing Bridge base information using EDM

Use this procedure to view the Base tab. The Base tab displays the MAC address used by the bridge, the number of ports controlled by the bridge , and the type of bridge.

Procedure

1. In the navigation tree, double-click **Edit**.
2. Double-click **Bridge**.
3. In the work area, click the **Base** tab.

Bridge Base field descriptions

The following table describes the fields on the Base tab.

Name	Description
BridgeAddress	Specifies the MAC address used by the bridge which must be referred to in a unique fashion; moreover, it should be the smallest MAC address (numerically) of all ports that belong to the bridge. However, it is only required to be unique when integrated with dot1dStpPriority. A unique BridgeIdentifier is formed that is used in the Spanning Tree Protocol.
NumPorts	Specifies the number of ports controlled by the bridging entity.
Type	Indicates the type of bridging this bridge can perform. If the bridge is actually performing a certain type of bridging, this will be indicated by entries in the port table for the given type.

Viewing information about specific unicast MAC address using EDM

Use this procedure to view information about a specific unicast MAC address that has forwarding information for the bridge.

Procedure

1. In the navigation tree, double-click **Edit**.
2. Double-click **Bridge**.
3. Select the **Transparent** tab.

Bridge Transparent field descriptions

The following table describes the fields on the Transparent tab.

Name	Description
LearnedEntryDiscards	Specifies the number of Forwarding database entries learned that have been discarded due to a lack of space in the Forwarding database. If this counter is increasing, it indicates that the Forwarding database is becoming full regularly. This condition will affect the performance of the subnetwork. If the counter has a significant value and is not presently increasing, it indicates that the problem has been occurring but is not persistent.
AgingTime	Specifies the time-out period in seconds for aging out dynamically learned forwarding information. ❗ **Important:** The 802.1D-1990 specification recommends a default of 300 seconds.

Displaying current MAC Address Table using EDM

Use this procedure to view the current MAC Address Table (Forwarding table) on the switch.

Procedure

1. In the navigation tree, double-click **Edit**.
2. Double-click **Bridge**.
3. Select the **Forwarding** tab.

Bridge Forwarding field descriptions

The following table describes the fields on the Forwarding tab.

Name	Description
Id	Specifies the VLAN identifier.

Name	Description
Address	Specifies a unicast MAC address for which the bridge has forwarding or filtering information.
Port	Indicates that either the value "0" or the port number on a frame has been seen. The source address must be equal to the value of the corresponding instance of dot1dTpFdbAddress. A value of "0" indicates that the port number has not been learned, so the bridge does have the forwarding/ filtering information for this address (located in the dot1dStaticTable). You should assign the port value to this object whenever it is learned even for addresses for which the corresponding value of dot1dTpFdbStatus is not learned(3).
Status	The values of this field include: • **invalid**: Entry is not longer valid, but has not been removed from the table. • **learned**: Value of the corresponding instance of dot1dTpFdbPort was learned and is being used. • **self**: Value of the corresponding instance of dot1dTpFdbAddress represents an address of the bridge. The corresponding instance of dot1dTpFdbPort indicates that a specific port on the bridge has this address. • **mgmt(5)**: Value of the corresponding instance of dot1dTpFdbAddress is also the value of an existing instance of dot1dStaticAddress. • **other**: none of the preceding. This would include where some other MIB object (not the corresponding instance of dot1dTpFdbPort or an entry in the dot1dStaticTable) is being used to determine if frames addressed to the value of dot1dTpFdbAddress are being forwarded.

Graphing port bridge statistics using EDM

Use this procedure to graph port bridge statistical information.

Procedure

1. From the Device Physical View, click a port.
2. In the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **Bridge** tab.
5. Click the down arrow to the right of the **Poll Interval** dialog box.
6. Select a value from the list.
7. To reset the statistics counters, click **Clear Counters**.
8. To select bridge statistical information to graph, click an information row.
9. Click **Line Chart, Area Chart, Bar Chart,** or **Pie Chart** column.

Bridge tab field descriptions

The following table describes the fields on the Bridge tab.

Name	Description
DelayExceededDiscards	Specifies the number of frames discarded by the port due to excessive transit delays through the bridge. It is incremented by both transparent and source route bridges.
MtuExceededDiscards	Specifies the number of frames discarded by the port due to an excessive size. It is incremented by both transparent and source route bridges.
InFrames	Specifies the number of frames that have been received by this port from its segment.
OutFrames	Specifies the number of frames that have been received by this port from its segment.
InDiscards	Provides count of valid frames received which were discarded (filtered) by the Forwarding Process.

Chapter 17: Configuring Multi-Link Trunking using Enterprise Device Manager

Multi-Link Trunking (MLT) is a point-to-point connection that aggregates multiple ports so that they logically act like a single port with the aggregated bandwidth. You can achieve higher aggregate throughput on a switch-to-switch or switch-to-server application by grouping multiple ports into a logical link . Multi-Link Trunking provides media and module redundancy.

Multi-Link Trunk features

A number of Avaya products implement Multi-Link Trunking (MLT) and have different features and requirements based on the architecture of the device. For the Ethernet Routing Switch 3500 Series , Multi-Link Trunking has the following general features and requirements:

- A unit can have up to six Multi-Link Trunks (MLTs).
- Up to four ports can belong to an MLT.
- Multi-Link Trunking is supported on 10BASE-T, 100BASE-TX, 1000Base-T, and SFP ports.
- Multi-Link Trunking is compatible with the Spanning Tree Protocol
- IEEE 802.1Q tagging is supported on an MLT.
- The distribution algorithm is user-programmable. The default algorithm that distributes traffic across an MLT is based on the source and destination MAC addresses (BASIC mode). An algorithm that distributes traffic based on the source and destination IP addresses (ADVANCE mode) is also available.
- Distributed MLT (DMLT) is supported. DMLT is MLT with ports from two or more stack unit.

  Note:

  Note that stacking is not supported in Release 5.0.

Configuring Multi-Link Trunks using EDM

Use this procedure to display and configure MLTs using EDM.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. From the VLAN tree, 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 field, type a name for the MLT, or accept the default name.
7. In the trunk row, double-click the cell in the **PortMembers** column.
8. From the list, select multiple 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 in the **Enable** column.
13. From the list, select **true** to enable the MLT, or **false** to disable the MLT.
14. To create additional MLTs, repeat steps 4 to 13.
15. On the toolbar, click **Apply**.

Multi-Link Trunks field descriptions

The following table describes the fields on the Multi-Link Trunks tab.

Name	Description
Id	Specifies the MLT identification number (assigned consecutively).
PortType	Specifies the access or trunk port.
Name	Specifies the name given to the MLT.
PortMembers	Specifies the ports assigned to the MLT.
VlanIds	Specifies the VLANs assigned to the MLT.
Loadbalance(Mode)	Specifies the load balance mode. Values include: • basic • advanced
Enable	Specifies enabling of the MLT.

Displaying MLT utilization using EDM

Use this procedure to views MLT utilization information during the last hour.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **MLT Utilization** tab.

MLT Utilization field descriptions

The following table describes the fields on the MLT Utilization tab.

Name	Description
MtId	Specifies the MLT Identification number.
PortIfIndex	Specifies the port identification number.
TrafficType	Specifies the traffic type.
TrafficLast5Min	Specifies the MLT traffic in the last five minutes.
TrafficLast30Min	Specifies the MLT traffic in the last thirty minutes.
TrafficLast1Hour	Specifies the MTL traffic in the last hour.

Graphing Multi-Link Trunk statistics using EDM

Use this procedure to display and graph MLT interface statistics.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **MLT/LACP**.
3. In the work area, click the **Multi-Link Trunks**
4. To select an MLT to graph, click the trunk Id.
5. Click **Graph**.
6. Click the **Interface** tab.

7. Select a **Poll Interval** from the list.
8. From the list, select a poll interval time.
9. To reset the MLT statistics counters, click **Clear Counters**.
10. To select statistics to graph, click a statistic type row under one of the display columns.
11. Click **Line Chart, Area Chart, Bar Chart,** or **Pie Chart**.
12. To return to the Multi-Link Trunks — Graph work area, click **Close**.

Multi-Link Trunks field descriptions

The following table describes the fields on the Multi-Link Trunks tab.

Name	Description
InMulticastPkts	Specifies 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	Specifies the total number of packets that higher-level protocols requested to 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	Specifies the number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
OutBroadcastPkts	Specifies the total number of packets that higher-level protocols requested to be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.
HCInOctets	Specifies the total number of octets received on the MLT interface, including framing characters.
HCOutOctets	Specifies the total number of octets transmitted out of the MLT interface, including framing characters.
HCInUcastPkts	Specifies the number of packets delivered by this MLT to a higher MLT that were not

Name	Description
	addressed to a multicast or broadcast address at this sublayer.
HCOutUcastPkts	Specifies the number of packets that high-level protocols requested to be transmitted that were not addressed to a multicast address at this MLT. This total number includes those packets discarded or unsent.
HCInMulticastPkts	Specifies 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	Specifies the total number of packets that high-level protocols requested to 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	Specifies the number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
HCOutBroadcast	Specifies the total number of packets that high-level protocols requested to be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.

Graphing Multi-Link Trunk Ethernet error statistics using EDM

Use this procedure to display and graph Multi-Link Trunk Ethernet error statistics.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **MLT/LACP**.
3. In the work area, click the **Multi-Link Trunks**
4. To select an MLT to graph, click the trunk Id.
5. Click **Graph**.
6. Click the **Ethernet Errors** tab.

