



Configuration — VLANs, Spanning Tree, and Multi-Link Trunking Avaya Ethernet Routing Switch 4500 Series

5.5
NN47205-501, 07.01
April 2011

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 Web sites 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 Web site: <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.

Licenses

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

Copyright

Except where expressly stated otherwise, no use should be made of 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

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

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: New in this release	11
Features.....	11
SLPP Guard.....	11
STP BPDU filtering ignore-self.....	11
Chapter 2: Introduction	13
ACLI command modes.....	13
Navigation.....	14
Chapter 3: VLAN Fundamentals	15
Virtual Local Area Networks.....	15
IEEE 802.1Q Tagging.....	16
VLANs Spanning Multiple Switches.....	21
VLAN Summary.....	24
VLAN Configuration Rules.....	25
VLAN Configuration Control.....	26
MAC Flush.....	27
Chapter 4: MLT Fundamentals	29
MultiLink trunks.....	29
Client-server configuration using MultiLink trunks.....	29
Before Trunks are Configured.....	30
MultiLink Trunking Configuration Rules.....	31
MLT load-balancing.....	32
MLT Enable or Disable Whole Trunk.....	33
Removal of MLT restrictions.....	34
Add and delete links from existing MultiLink trunks.....	34
How a MultiLink trunk reacts to losing distributed trunk members.....	34
Spanning Tree Considerations for MultiLink trunks.....	35
Additional Tips About the MultiLink Trunking Feature.....	38
SLPP Guard.....	39
Chapter 5: STP Fundamentals	41
Spanning Tree Protocol groups.....	41
STG Configuration Guidelines.....	42
Spanning Tree Fast Learning.....	43
STG port membership mode.....	44
802.1t path cost calculation.....	44
802.1D compliancy support.....	44
Rapid Spanning Tree Protocol.....	44
Multiple Spanning Tree Protocol.....	45
Interoperability with legacy STP.....	45
Differences in STP and RSTP port roles.....	46
Rapid convergent.....	47
BPDU-Filtering.....	48
STP BPDU filtering ignore-self.....	49
Chapter 6: ADAC Fundamentals	51
Autodetection and Autoconfiguration of IP Phones.....	51

ADAC operation.....	51
Auto-detection of IP Phones.....	52
Auto-Detection by MAC address.....	52
Auto-Detection by LLDP (IEEE 802.1ab).....	54
Auto-Configuration of IP Phones.....	55
Initial user settings.....	56
Port Restrictions.....	56
Operating modes.....	57
Dynamic VLAN Autoconfiguration.....	61
ADAC and stacking.....	62
ADAC Uplink port as part of trunk.....	62
ADAC and EAP configuration.....	63
ADAC User Restrictions.....	64
ADAC management.....	65
Chapter 7: LACP and VLACP Fundamentals.....	67
IEEE 802.3ad Link Aggregation.....	67
Link aggregation rules.....	68
VLACP.....	69
Virtual LACP (VLACP) overview.....	69
VLACP features.....	72
Chapter 8: Configuring VLANs using ACLI.....	73
Displaying VLAN information.....	73
Displaying VLAN interface information.....	74
Displaying port membership in VLANs.....	74
Displaying the management VLAN.....	75
Configuring the management VLAN.....	75
Deleting the management VLAN IP address.....	75
Resetting the management VLAN.....	76
Creating VLANs.....	76
Deleting a VLAN.....	78
Removing a MAC address from allowed flooding.....	78
Configuring VLAN name.....	79
Configuring automatic PVID.....	79
Configuring port VLAN settings.....	79
Configuring VLAN member ports.....	80
Configuring VLAN Configuration Control.....	81
Displaying VLAN Configuration Control settings.....	82
Modifying VLAN Configuration Control.....	82
Managing MAC address forwarding database table.....	83
Displaying the MAC address forwarding table.....	83
Configuring aging time for unseen MAC addresses.....	84
Setting aging time for unseen MAC addresses to default.....	84
Clearing the MAC address table.....	85
Clearing the MAC address table on a VLAN.....	85
Clearing the MAC address table on a FastEthernet interface.....	86
Clearing the MAC address table on a trunk.....	86
Removing a single address from the MAC address table.....	87
Chapter 9: Configuring MultiLink Trunking using ACLI.....	89
Configuring a Multi Link Trunk using ACLI.....	89

Displaying MLT configuration using ACLI.....	90
Viewing IP address-based MLT hashing information using ACLI.....	90
Viewing MAC address-based MLT hashing using ACLI.....	92
Displaying STG MLT properties using ACLI.....	93
Configuring STP participation for MLTs using ACLI.....	94
Enabling all ports shutdown in the MLT using ACLI.....	94
Disabling MLT Enable or Disable Whole Trunk feature using ACLI.....	95
Displaying the current MLT Enable or Disable Whole Trunk mode of operation using ACLI.....	95
Selecting an SLPP Guard Ethernet type using ACLI.....	96
Configuring SLPP Guard using ACLI.....	97
Viewing the SLPP Guard status using ACLI.....	98