7. Select a **Poll Interval** from the list.
8. From the list, select a poll interval time.
9. To reset the MLT statistics counters, click **Clear Counters**.
10. To select statistics to graph, click a statistic type row under one of the display columns.
11. Click **Line Chart, Area Chart, Bar Chart,** or **Pie Chart**.
12. To return to the Multi-Link Trunks — Graph work area, click **Close**.

Ethernet Errors field descriptions

The following table describes the fields on the Ethernet Errors tab.

Name	Description
AlignmentErrors	Specifies the 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 IEEE802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
FCSErrors	Specifies the 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.
IMacTransmitError	Specifies the 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

Name	Description
	LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object.
IMacReceiveError	Specifies the 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 can represent a count of received errors on a particular interface that are not otherwise counted.
CarrierSenseError	Specifies 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	Specifies the 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	Specifies the 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.
DeferredTransmiss	Specifies the count of frames for which the first transmission attempt on a particular MLT is delayed because the medium is busy. The

Name	Description
	count represented by an instance of this object does not include frames involved in collisions.
SingleCollFrames	Specifies the 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.
MultipleCollFrames	Specifies the 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	Specifies the number of times that a collision is detected on a particular MLT later than 512 bit-times into the transmission of a 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	Specifies the count of frames for which transmission on a particular MLT fails due to excessive collisions.

Link Aggregation Control Protocol

With Link Aggregation (LA), you can create and manage a trunk group. You can control and configure a trunk group automatically through the use of the Link Aggregation Control Protocol (LACP). Use the procedures in this section to view and configure Link Aggregation Groups (LAG) and LACP.

Displaying LAG information using EDM

Use this procedure to view Link Aggregation Group (LAG) configuration information.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **MLT/LACP**.
3. Select the **LACP** tab.

LACP field descriptions

The following table describes the fields on the LACP tab.

Name	Description
Index	Specifies the unique identifier allocated to this Aggregator by the local System. This attribute identifies an Aggregator instance among the subordinate managed objects of the containing object. This value is read-only.
MacAddress	Specifies the MAC address used by this bridge when it must be referred to in a unique fashion.
AggregateOrIndividual	Specifies the read-only Boolean value indicating whether the Aggregation Port is able to Aggregate ('TRUE') or is only able to operate as an Individual link ('FALSE').
ActorLagId	Specifies the combined information of ActorSystemPriority, ActorSystemID, and ActorOperKey in "ActorSystemPriority-ActorSystemID-ActorOperKey" format.
ActorSystemPriority	Specifies the 2-octet read-write value used to define the priority value associated with the Actor's System ID.
ActorSystemID	Specifies the 6-octet read-only MAC address value that defines the value of the System ID for the System that contains this Aggregation Port.

Name	Description
ActorOperKey	Specifies the current operational value of the Key for the Aggregation Port. This is a 16-bit read-only value.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation Port. This is a 16-bit read-write value.
PartnerLagId	Specifies the combined information of PartnerSystemPriority, PartnerSystemID, and PartnerOperKey in "PartnerSystemPriority-PartnerSystemID-PartnerOperKey" format.
PartnerSystemPriority	Specifies the 2-octet read-only value that indicates the priority value associated with the Partner's System ID.
PartnerSystemID	Specifies the 6-octet read-only MAC address value consisting of the unique identifier for the current protocol Partner of this Aggregator. A value of zero indicates that there is no known Partner. If the aggregation is manually configured, this System ID value will be a value assigned by the local System.
PartnerOperKey	Specifies the current operational value of the Key for the Aggregator's current protocol Partner. This is a 16-bit read-only value.
CollectorMaxDelay	Specifies the value of this 16-bit read-write attribute defines the maximum delay, in tens of microseconds, that can be imposed by the Frame Collector between receiving a frame from an Aggregator Parser, and either delivering the frame to its MAC Client or discarding the frame.

Link Aggregation Group configuration using EDM

Use the procedures in this section to display or modify LAG member configuration.

Displaying LACP for LAG members using EDM

Use this procedure to display the existing LACP configuration for LAG members.

Procedure

1. In 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.

LACP Ports field descriptions

The following table describes the fields on the LACP Ports tab.

Name	Description
Index	Indicates the unique identifier allocated to an Aggregator by the local system.
AdminEnabled	Indicates the current administrative setting for the port. Values include: • **true**: enables the port to participate in LACP. • **false**: disables the port from participating in LACP.
OperEnabled	Specifies the current operational state for the port: • **true**: the port is participating in LACP. • **false**: the port is not participating in LACP.
ActorAdminState	Specifies the Actor administrative state for the port. Values include: • lacpActive • aggregation • shortTimeout
ActorOperState	Specifies the current operational values of Actor state transmitted by the Actor in LACPDUs.
AggregateOrIndividual	Specifies whether the port represents an Aggregate or an Individual link.
ActorPortPriority	Specifies the priority value assigned to this Aggregation port. RANGE: 0 to 65535.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation Port. RANGE: 1 to 4095.

Name	Description
ActorOperKey	Specifies the current operational value of the Key for the Aggregation Port.
SelectedAggID	Specifies the identifier value of the Aggregator that this Aggregation Port has currently selected. Zero indicates that the Aggregation Port has not selected an Aggregator, either because it is in the process of detaching from an Aggregator or because no suitable Aggregator exists for it to select.
AttachedAggID	Specifies 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	Specifies 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	Specifies the MLT that the port is assigned to. If the port is not assigned to an MLT, the MltId value is 0.
PartnerOperPort	Specifies the operational port number assigned by the port protocol partner.
OperStatus	Specifies the operational status of the interface. Values include: • **up**: operational • **down**: not operational

Configuring LACP for specific LAG members using EDM

Use this procedure to configure LACP for LAG members.

Before you begin

- Ensure members you want to configure are not ADAC Call Server or Uplink ports.
- Disable ADAC for members you want 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

1. In 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. Set 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. On the toolbar, click **Apply**.

LACP Ports field descriptions

The following table describes the fields on the LACP Ports tab.

Name	Description
Index	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
AdminEnabled	Indicates the current administrative setting for the port. Values include: • **true**: enables the port to participate in LACP. • **false**: disables the port from participating in LACP.

Name	Description
	Important: You cannot enable ports to participate in LACP if they are members of an enabled MLT.
OperEnabled	Specifies the current operational state for the port: • **true**: the port is participating in LACP. • **false**: the port is not participating in LACP.
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	Specifies whether the port represents an Aggregate or an Individual link. This is a read-only cell.
ActorPortPriority	Specifies the priority value assigned to this Aggregation port. RANGE: 0 to 65535.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation Port. RANGE: 1 to 4095.
ActorOperKey	Specifies the current operational value of the Key for the Aggregation Port. This is a read-only cell.
SelectedAggID	Specifies 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	Specifies the identifier value of the Aggregator that this Aggregation Port is currently attached to. Zero indicates that the

Name	Description
	Aggregation Port is not currently attached to an Aggregator. This value is read-only.
ActorPort	Specifies 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.
MtId	Specifies 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	Specifies the operational port number assigned by the port's protocol partner. This is a read-only cell.
OperStatus	Specifies the operational status of the interface. Values include: • **up**: operational • **down**: not operational This is a read-only cell.

LACP configuration for ports using EDM

You can use the information in this section to display or modify the LACP configuration for switch ports.

Displaying the LACP configuration for ports using EDM

Use this procedure to view the existing LACP configuration for switch ports.

Procedure

1. In 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.

LACP field descriptions

The following table describes the fields on the LACP tab.

Name	Description
Index	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.

Name	Description
AdminEnabled	Indicates the current administrative setting for the port. Values include: • **true**: enables the port to participate in LACP. • **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	Specifies the current operational state for the port: • **true**: the port is participating in LACP. • **false**: 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	Specifies whether the port represents an Aggregate or an Individual link. This is a read-only cell.
ActorPortPriority	Specifies the priority value assigned to this Aggregation port. RANGE: 0 to 65535.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation Port. RANGE: 1 to 4095.
ActorOperKey	Specifies the current operational value of the Key for the Aggregation Port. This is a read-only cell.
SelectedAggID	Specifies the identifier value of the Aggregator that this Aggregation Port has currently selected. Zero indicates that the Aggregation Port has not selected an

Name	Description
	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	Specifies 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	Specifies 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	Specifies 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	Specifies the operational port number assigned by the port's protocol partner. This is a read-only cell.
OperStatus	Specifies the operational status of the interface. Values include: • **up**: operational • **down**: not operational This is a read-only cell.

Configuring LACP for specific ports using EDM

Use this procedure to modify the LACP configuration for one or more switch ports.

Before you begin

- Ensure ports you want to configure are not ADAC Call Server or Uplink ports.
- Disable ADAC for ports you want 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

1. In 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 **AdminEnabled** column.
7. Set a value from the list — **true** to enable LACP for the port, or **false** to disable LACP for the port.
8. In the port row, double-click the cell in the **ActorAdminState** column.
9. Select an individual or combination of check boxes.
10. Click **OK**.
11. In the port row, double-click the cell in the **ActorPortPriority** column.
12. In the dialog box, edit the value as required.
13. In the port row, double-click the cell in the **ActorAdminKey** column.
14. In the dialog box, edit the value as required.
15. Repeat steps 5 through 14 to configure LACP for additional ports as required.
16. On the toolbar, click **Apply**.

LACP field descriptions

The following table describes the fields on the LACP tab.

Name	Description
Index	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
ActorSystemPriority	Specifies the priority value associated with the Actor System ID. RANGE: 0 to 65535.
AdminEnabled	Indicates the current administrative setting for the port. Values include: • **true**: enables the port to participate in LACP. • **false**: disables the port from participating in LACP.

Name	Description
	Important: You cannot enable ports to participate in LACP if they are members of an enabled MLT.
OperEnabled	Specifies the current operational state for the port: • **true**: the port is participating in LACP. • **false**: 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	Specifies whether the port represents an Aggregate or an Individual link. This is a read-only cell.
ActorPortPriority	Specifies the priority value assigned to this Aggregation port. RANGE: 0 to 65535.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation port. RANGE: 1 to 4095.
ActorOperKey	Specifies the current operational value of the Key for the Aggregation Port. This is a read-only cell.
SelectedAggID	Specifies 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	Specifies the identifier value of the Aggregator that this Aggregation Port is

Name	Description
	currently attached to. Zero indicates that the Aggregation Port is not currently attached to an Aggregator. This value is read-only.
ActorPort	Specifies 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.
MtId	Specifies 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	Specifies the operational port number assigned by the port's protocol partner. This is a read-only cell.
OperStatus	Specifies the operational status of the interface. Values include: • **up**: operational • **down**: not operational This is a read-only cell.

Graphing port LACP statistics using EDM

Use this procedure to display and graph LACP statistics for switch ports.

Procedure

1. From the Device Physical View, click a port.
2. In the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **LACP** tab.
5. Select a **Poll Interval** from the list.
6. Select a value from the list.
7. To select LACP statistics to graph, click a static type row under one of the displayed columns.
8. Click **Line Chart, Area Chart, Bar Chart,** or **Pie Chart** .

LACP field descriptions

The following table describes the fields on the LACP tab.

Name	Description
LACPDUsRx	Specifies the number of valid LACPDUs received on this Aggregation Port. This value is read-only.
MarkerPDUsRx	Specifies the number of valid Marker PDUs received on this Aggregation Ports. This value is read-only.
MarkerResponse PDUsRx	Specifies the number of valid Marker Response PDUs received on this Aggregation Port. This value is read-only.
UnknownRx	Specifies the number of frames 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	Specifies 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	Specifies the number of LACPDUs that are transmitted on this Aggregation Port. This value is read-only.
MarkerPDUsTx	Specifies the number of Marker PDUs transmitted on this Aggregation Port. This value is read-only.
MarkerResponse PDUsTx	Specifies the number of Marker Response PDUs that are transmitted on this Aggregation Port. This value is ready only.

Configuring MLT and VLACP global settings using EDM

Use the information in this section to:

- enable or disable VLACP globally
- set the VLACP Multicast MAC Address
- enable or disable MLT whole trunk mode globally

Configuring MLT whole trunk using EDM

Use this procedure to configure the MLT whole trunk mode of a switch.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. On the work area, click the **Global** tab.
4. Select **MltDisablePortsOnShutdown** to enable or disable the MLT whole trunk feature.
5. On the toolbar, click **Apply**.

Enabling or disabling global VLACP using EDM

Use this procedure to enable or disable VLACP for the switch.

Procedure

1. In 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. Do one of the following:
   - To enable VLACP, select the **VlacpEnable** check box.
   - To disable VLACP, deselect the **VlacpEnable** check box.
5. Type a value in the **VlacpMulticastMACAddress** dialog box.
6. On the toolbar, click **Apply**.

Global field descriptions

The following table describes the fields on the Global tab.

Name	Description
VlacpEnable	Enables or disables VLACP on the switch.
VlacpMulticastMACAddress	Identifies a multicast MAC address used exclusively for VLACPDUs. DEFAULT: 01:80:c2:00:11:00.

VLACP configuration for ports using EDM

Use the procedures in this section to view and configure VLACP at the port level.

Displaying the VLACP configuration for ports using EDM

Use this procedure to view the VLACP tab for ports.

Procedure

1. In 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.

VLACP field descriptions

The following table describes the fields on the VLACP tab.

Name	Description
rePortIndex	Specifies the switch and port number.
AdminEnable	Enables (True) or disables (False) VLACP on a port. DEFAULT: Disabled (False)

Name	Description
OperEnable	Specifies whether the VLACP is operationally enabled or disabled. This is a read-only field.
FastPeriodicTimer	Specifies the number of milliseconds between periodic transmissions using short timeouts. RANGE: 400 to 20000 milliseconds DEFAULT: 500
SlowPeriodicTimer	Specifies the number of milliseconds between periodic transmissions using long timeouts. RANGE: 10000 to 30000 milliseconds DEFAULT: 30000
Timeout	Specifies whether the timeout control value is a short or long timeout.
TimeoutScale	Specifies a timeout scale for the port, where timeout = (periodic time) * (timeout scale) **Note:** With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. However, if the timeout-scale is set to 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. To prevent this scenario from happening, set the timeout-scale to a value larger than 1. RANGE: 1 to 10 DEFAULT: 3
EtherType	Specifies VLACP protocol identification. The ID value is a 4–digit Hex number, with a default of 8103.
EtherMacAddress	Specifies the MAC address of the switch to which this port is sending VLACPDUs. It cannot be configured as **Note:** VLACP has only one multicast MAC address, configured using the MulticastMACAddress field in the VLACP

Name	Description
	Global tab, which is the Layer 2 destination address used for the VLACPDUs. The port-specific EtherMACAddresss parameter does not specify a multicast MAC address, but instead specifies the MAC address of the switch to which this port is sending VLACPDUs. You are not always required to configure EtherMACAddresss. If not configured, the first VLACP-enabled switch that receives the PDUs from a unit assumes that it is the intended recipient and processes the PDUs accordingly. If you want an intermediate switch to drop VLACP packets, configure the EtherMACAddresss field with the desired destination MAC address. With EtherMACAddresss configured, the intermediate switches do not misinterprett he VLACP packets. DEFAULT: 00:00:00:00:00:00.
PortState	Specifies whether the VLACP port state is up or down. This is a read-only field.

Configuring VLACP for specific ports using EDM

Use this procedure to configure VLACP for a single port or multiple ports.

Procedure

1. In 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.
5. To select a port to edit, click the port **rePortIndex**row.
6. In the port row, double-click the cell in the **AdminEnabled** column.
7. Set a value from the list — **true** to enable VLACP for the port, or **false** to disable VLACP for the port.
8. In the port row, double-click the cell in the **FastPeriodicTimer** column.
9. Type a value in the dialog box.
10. In the port row, double-click the cell in the **SlowPeriodicTimer** column.

11. Type a value in the dialog box.
12. In the port row, double-click the cell in the **Timeout** column.
13. Type a value in the dialog box.
14. In the port row, double-click the cell in the **TimeoutScale** column.
15. Type a value in the dialog box.
16. In the port row, double-click the cell in the **EtherType** column.
17. Type a value in the dialog box.
18. In the port row, double-click the cell in the **EtherMacAddress** column.
19. Type a value in the dialog box.
20. Repeat steps 5 through 19 to configure VLACP for additional ports as required.
21. On the toolbar, click **Apply**.

VLACP field descriptions

The following table describes the fields on the VLACP tab.

Name	Description
rePortIndex	Specifies the switch and port number.
AdminEnable	Indicates whether VLACP is enabled (True) or disabled (False) on ports. DEFAULT: Disabled (False)
OperEnable	Specifies whether the VLACP is operationally enabled or disabled. This is a read-only field. **Important:** VLACP in only operational when OperEnable is true and PortState is up.
FastPeriodicTimer	Specifies the number of milliseconds between periodic transmissions using short timeouts. RANGE: 400 to 20000 milliseconds DEFAULT: 500
SlowPeriodicTimer	Specifies the number of milliseconds between periodic transmissions using long timeouts. RANGE: 10000 to 30000 milliseconds DEFAULT: 30000

Name	Description
Timeout	Specifies whether the timeout control value is a short or long timeout.
TimeoutScale	Specifies a scale value used to calculate timeout from periodic time. ✱ **Note:** With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. However, if the timeout-scale is set to 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. To prevent this scenario from happening, set the timeout-scale to a value larger than 1. RANGE: 1 to 10 DEFAULT: 3
EtherType	Specifies VLACP protocol identification. The value can be entered as a numerical value ranging from 33025–33279 or a hexadecimal equivalent (8101–81ff). 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. DEFAULT: 8103
EtherMacAddress	Specifies the MAC address of the switch to which this port is sending VLACPDUs. It cannot be configured as ✱ **Note:** 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 the EtherMACAddresss field with the desired destination MAC address. With

Name	Description
	EtherMACAddresss configured, the intermediate switches do not misinterpret the VLACP packets. DEFAULT: 00:00:00:00:00:00.
PortState	Specifies whether the VLACP port state is up or down. This is a read-only field. **Important:** VLACP is only operational when OperEnable is ture and PortState is up.

Chapter 18: Configuring ADAC for Avaya IP phones using Enterprise Device Manager

This chapter provides procedure you can use to configure Auto-Detection and Auto-Correction (ADAC) using Enterprise Device Manager.

Configuring ADAC globally using EDM

Use this procedure to configure ADAC settings for the switch.