Chapter 10: Configuring Spanning Tree Protocol using ACLI.....101

Configuring STP operation mode using ACLI.....	101
Configuring STP BPDU filtering using ACLI.....	101
Configuring STP BPDU filtering ignore-self using ACLI.....	102
Viewing the STP BPDU Filtering ignore-self status using ACLI.....	103
Creating and Managing STGs using ACLI.....	103
Configuring path cost calculation using ACLI.....	103
Configuring STG port membership using ACLI.....	104
Displaying spanning tree configuration information using ACLI.....	104
Creating a spanning tree group using ACLI.....	105
Deleting a spanning tree group using ACLI.....	105
Enabling a spanning tree group using ACLI.....	105
Disabling a spanning tree group using ACLI.....	106
Configuring STP values by STG using ACLI.....	106
Restoring default spanning tree value for a STG using ACLI.....	107
Setting STP and STG participation using ACLI.....	108
Setting default spanning tree values for ports using ACLI.....	109
Disable spanning tree for a port using ACLI.....	110
STP 802.1D compliancy support configuration using ACLI.....	110
Enabling STP 802.1D compliancy support using ACLI.....	110
Disabling STP 802.1D compliancy support using ACLI.....	111
Viewing STP 802.1D compliancy support status using ACLI.....	111
STP 802.1t cost calculation support configuration using ACLI.....	112
Enabling STP 802.1t cost calculation support using ACLI.....	112
Disabling STP 802.1t cost calculation support using ACLI.....	113
Viewing STP 802.1t cost calculation status using ACLI.....	113
Managing RSTP using ACLI.....	114
Configuring RSTP parameters using ACLI.....	114
Configuring RSTP parameters per port using ACLI.....	115
Displaying RSTP bridge-level configuration details using ACLI.....	116
Displaying RSTP port-level configuration details using ACLI.....	116
Configuring RSTP SNMP traps using ACLI.....	117
Enable RSTP SNMP traps using ACLI.....	117
Reset RSTP SNMP traps settings to default using ACLI.....	118
Verifying RSTP SNMP traps settings using ACLI.....	118
Managing MSTP using ACLI.....	119
Configuring MSTP parameters for CIST Bridge using ACLI.....	119
Configuring MSTP parameters for Common Spanning Tree using ACLI.....	120
Configuring MSTP region parameters using ACLI.....	121

Configuring MSTP parameters for bridge instance using ACLI.....	122
Disabling a MSTP bridge instance using ACLI.....	122
Deleting a MSTP bridge instance using ACLI.....	123
Displaying MSTP status by selected bridge using ACLI.....	123
Displaying MSTP CIST port information using ACLI.....	123
Displaying MSTP MSTI settings using ACLI.....	124
Chapter 11: Configuring ADAC using ACLI.....	127
Configuring ADAC globally using ACLI.....	127
Disabling ADAC globally using ACLI.....	128
Restoring default ADAC settings using ACLI.....	129
Configuring per port ADAC settings using ACLI.....	130
Disable ADAC settings per port using ACLI.....	131
Configuring per port ADAC defaults for a specified port using ACLI.....	131
Configuring the autodetection method using ACLI.....	132
Disabling autodetection using ACLI.....	133
Setting autodetection method to default using ACLI.....	133
Configuring autodetection for a specified port using ACLI.....	134
Disabling autodetection on specified ports using ACLI.....	134
Restoring default ADAC setting for ports using ACLI.....	135
Adding a range of MAC addresses for autodetection using ACLI.....	135
Deleting a range of MAC addresses used by autodetection using ACLI.....	136
Resetting supported MAC address ranges using ACLI.....	136
Displaying global ADAC settings for a device using ACLI.....	136
Displaying ADAC settings per port using ACLI.....	137
Displaying configured ADAC MAC ranges using ACLI.....	137
Displaying detection mechanism configured per port using ACLI.....	137
ADAC UFA configuration example.....	138
ADAC ACLI configuration commands.....	140
Verifying new ADAC settings.....	140
Chapter 12: LACP and VLACP configuration using ACLI.....	143
Configuring LACP using ACLI.....	143
Displaying LACP settings using ACLI.....	143
Displaying per port LACP configuration information using ACLI.....	143
Displaying LACP port statistics using ACLI.....	144
Clearing LACP port statistics using ACLI.....	144
Displaying port debug information using ACLI.....	145
Displaying LACP aggregators or LACP trunks using ACLI.....	145
Configuring LACP system priority using ACLI.....	145
Enabling port aggregation mode using ACLI.....	146
Disabling port aggregation mode using ACLI.....	146
Configuring administrative LACP key using ACLI.....	146
Configuring LACP mode of operation using ACLI.....	147
Configuring per port LACP priority using ACLI.....	148
Configuring LACP periodic transmission timeout interval using ACLI.....	148
Configuring VLACP using ACLI.....	149
Enabling VLACP using ACLI.....	149
Configuring multicast MAC address for VLACP using ACLI.....	149
Configuring VLACP parameters per port using ACLI.....	150
Disabling VLACP using ACLI.....	152
Resetting multicast MAC address for VLACP to default using ACLI.....	152