Procedure

1. In the navigation tree, double-click **Edit**.
2. Double-click **ADAC** to open the ADAC work area.
3. Click the **ADAC** tab.
4. Select the **AdminEnable** box to enable ADAC globally.

   OR

   Clear the **AdminEnable** to disable ADAC globally.
5. Click an **OperatingMode** radio button.
6. Select the **NotificationControlEnable** check box to enable trap notifications globally.

   OR

   Clear the **NotificationControlEnable** check box to disable trap notifications.
7. In the **VoiceVlan** dialog box, type a value.
8. Click the **CallServerPort** elipsis (...).
9. From the Call Server Port list, select Call Server ports.
10. Click **OK**.
11. Click the **UplinkPort** elipsis (...).
12. From the uplink port list, select uplink ports.
13. Click **OK**.

14. Click a **MacAddrRangeControl** radio button.
15. On the toolbar, 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.

ADAC field descriptions

The following table describes the fields on the ADAC tab.

Name	Description
AdminEnable	Enables and 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	Specifies 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	Specifies the Voice VLAN ID.
CallServerPortList	Specifies the Call Server port. A maximum of 8 Call Server ports are supported.

Name	Description
UplinkPortList	Specifies the Uplink port. A maximum of 8 uplink ports are supported.
MacAddrRangeControl	Provides two options for configuring the MAC address range table: • **none**: no MAC address range table selected • **clearTable**: clears the MAC address range table. • **defaultTable**: sets the MAC address range table to its default values.

ADAC port information management using EDM

Use the information in this section to configure ADAC for switch ports and to display port-based ADAC information.

Displaying port ADAC for information using EDM

Use this procedure to view ADAC configuration information for switch ports.

Procedure

1. In the navigation tree, double-click **Edit**.
2. Double-click **Chassis**.
3. Double-click **Ports**.
4. Double-click **ADAC**.
5. In the **Ports** work area, click the **ADAC** tab.
   OR
   In the **ADAC** work area, click the **ADAC Ports** tab.
6. On the toolbar, you can click **Refresh** to update the data.

ADAC or ADAC Ports field descriptions

The following table describes the fields on the ADAC or ADAC Ports tab.

Name	Description
Index	Indicates the switch position and the port number. DEFAULT: 1
AdminEnable	Indicates whether ADAC is enabled (true) or disabled (false) for the port.
OperEnable	Indicates ADAC operational state: true (enabled) or false (disabled).
ConfigStatus	Indicates the ADAC status for the port. Values include: • **configApplied**: the ADAC configuration is applied to this port. • **configNotApplied**: the ADAC configuration is not applied to this port.
TaggedFramesPvid	Indicates a unique PVID between 1 and 4094. A value of 0 indicates that Auto-Configuration cannot change the PVID for the port.
TaggedFramesTagging	Indicates the ADAC operating mode. Values include: • **tagAll**: tags all frames • **tagPvidOnly**: tags frames by the unique PVID • **untagPvidOnly**: untags frames by the unique PVID • **noChange**: accepts frames without change
AdacPortType	Indicates how ADAC classifies the port. Values include: • **telephony**: when Auto-Detection is enabled for the port. • **telephony:** auto-detection is enabled.. • **callServer**: port is configured as a call server

Name	Description
	• **uplink**: port is configured as an uplink or is part of the same trunk as the uplink port. • **other**: the port is not classified as either telephony, callServer, or uplink.
MacDetectionEnable	Indicates whether Auto-Detection of Avaya IP Phones, based on MAC address, is enabled (true) or disabled (false) on the interface.
LldpDetectionEnable	Indicates whether Auto-Detection of Avaya IP Phones, based on 802.1AB, is enabled (true) or disabled (false) on the interface. When cleared, indicates that Auto- Detection of Avaya IP Phones, based on 802.1AB, is disabled on the interface.

Configuring ADAC for specific ports using EDM

Use this procedure to configure ADAC for one or more ports in a switch.

Procedure

1. In the navigation tree, double-click **Edit**.
2. Double-click **Chassis**.
3. Double-click **Ports**

   OR

   Double-click **ADAC**.
4. In the Ports work area, click the **ADAC** tab.

   OR

   In the ADAC work area, click **ADAC Ports** tab.
5. To select a port to edit, click the port **Index**.
6. In the port row, double-click the cell in the **AdminEnable** column.
7. Select a value from the list — true to enable ADAC for the port, or false to disable ADAC for the port.
8. In the port row, double-click the cell in the **TaggedFramesPvid** column.
9. Type a value in the dialog box.
10. In the port row, double-click the cell in the **TaggedFramesTagging** column.
11. Select a value from the list.

12. In the port row, double-click the cell in the **MacDetectionEnable** column.
13. 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.
14. In the port row, double-click the cell in the **LldpDetectionEnable** column.
15. Select a value from the list — true to enable LLDP detection for the port, or false to disable LLDP detection for the port.
16. Repeat steps 5 through 15 to configure ADAC for additional ports.
17. On the toolbar, click **Apply**.

ADAC or ADAC Ports field descriptions

The following table describes the fields on the ADAC or ADAC Ports tab.

Name	Description
Index	Indicates the switch position and the port number. DEFAULT: 1
AdminEnable	Indicates whether ADAC is enabled (true) or disabled (false) for the port.
OperEnable	Indicates ADAC operational state: true (enabled) or false (disabled). This is a read-only cell. ❗ **Important:** If OperEnable is False and AdminEnable is True, then Auto-Detection/Auto-Configuration is disabled. This can occur due to a condition such as reaching the maximum number of devices supported per port.
ConfigStatus	Indicates the ADAC status for the port. This is a read-only cell. Values include: • **configApplied**: the ADAC configuration is applied to this port. • **configNotApplied**: the ADAC configuration is not applied to this port.
TaggedFramesPvid	Indicates a unique PVID between 1 and 4094. A value of 0 indicates that Auto-Configuration cannot change the PVID for the port.

Name	Description
TaggedFramesTagging	Indicates the ADAC operating mode. Values include: • **tagAll**: tags all frames • **tagPvidOnly**: tags frames by the unique PVID • **untagPvidOnly**: untags frames by the unique PVID • **noChange**: accepts frames without change
AdacPortType	Indicates how ADAC classifies the port. This is a read-only cell. Values include: • **telephony**: when Auto-Detection is enabled for the port. • **telephony**: auto-detection is enabled.. • **callServer**: port is configured as a call server • **uplink**: port is configured as an uplink or is part of the same trunk as the uplink port. • **other**: the port is not classified as either telephony, callServer, or uplink.
MacDetectionEnable	Indicates whether Auto-Detection of Avaya IP Phones, based on MAC address, is enabled (true) on the interface. When cleared, this indicates that Auto-Detection of Avaya IP Phones, based on MAC address, is disabled on the interface. ❗ **Important:** MacDetectionEnable cannot be set to false if no other supported detection mechanism is enabled on the port.
LldpDetectionEnable	Indicates whether Auto-Detection of Avaya IP Phones, based on 802.1AB, is enabled (true) or disabled (false) on the interface. When cleared, indicates that Auto- Detection of Avaya IP Phones, based on 802.1AB, is disabled on the interface. ❗ **Important:** LLdpDetectionEnable cannot be set to False if no other supported detection mechanism is enabled on the port.

ADAC MAC address range configuration using EDM

Use the information in this section to manage the ADAC MAC address range table.

Displaying the MAC address range table using EDM

Use this procedure to display the MAC address range table.

Procedure

1. In the navigation tree, double-click **Edit**.
2. Double-click **ADAC** to open the Chassis work area.
3. Select the **ADAC MAC Ranges** tab.

ADAC MAC Ranges field descriptions

The following table describes the fields on the ADAC MAC Ranges tab.

Name	Description
MacAddrRangeLowEndIndex	Indicates the low-end MAC address of the range.
MacAddrRangeHighEndIndex	Indicates the high-end MAC address of the range.

Creating MAC address ranges using EDM

Use this procedure to add new MAC address ranges to the ADAC MAC address range table.

Procedure

1. In 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. On the toolbar, click **Apply**.

Deleting MAC address ranges using EDM

Use this procedure to remove MAC address ranges from the ADAC MAC address range table.

Procedure

1. In 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**.
6. Click **Yes** to confirm the deletion of the MAC address range from the table.

Chapter 19: Configuring Link Layer Discovery Protocol using Enterprise Device Manager

Use the information in this section to configure LLDP properties for local and neighbor systems.

Displaying the optional TLVs using EDM

With the LLDP Port tab, you can set the optional TLVs to include in the LLPDUs transmitted by each port.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.
5. In the work area, click the **Port** tab.

Port tab field descriptions

The following table describes the fields on the Port tab.

Name	Description
PortNum	Specifies the Port number.
AdminStatus	Specifies the administratively desired status of the local LLDP agent: • **txOnly**: the LLDP agent transmits LLDP frames on this port and does not store

Name	Description
	information about the remote systems to which it is connected. • **rxOnly**: the LLDP agent receives but does not transmit LLDP frames on this port. • **txAndRx**: the LLDP agent transmits and receives LLDP frames on this port. • **disabled**: the LLDP agent does not transmit or receive LLDP frames on this port. If the port receives remote system information which is stored in other tables before AdminStatus is disabled, the information ages out..
NotificationEnable	Controls, on a per-port basis, whether notifications from the agent are enabled. • **true**: indicates that notifications are enabled. • **false**: indicates that notifications are disabled.
TLVsTxEnable	Sets the optional Management TLVs to be included in the transmitted LLDPDUs: • **portDesc**: Port Description TLV • **sysName**: System Name TLV • **sysDesc**: System Description TLV • **sysCap**: System Capabilities TLV ❗ **Important:** The Local Management tab controls Management Address TLV transmission.
CapSupported(med)	Identifies which MED system capabilities are supported on the local system.
TLVsTxEnable(med)	Sets the optional organizationally defined TLVs for MED devices to include in the transmitted LLDPDUs: • **capabilities**: Capabilities TLVs • **networkPolicy**: Network Policy TLVs • **location**: Emergency Communications System Location TLVs

Name	Description
	• **extendedPSE**: Extended PoE TLVs with PSE capabilitiies • **inventory**: Hardware Revision, Firmware Revision, Software Revision, Serial Number, Manufacturer Name, Model Name, and Asset ID TLVs.
NotifyEnable(med)	A value of **true** enables sending the topology change traps on this port. A value of **false** disables sending the topology change traps on this port.

Displaying LLDP global configuration using EDM

Use the following procedure to display and configure LLDP transmit properties and view remote table statistics.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics work area, click the **802.1AB** tab.
4. In the 802.1AB section, click the **LLDP** tab.
5. In the LLDP section, configure as required.
6. On the toolbar, click **Apply**.

Variable definitions

The following table describes the fields on the LLDP Globals tab.

Name	Description
lldpMessageTxInterval	The interval (in seconds) at which LLDP frames are transmitted on behalf of this LLDP agent.
lldpMessageTxHoldMultiplier	The time-to-live value expressed as a multiple of the object. The actual time-to-live value used in LLDP frames, transmitted on

Name	Description
	behalf of this LLDP agent, is expressed by the following formula: TTL = min(65535, (lldpMessageTxInterval *lldpMessageTxHoldMultiplier))
lldpReinitDelay	The delay (in seconds) from when the LLDP Port AdminStatus of a particular port is disabled until reinitialization begins.
lldpTxDelay	The delay (in seconds) between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB.
lldpNotificationInterval	The transmission intervals of LLDP notifications. The agent must not generate more than one notification event in the indicated period. If notification transmission is enabled for particular ports, the suggested default throttling period is 5 seconds.
RemTablesLastChangeTime	The value of the systemUpTime object at the time an entry is created, modified, or deleted in tables associated with the LLDP Remote Systems Data objects, and all LLDP extension objects associated with remote systems.
RemTablesInserts	The number of times the complete set of information is inserted into tables. Any failures occurring during insertion of the information set, which result in deletion of previously inserted information, do not trigger changes. If the failure is the result of a lack of resources, the counter is incremented once.
RemTablesDeletes	The number of times the complete set of information advertised is deleted from tables. This counter is incremented only once when the complete set of information is completely deleted from all related tables. Partial deletions, such as a deletion of rows from some tables, but not from all tables, are not allowed, and thus, do not change the value of this counter.
RemTablesDrops	The number of times the complete set of information can not be entered into tables because of insufficient resources.

Name	Description
RemTablesAgeouts	The number of times the complete set of information is deleted from tables because the information timeliness interval has expired. This counter increments once when the complete set of information is completely invalidated (aged out) from all related tables. Partial aging, similar to deletion case, is not allowed, and thus, does not change the value of this counter.
FastStartRepeatCount	Set the value (1 to 10) for number of LLDPDUs to be sent at startup to advertise information such as Emergency Call Service Location Identification Discovery of endpoints in Voice over Internet Protocol (VoIP) environments.

Displaying LLDP transmit statistics by port using EDM

Use this procedure to view LLDP transmit statistics by port.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
   In the Diagnostics tree, click **802.1AB**.
3. In the 802.1AB tree, click **LLDP**.
4. In the work area, click the **TX Stats** tab.

TX Stats tab field descriptions

The following table describes the fields on the TX Stats tab.

Name	Description
PortNum	Specifies the port number
FramesTotal	Specifies the number of LLDP frames transmitted by this LLDP agent on the indicated port

Graphing LLDP transmit statistics using EDM

Use this procedure to graph LLDP transmit statistics.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. In the work area, click the **TX Stats** tab.
6. From the TX Stats tab, select the port for which you want to display statistics.
7. Click **Graph**. The TX Stats — Graph dialog box appears.
8. Highlight a data column to graph.
9. Click one of the graph buttons.

Displaying LLDP receive statistics by port using EDM

Use this procedure to view LLDP receive statistics by port.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.
5. In the work area, click the **RX Stats** tab.

RX Stats tab field descriptions

The following table describes the fields on the RX Stats tab.

Name	Description
PortNum	Displays the port number.
FramesDiscardedTotal	Displays the number of LLDP frames received on the port and discarded for any reason. This counter provides an indication that LLDP header formatting problems exist with the local LLDP agent in the sending system, or that LLDPDU validation problems exist with the local LLDP agent in the receiving system.
FramesErrors	Displays the number of invalid LLDP frames received on the port, while the LLDP agent is enabled.
FramesTotal	Displays the number of valid LLDP frames received on the port, while the LLDP agent is enabled.
TLVsDiscardedTotal	Displays the number of LLDP TLVs discarded for any reason.
TLVsUnrecognizedTotal	Displays the number of LLDP TLVs received on a given port that are not recognized by this LLDP agent on the indicated port. An unrecognized TLV is referred to as the TLV whose type value is in the range of reserved TLV types (000 1001 - 111 1110) in Table 9.1 of IEEE 802.1AB-2004. An unrecognized TLV can be a basic management TLV from a later LLDP version.
AgeoutsTotal	Displays the counter represents the number of age-outs that occurred on a given port. An age-out is "the number of times the complete set of information advertised by a particular MSAP is deleted from tables in lldpRemoteSystemsData and lldpExtensions objects because the information timeliness interval has expired." This counter is similar to lldpStatsRemTablesAgeouts, except that it is on a per-port basis. This enables NMS to poll tables associated with the lldpRemoteSystemsData objects and all

Name	Description
	LLDP extension objects associated with remote systems on the indicated port only. This counter is set to zero during agent initialization. When the admin status for a port changes from disabled to rxOnly, txOnly or txAndRx, the counter associated with the same port is reset to 0. The agent also flushes all remote system information associated with the same port. This counter is incremented only once when the complete set of information is invalidated (aged out) from all related tables on a particular port. Partial aging is not allowed, and thus, does not change the value of this counter.

Graphing LLDP receive statistics using EDM

Use this procedure to graph LLDP receive statistics.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. In the work area, click the **RX Stats** tab.
6. From the RX Stats tab, select the port for which you want to display statistics.
7. Click **Graph**. The RX Stats — Graph dialog box appears.
8. Highlight a data column to graph.
9. Click one of the graph buttons.

Displaying the LLDP properties for the local system using EDM

Use this procedure to view LLDP properties for the local system using EDM.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.
5. In the work area, click the **Local System** tab.

Local System tab field descriptions

The following table describes the fields on the Local System tab.

Name	Description
AssetID	Displays the vendor-specific asset tracking identifier.
ChassisIdSubtype	Displays the type of encoding used to identify the local system chassis. Can be: • chassisComponent • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • local
ChassisId	Displays the Chassis Identification.
DeviceClass	Displays the MED device class
DeviceType	Displays the type of Power-via-MDI (Poe). Can be: • pseDevice • pdDevice • none
FirmwareRev	Displays vendor-specific firmware revision string.
HardwareRev	Displays vendor-specific hardware revision string.

Name	Description
MfgName	Displays vendor-specific manufacturer name.
ModelName	Displays vendor-specific model name.
PDPowerPriority	Defines the priority as: • critical • high • low
PDPowerReg	Specifies the value of the power required (in units of 0.1 watts) by a PoweredDevice (PD).
PDPowerSource	Defines the type of Power Source.
PSEPowerSource	Defines the type of PSE Power Source as Primary or Back-up.
SerialNum	Displays vendor-specific serial number.
SoftwareRev	Displays vendor-specific software revision string.
SysName	Displays local system name.
SysDesc	Displays local system description.
SysCapSupported	Identifies the system capabilities supported on the local system.
SysCabEnabled	Identifies the system capabilities enabled on the local system.

Displaying the LLDP port properties for the local system using EDM

Use this procedure to view LLDP port properties for the local system using EDM.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.

5. In the work area, click the **Local Port** tab.

Local Port tab field descriptions

The following table describes the fields on the Local Port tab.

Name	Description
PortNum	Displays the Port number.
PortIdSubtype	Displays the type of port identifier encoding used in the associated PortId object. Can be: • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • agentCircuitId • local
PortId	Displays the string value used to identify the port component associated with a given port in the local system.
PortDesc	Displays the string value used to identify the 802 LAN station port description associated with the local system. If the local agent supports IETF RFC 2863, the PortDesc object has the same value as the ifDescr object.

LLDP local management using EDM

Use the following procedures to display, enable, or disable local management information.

Displaying LLDP local management information using EDM

Use this procedure to display LLDP management properties for the local system.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.
5. In the work area, click the **Local Management** tab.

Local Management tab field descriptions

The following table describes the fields on the Local Management tab.

Name	Description
AddrSubtype	Indicates the type of management address identifier encoding used in the associated Addr object.
Addr	Indicates the string value used to identify the management address component associated with the local system. This address is used to contact the management entity. The switch supporte IPv4 and IPv6 management addresses. ✱ **Note:** If you configure both IPv4 and IPv6 management addresses, the switch displays each on a separate row.
AddrLen	Identifies the numbering method used to define the interface number associated with the remote system.
AddrIfSubtype	When displayed, indicates that frame tagging is enabled on the port, for exchanging Layer 2 priority tagging information between the switch and an Avaya IP phone.
AddrIfId	Indicates the integer value used to identify the interface number of the management address component associated with the local system.
AddrOID	Indicates the value used to identify the type of hardware component or protocol entity

Name	Description
	associated with the management address advertised by the local system agent.
AddrPortsTxEnable	Identifies the ports on which the local system management address TLVs are transmitted in the LLPDUs.

Enabling or disabling LLDP Management Address TLV transmission using EDM

Use this procedure to enable or disable the transmission of Management Address TLVs on the local system.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.
5. In the work area, click the **Local Management** tab.
6. Double-click the cell in the **AddPortsTxEnable** column for an IPv4 or IPv6 row.
7. To enable the transmission of Management Address TLVs, select one or more port numbers.

   OR

   To disable the transmission of Management Address TLVs, deselect one or more port numbers.
8. Click **Ok**.
9. On the toolbar, click **Apply**.

Displaying LLDP properties for the remote system using EDM

Use this procedure to view LLDP properties for the remote system using EDM.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.
5. In the work area, click the **Neighbor** tab.

Neighbor tab field descriptions

The following table describes the fields on the Neighbor tab.

Name	Description
TimeMark	Displays the TimeFilter for this entry. See the TimeFilter textual convention in IETF RFC 2021 for details about TimeFilter.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign montonically increasing index values to new entries, starting with one, after each restart.
ChassisIdSubtype	Displays the type of encoding used to identify the remote system chassis: • chassisComponent • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • local
ChassisId	Specifies the remote chassis ID
SysCapSupported	Identifies the system capabilities supported on the remote system.
SysCapEnabled	Identifies the system capabilities that are enabled on the remote system.

Name	Description
SysName	Displays the remote system name.
SysDesc	Displays the remote system description.
PortIdSubtype	Displays the type of encoding used to identify the remote port. • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • agentCircuitId • local
PortId	Displays remote port ID.
PortDesc	Displays remote port description.

Displaying LLDP management properties for the remote system using EDM

Use this procedure to display LLDP management properties for the remote system using EDM.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.
5. In the work area, click the **Neighbor Mgmt Address** tab.

Neighbor Mgmt Address tab field descriptions

The following table describes the fields on the Neighbor Mgmt Address tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Indicates the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
AddrSubtype	Indicates the type of encoding used in the associated Addr object.
Addr	Indicates the management address associated with the remote system. The switch supports IPv4 and IPv6 management addresses. ✱ **Note:** If you configure both IPv4 and IPv6 management addresses, the switch displays each on a separate row.
AddrIfSubtype	Indicates the numbering method used to define the interface number associated with the remote system. • unknown • ifindex • systemPortNumber
AddrIfId	Indicates the integer value used to identify the interface number of the management address component associated with the remote system.
AddrOID	Indicates the value used to identify the type of hardware component or protocol entity associated with the management address advertised by the remote system agent.

Displaying Unknown TLVs received on the local system using EDM

Use this procedure to view details about unknown TLVs received on the local system.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.
5. In the work area, click the **Unknown TLV** tab.

Unknown TLV tab field descriptions

The following table describes the fields on the Unknown TLV tab.

Name	Description
TimeMark	Displays the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each restart.
UnknownTLVType	Displays the value extracted from the type field of the unknown TLV.
UnknownTLVInfo	Displays the value extracted from the value field of the unknown TLV.

Displaying organizationally specific properties for the remote system using EDM

Use this procedure to view organizationally specific properties for the remote system using EDM.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.
5. In the work area, click the **Organizational Defined Info** tab.

Organizational Defined Info tab field descriptions

The following table describes the fields on the Organizational Defined Info tab.

Name	Description
TimeMark	Displays the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each restart.
OrgDefInfoOUI	Displays the Organizationally Unique Identifier (OUI), as defined in IEEE 802-2001, which is a 24 bit (three octets) globally unique assigned number referenced by various standards, of the information received from the remote system.
OrgDefInfoSubtype	Displays the integer value used to identify the subtype of the organizationally defined information received from the remote

Name	Description
	system. The subtype value is required to identify different instances of organizationally defined information that cannot be retrieved without a unique identifier that indicates the particular type of information in the information string.
OrgDefInfoIndex	Represents an arbitrary local integer value used by this agent to identify a particular unrecognized organizationally defined information instance, unique only for the OrgDefInfoOUI and lldpRemOrgDefInfoSubtype of the same remote system. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each restart. It is unlikely that the lldpRemOrgDefInfoIndex wraps between restarts.
OrdDefInfo	Identifies the organizationally defined information of the remote system. The encoding for this object is the same as that defined for SnmpAdminString TC.

Displaying LLDP MED policy properties for the local system using EDM

Use this procedure to display LLDP Media Endpoint Devices (MED) policy properties for the local system.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Local Policy** tab.

Local Policy tab field descriptions

The following table describes the fields on the LLDP MED Local Policy tab.

Name	Description
PortNum	Indicates the port number.
PolicyAppType	Shows the policy application type.
PolicyVlanID	Indicates the extension of the VLAN Identifier for the port, as defined in IEEE 802.1P-1998. A value of 1 through 4094 is used to define a valid PVID. A value of 0 is used if the device is using priority tagged frames, meaning that only the 802.1p priority level is significant and the default VID of the ingress port is being used instead. A value of 4095 is reserved for implementation use.
PolicyPriority	Indicates the value of the 802.1p priority which is associated with the local port.
PolicyDscp	Contains the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the given port on the local system.
PolicyUnknown	Indicates whether the network policy unknown (true) or defined (false). When the value is true, the system ignores the contents of PolicyVlanID, PolicyPriority, and PolicyDscp.
PolicyTagged	Indicates whether the application is using a tagged VLAN, untagged VLAN, or does not support a port based VLAN operation.

Local location information management using EDM

Use the information in this section to view and add local location information for remote network devices connected to a switch.

Displaying device location information using EDM

Use this procedure to display local location information for remote network devices connected to a switch.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Local Location** tab.

Local Location tab field descriptions

The following table describes the fields on the Local Location tab.

Name	Description
PortNum	Identifies the port number of the local system to which the remote device is connected.
LocationSubtype	Indicates the location subtype advertised by the remote device, as one of the following: • **unknown** • **coordinateBased**: location information is based on geographical coordinates of the remote device • **civicAddress**: location information is based on the civic address of the remote device • **elin**: location information is based on the Emergency Location Information Number (ELIN) of the remote device
LocationInfo	Displays local location information advertised by the remote device. The information displayed in this cell is directly associated with the location subtype value.

Adding ELIN based device location information using EDM

Use this procedure to add information to the local location table for remote network devices connected to a switch, based on an Emergency Location Information Number (ELIN).

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Local Location** tab.
6. In the port row with **elin** as the location subtype, double-click the cell in the **LocationInfo** column.
7. Type an alphanumeric value from 10–25 characters in length.
8. Click **Apply**.

Adding coordinate and civic address based device location information using EDM

Use this procedure to add local location information to the local location table for remote network devices connected to a switch, based on geographical coordinates and a civic address.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB.**
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Local Location** tab.
6. To add location information based on geographical coordinates for the remote device, click the **coordinateBased** cell in the LocationSubtype column for a port.
7. To add location information based on the civic address for the remote device, click the **civicAddress** cell in the LocationSubtype column for a port.
8. Click **Location Detail**.

9. Insert the local location information for the remote device.
10. Click **Ok**.
11. Click **Apply**.

Local Location tab field descriptions

The following table describes the fields on the Local Location tab.

Name	Description
Latitude	Specifies the latitude in degrees, and its relation to the equator (North or South).
Longitude	Specifies the longitude in degrees, and its relation to the prime meridian (East or West).
Altitude	Specifies the altitude, and the units of measurement used (meters or floors).
Map Datum	Specifies the map reference datum. Values are as follows: • **WGS84**: World Geodesic System 1984, Prime Meridian Name: Greenwich • **NAD83/NAVD88**: North American Datum 1983/ North American Vertical Datum of 1988 • **NAD83/MLLW**: North American Datum 1983 / Mean Lower Low Water

Display local PSE PoE information using EDM

Use this procedure to view the local Power over Ethernet (PoE) Power Supply for Ethernet (PSE) information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.

5. In the work area, click the **Local PoE PSE** tab.
6. Click **Refresh** to update the information.

Local PoE PSE tab field descriptions

The following table describes the fields on the Local PoE PSE tab.

Name	Description
PortNum	Displays the port number.
PSEPortPowerAvailable	Displays the power available over the PoE port in watts.
PSEPortPDPriority	Displays the priority rating for the port.

Displaying Neighbor Capabilities using EDM

Use this procedure to view Neighbor Capabilities information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor Capabilities** tab.
6. Click **Refresh** to update the information.

Neighbor Capabilities tab field descriptions

The following table describes the fields on the Neighbor Capabilities tab.

Name	Description
TimeMark	Specifies the TimeFilter for this entry.

Name	Description
Local PortNum	Identifies the local port on which the remote system information is received.
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
CapSupported	Identifies the MED system capabilities supported on the remote system.
CapCurrent	Identifies the MED system capabilities that are enabled on the remote system.
DeviceClass	Provides the remote MED device class.

Displaying Neighbor Policy using EDM

Use this procedure to view Neighbor Policy information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor Policy** tab.
6. Click **Refresh** to update the information.

Neighbor Policy tab field descriptions

The following table describes the fields on the Neighbor Policy tab.

Name	Description
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.

Name	Description
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PolicyAppType	Shows the policy application type.
PolicyVlanID	Displays an extension of the VLAN Identifier for the port, as defined in IEEE 802.1P-1998. A value of 1 through 4094 is used to define a valid PVID. A value of 0 is used if the device is using priority tagged frames, meaning that only the 802.1P priority level is significant and that the default VID of the ingress port is being used instead. A value of 4095 is reserved for implementation use.
PolicyPriority	Indicates the value of the 802.1P priority which is associated with the remote system connected to the port.
PolicyDscp	Displays the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the remote system connected to the port.
PolicyUnknown	A value of **true** indicates that the network policy for the specified application type is currently unknown. In this case, the VLAN ID, the Layer 2 priority, and the DSCP value fields are ignored. A value of **false** indicates that this network policy is defined.
PolicyTagged	A value of **true** indicates that the application is using a tagged VLAN. A value of **false** indicates that for the specific application, the device is using an untagged VLAN or does not support a port based VLAN operation. In this case, both the VLAN ID and the Layer 2 priority fields are ignored, and only the DSCP value has relevance.

Neighbor location information management using EDM

Use the information in this section to view and add neighbor location information for network devices connected to a switch.

Displaying neighbor location information using EDM

Use this procedure to view Neighbor Location information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor Location** tab.
6. Click **Refresh** to update the information.

Neighbor Location tab field descriptions

The following table describes the fields on the Neighbor Location tab.

Name	Description
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.

Name	Description
LocationSubtype	Displays the location subtype advertised by the remote device, as one of: • **unknown** • **coordinateBased**: location information is based on geographical coordinates of the remote device • **civicAddress**: location information is based on the civic address of the remote device • **elin**: location information is based on the Emergency Location Information Number (ELIN) of the remote device
LocationInfo	Displays local location information advertised by the remote device. The information displayed in this cell is directly associated with the location subtype value.

Adding coordinate-based neighbor location information using EDM

Use this procedure to add coordinate-based location information to the neighbor location table.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor Location** tab.
6. In the table, select a location with the **LocationSubtype** listed as **coordinateBased**.
7. In the toolbar, click the **Location Details** button.
8. Insert coordinate-based neighbor location information criteria.
9. Click **Close**.

Adding civic address location information using EDM

Use this procedure to add civic address-based location information to the neighbor location table.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor Location** tab.
6. In the table, select a location with the **LocationSubtype** listed as **civicAddress**.
7. In the toolbar, click **Location Details** .
8. Insert civic address-based neighbor location information criteria.
9. Click **Close**.

Displaying PoE information for switch ports using EDM

Use this procedure to display the PoE configuration for switch ports.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Ports**.
4. In the work area, click the **PoE** tab.

Variable definitions

The following table describes the fields on the PoE tab.

Name	Description
Unit	Indicated switch position.
Port	Indicates the switch port number.
AdminEnable	Lets you enable or disable PoE on this port. DEFAULT: enabled
DetectionStatus	Displays the operational status of the power-device detecting mode on the specified port: • disabled—detecting function disabled • searching—detecting function is enabled and the system is searching for a valid powered device on this port • deliveringPower—detection found a valid powered device and the port is delivering power. • fault—power-specific fault detected on port • test—detecting device in test mode • otherFault **Important:** Avaya recommends against using the test operational status.
PowerClassifications	Classification is a way to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points, and others can be classified according to their power requirements.
PowerPriority	Lets you set the power priority for the specified port to: • critical • high • low
PowerLimit(watts)	Specifies the maximum power that the switch can supply to a port. DEFAULT: 16W

Name	Description
Voltage(volts)	Indicates the voltage measured in Volts.
Current(amps)	Indicates the current measured in amps.
Power(watts)	Indicates the power measured in watts.

Displaying Neighbor PoE information using EDM

Use this procedure to view Neighbor Power over Ethernet (PoE) information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor PoE** tab.
6. Click **Refresh** to update the information.

Neighbor PoE tab field descriptions

The following table describes the fields on the Neighbor PoE tab.

Name	Description
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.

Name	Description
PoEDeviceType	Defines the type of Power-via-MDI (Power over Ethernet) advertised by the remote device as follows: • **pseDevice**: Indicates that the device is advertised as a Power Sourcing Entity (PSE). • **pdDevice**: Indicates that the device is advertised as a Powered Device (PD). • **none**: Indicates that the device does not support PoE.

Displaying Neighbor PoE PSE information using EDM

Use this procedure to view Neighbor Power over Ethernet (PoE) Power Supply for Ethernet (PSE) information using EDM.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor PoE PSE** tab.
6. Click **Refresh** to update the information.

Neighbor PoE PSE tab field descriptions

The following table describes the fields on the Neighbor PoE PSE tab.

Name	Description
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP.

Name	Description
	An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PSEPowerAvailable	Specifies the power available (in units of 0.1 watts) from the PSE connected remotely to this port.
PSEPowerSource	Defines the type of PSE Power Source advertised by the remote device, as follows: • **primary**: Indicates that the device advertises its power source as primary. • **backup**: Indicates that the device advertises its power source as backup.
PSEPowerPriority	Specifies the priority advertised by the PSE connected remotely to the port, as follows: • **critical**: Indicates that the device advertises its power priority as critical, see RFC 3621. • **high**: Indicates that the device advertises its power priority as high, see RFC 3621. • **low**: Indicates that the device advertises its power priority as low, see RFC 3621.

Displaying Neighbor PoE PD information using EDM

Use this procedure to view Neighbor Power over Ethernet (PoE) Powered Device (PD) information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor PoE PD** tab.
6. Click **Refresh** to update the information.

Neighbor PoE PD tab field descriptions

The following table describes the fields on the Neighbor PoE PD tab.

Name	Description
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PDPowerReq	Specifies the value of the power required (in units of 0.1 watts) by a Powered Device (PD) connected remotely to this port.
PDPowerSource	Defines the type of Power Source advertised as being used by the remote device, as follows: • **fromPSE**: Indicates that the device advertises its power source as received from a PSE. • **local**: Indicates that the device advertises its power source as local. • **localAndPSE**: Indicates that the device advertises its power source as using both local and PSE power.
PDPowerPriority	Specifies the priority advertised by the PD connected remotely to the port, as follows: • **critical**: Indicates that the device advertises its power priority as critical, see RFC 3621. • **high**: Indicates that the device advertises its power priority as high, see RFC 3621. • **low**: Indicates that the device advertises its power priority as low, see RFC 3621.

Displaying Neighbor Inventory information using EDM

Use this procedure to view Neighbor Inventory information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor Inventory** tab.
6. Click **Refresh** to update the information.

Neighbor Inventory tab field descriptions

The following table describes the fields on the Neighbor Inventory tab.

Name	Description
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
HardwareRev	Displays the vendor-specific hardware revision string as advertised by the remote device.
FirmwareRev	Displays the vendor-specific firmware revision string as advertised by the remote device.
SoftwareRev	Displays the vendor-specific software revision string as advertised by the remote device.

Name	Description
SerialNum	Displays the vendor-specific serial number as advertised by the remote device.
MfgName	Displays the vendor-specific manufacturer name as advertised by the remote device.
ModelName	Displays the vendor-specific model name as advertised by the remote device.
AssetID	Displays the vendor-specific asset tracking identifier as advertised by the remote device.

Avaya TLV transmit flags using EDM

Use the information in this section to view or enable the transmission of optional proprietary Avaya TLVs from switch ports to Avaya IP phones.

Displaying the Avaya TLV transmit flag status using EDM

Use this procedure to view the status of transmit flags for switch ports on which Avaya IP phone support TLVs are configured.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Port Config** tab.

Port Config tab field descriptions

The following table describes the fields on the Port Config tab.

Name	Description
poeConservationLevel	Enables or disables the TLV for requesting a specific power conservation level for an

Name	Description
	Avaya IP phone connected to the switch port. **Important:** Only Ethernet ports on switches that support PoE can request a specific power conservation level for an Avaya IP phone.
callServer	Enables or disables the TLV for advertising call server IPv4 addresses to an Avaya IP phone connected to the switch port.
fileServer	Enables or disables the TLV for advertising file server IPv4 addresses to an Avaya IP phone connected to the switch port.
FramingTlv	Enables or disables the frame tagging TLV for exchanging Layer 2 priority tagging information between the switch and an Avaya IP phone.

Enabling or Disabling Avaya TLV transmit flags using EDM

Use this procedure to enable or disable the transmission of optional proprietary Avaya TLVs from switch ports to Avaya IP phones.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Port Config** tab.
6. To select a port, click **PortNum**.
7. In the port row, double-click the cell in the **TLVsTxEnable** column.
8. Select a check box to enable a TLV.

   OR

   Clear a check box to disable a TLV.
9. Click **Ok**.

10. On the toolbar, click **Apply**.

Port Config tab field descriptions

The following table describes the fields on the Port Config tab.

Name	Description
poeConservationLevel	Enables or disables the TLV for requesting a specific power conservation level for an Avaya IP phone connected to the switch port. **Important:** Only Ethernet ports on switches that support PoE can request a specific power conservation level for an Avaya IP phone.
callServer	Enables or disables the TLV for advertising call server IPv4 addresses to an Avaya IP phone connected to the switch port.
fileServer	Enables or disables the TLV for advertising file server IPv4 addresses to an Avaya IP phone connected to the switch port.
FramingTlv	Enables or disables the frame tagging TLV for exchanging Layer 2 priority tagging information between the switch and an Avaya IP phone.

PoE conservation level and 802.1Q framing TLV management using EDM

Use the following procedures to display or configure PoE conservation levels and 802.1Q framing TLV.

Configuring the PoE conservation level request TLV using EDM

Use this procedure to request a specific power conservation level for an Avaya IP phone connected to a switch port.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Local Port** tab.
6. To select a port, click the **PortNum**.
7. In the port row, double-click the cell in the **PoeConsLevelRequest** column.
8. Type a value in the box.
9. On the toolbar, click **Apply**.

Local Port tab field descriptions

The following table describes the fields on the Local Port tab.

Name	Description
PoeConsLevelRequest	Specifies the power conservation level to request for a vendor-specific PD. With the default value, the switch does not request a power conservation level for an Avaya IP phone connected to the port. RANGE: 0 to 255 DEFAULT: 0

Displaying the PoE conservation level request and 802.1Q framing TLV configuration using EDM

Use this procedure to display the configuration status of the PoE conservation level request and 802.1Q framing TLVs that the switch can transmit to Avaya IP phones.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.

5. In the work area, click the **Local Port** tab.

Local Port tab field descriptions

The following table describes the fields on the Local Port tab.

Name	Description
Dot1QFramingRequest	Specifies the frame tagging mode. Values include: • **tagged**: frames are tagged based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. • **non-tagged**: frames are not tagged with 802.1Q priority. • **auto**: an attempt is made to tag frames based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. If there is no LLDP-MED Network Policy information available, an attempt is made to tag frames based on server configuration. If that fails, traffic is transmitted untagged. DEFAULT: auto
PoeConsLevelRequest	Specifies the power conservation level to request for a vendor-specific PD. With the default value, the switch does not request a power conservation level for an Avaya IP phone connected to the port. RANGE: 0 to 255 DEFAULT: 0

Configuring the 802.1Q framing TLV using EDM

Use this procedure to configure the frame tagging mode for exchanging Layer 2 priority tagging information between the switch and an Avaya IP phone.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.

4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Local Port** tab.
6. To select a port, click the **PortNum**.
7. In the port row, double-click the cell in the **Dot1QFramingRequest** column.
8. Select a value from the list.
9. On the toolbar, click **Apply**.

Local Port tab field descriptions

The following table describes the fields on the Local Port tab.

Name	Description
Dot1QFramingRequest	Specifies the frame tagging mode. Values include: • **tagged**: frames are tagged based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. • **non-tagged**: frames are not tagged with 802.1Q priority. • **auto**: an attempt is made to tag frames based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. If there is no LLDP-MED Network Policy information available, an attempt is made to tag frames based on server configuration. If that fails, traffic is transmitted untagged. DEFAULT: auto

Local call server management using EDM

Use the following procedures to display or configure local call server features.

Displaying the switch call server IP address TLV configuration using EDM

Use this procedure to display information about the defined local call server IP addresses that switch ports can advertise to Avaya IP phones.

Important:

The switch does not support the advertisement of IPv6 addresses to Avaya IP phones.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Local Call Servers** tab.

Local Call Servers tab field descriptions

The following table describes the fields on the Local Call Servers tab.

Name	Description
CallServerNum	Displays the call server number
CallServerAddressType	Displays the call server IP address type
CallServerAddress	Displays the defined call server IP address

Configuring the switch call server IP address TLV using EDM

Use this procedure to define the local call server IP addresses that switch ports can advertise to Avaya IP phones.

You can define IP addresses for a maximum of 8 local call servers.

Important:

The switch does not support the advertisement of IPv6 addresses to Avaya IP phones.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **LocalCallServers** tab.
6. To select a port, click the **CallServerNum**.
7. In the port row, double-click the cell in the **CallServerAddress** column.
8. Type an IP address in the box.
9. On the toolbar, click **Apply**.

Local Call Servers tab field descriptions

The following table describes the fields on the Local Call Servers tab.

Name	Description
CallServerNum	Displays the call server number
CallServerAddressType	Displays the call server IP address type
CallServerAddress	Defines the local call server IP address to advertise

Local file server management using EDM

Use the following procedures to manage local file server information.

Configuring the switch file server IP address TLV using EDM

Use this procedure to define the local file server IP addresses that switch ports can advertise to Avaya IP phones.

You can define IP addresses for a maximum of 4 local file servers.

Note:

If your Avaya IP Handset uses SIP, 802.1AB (LLDP) TLVs do not provide all information for the IP Phone. You must specify a file server IP address TLV so the IP phone can download the SIP configuration information, because the IP Phone retrieves information related to the SIP domain, port number and transport protocol from the file server.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **LocalFileServers** tab.
6. To select a port, click the **FileServerNum**.
7. In the port row, double-click the cell in the **FileServerAddress** column.
8. Type an IP address in the box.
9. On the toolbar, click **Apply**.

Local File Servers tab field descriptions

The following table describes the fields on the Local File Servers tab.

Name	Description
FileServerNum	Displays the file server number.
FileServerAddressType	Displays the file server IP address type.
FileServerAddress	Defines file server IP address to advertise.

Displaying the switch file server IP address TLV configuration using EDM

Use this procedure to display information about the defined local file server IP addresses that switch ports can advertise to Avaya IP phones.

Important:

The switch does not support the advertisement of IPv6 addresses to Avaya IP phones.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.

3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Local File Servers** tab.

Local File Servers tab field descriptions

The following table describes the fields on the Local File Servers tab.

Name	Description
FileServerNum	Displays the file server number.
FileServerAddressType	Displays the file server IP address type.
FileServerAddress	Displays the defined file server IP address.

Displaying Avaya IP phone power level TLV information using EDM

Use this procedure to display power level information received on switch ports from an Avaya IP phone.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor Devices** tab.

Neighbor Devices tab field descriptions

The following table describes the fields on the Neighbor Devices tab.

Name	Description
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
CurrentConsLevel	Displays the PoE conservation level configured on the Avaya IP phone connected to the switch port.
TypicalPower	Displays the average power level used by the Avaya IP phone connected to the switch port.
MaxPower	Displays the maximum power level for the Avaya IP phone connected to the switch port.

Displaying remote call server IP address TLV information using EDM

Use this procedure to display remote call server IP address information received on switch ports from an Avaya IP phone.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor Call Servers** tab.

Neighbor Call Servers tab field descriptions

The following table describes the fields on the Neighbor Call Servers tab.

Name	Description
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
PortCallServerAddressType	Displays the call server IP address type used by the Avaya IP phone connected to the switch port.
PortCallServerAddress	Displays the call server IP address used by the Avaya IP phone connected to the switch port.

Displaying remote file server IP address TLV information using EDM

Use this procedure to display remote file server IP address information received on switch ports from an Avaya IP phone.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor File Servers** tab.

Neighbor File Servers tab field descriptions

The following table describes the fields on the Neighbor File Servers tab.

Name	Description
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
PortFileServerAddressType	Displays the file server IP address type used by the Avaya IP phone connected to the switch port.
PortFileServerAddress	Displays the fileserver IP address used by the Avaya IP phone connected to the switch port.

Displaying PoE conservation level support TLV information using EDM

Use this procedure to display PoE conservation level information received on switch ports from an Avaya IP phone.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor PoE** tab.

Neighbor PoE tab field descriptions

The following table describes the fields on the Neighbor PoE tab.

Name	Description
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
PoeConsLevelValue	Displays the PoE conservation level supported by the Avaya IP phone connected to the switch port.

Displaying remote 802.1Q Framing TLV information using EDM

Use this procedure to display Layer 2 frame tagging mode information received on switch ports from connected Avaya IP phones.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor Dot1Q** tab.

Neighbor Dot1Q tab field descriptions

The following table describes the fields on the Neighbor Dot1Q tab.

Name	Description
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
Dot1QFraming	Displays the Layer 2 frame tagging mode for the Avaya IP phone connected to the swtich port. Values include: • **tagged**: frames are tagged based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. • **non-tagged**: frames are not tagged with 802.1Q priority. • **auto**: an attempt is made to tag frames based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. If there is no LLDP-MED Network Policy information available, an attempt is made to tag frames based on server configuration. If that fails, traffic is transmitted untagged. DEFAULT: auto

Displaying remote IP TLV information using EDM

Use this procedure to display IP address configuration information received on switch ports from connected Avaya IP phones.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.

3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor IP Phone** tab.

Neighbor IP Phone tab field descriptions

The following table describes the fields on the Neighbor IP Phone tab.

Name	Description
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
PortPhoneAddressType	Displays the IP address type for the Avaya IP phone connected to the switch port.
PortPhoneAddress	Displays the IP address for the Avaya IP phone connected to the switch port.
PortPhoneAddressMask	Displays the IP address subnet mask for the Avaya IP phone connected to the switch port.
PortPhoneGatewayAddress	Displays the gateway IP address for the Avaya IP phone connected to the switch port.