Disabling VLACP on a port using ACLI.....	152
Displaying VLACP status using ACLI.....	153
Displaying VLACP configuration details for ports using ACLI.....	153
Chapter 13: Configuring VLANs using Enterprise Device Manager.....	155
VLAN management using EDM.....	155
Viewing VLAN information using EDM.....	155
Modifying an existing VLAN in STG mode using EDM.....	157
Modifying an existing VLAN in RSTP mode using EDM.....	159
Modifying an existing VLAN in MSTP mode using EDM.....	162
Creating a VLAN in STP mode using EDM.....	164
Creating a VLAN in RSTP mode using EDM.....	167
Creating a VLAN in MSTP mode using EDM.....	169
Deleting a VLAN using EDM.....	172
VLAN IPv4 address management using EDM.....	172
Viewing VLAN IPv4 address information using EDM.....	172
Assigning an IPv4 address to a using EDM.....	173
Deleting an IPv4 address from a VLAN using EDM.....	174
Configuring DHCP for a VLAN using EDM.....	175
Configuring RIP for a VLAN using EDM.....	176
Graphing OSPF statistics for a VLAN using EDM.....	178
VLAN IPv6 interface management using EDM.....	178
Viewing IPv6 interface information for a VLAN using EDM.....	179
Adding an IPv6 interface to a VLAN using EDM.....	180
Deleting an IPv6 interface from a VLAN using EDM.....	182
VLAN IPv6 address management using EDM.....	182
Viewing IPv6 address information for a VLAN using EDM.....	182
Adding an IPv6 address to a VLAN using EDM.....	184
Deleting an IPv6 address from a VLAN using EDM.....	185
VLAN configuration for ports using EDM.....	185
Viewing VLAN membership port information using EDM.....	186
Configuring VLAN membership ports using EDM.....	187
Selecting VLAN configuration control using EDM.....	189
Enabling AutoPVID using EDM.....	190
Port configuration for VLANs using EDM.....	190
Viewing port VLAN membership information using EDM.....	191
Configuring ports for VLAN membership using EDM.....	192
MAC address table management using EDM.....	194
Flushing the MAC address table using EDM.....	194
Flushing FastEthernet interface-based MAC addresses from the MAC address table using EDM.....	195
Flushing VLAN-based MAC addresses from the MAC address table using EDM.....	195
Flushing trunk-based MAC addresses from the MAC address table using EDM.....	196
Flushing a specific MAC address from the MAC address table using EDM.....	196
Chapter 14: Configuring MultiLink Trunking using Enterprise Device Manager.....	199
MLT configuration using EDM.....	199
MLT configuration using EDM navigation.....	199
Viewing MLT configurations using EDM.....	199
Creating an MLT using EDM.....	200
Modifying MLT port memberships using EDM.....	202
Viewing MLT utilization using EDM.....	203
Graphing MLT statistics using EDM.....	204

Graphing MLT Ethernet error statistics using EDM.....	205
Selecting an SLPP Guard Ethernet type using EDM.....	208
Configuring SLPP Guard using EDM.....	208
Viewing the SLPP Guard configuration using EDM.....	209
Chapter 15: Configuring Spanning Tree Protocol using Enterprise Device Manager....	211
Configuring the STP mode using EDM.....	211
Resetting the switch using EDM.....	212
Configuring STP BPDU filtering for specific ports using EDM.....	212
Configuring STG globally using EDM.....	213
Configuring STP BPDU filtering ignore self using EDM.....	215
STG configuration using EDM.....	215
Viewing an STG using EDM.....	216
Modifying an STG using EDM.....	217
Creating an STG using EDM.....	219
Deleting an STG using EDM.....	220
Moving a VLAN between STGs using EDM.....	221
Viewing STG Status using EDM.....	221
STG port membership management using EDM.....	222
Viewing STG port information using EDM.....	223
Configuring STG for port using EDM.....	224
Port STG membership configuration using EDM.....	225
Viewing STG port membership information using EDM.....	226
Configuring STG port membership using EDM.....	227
Chapter 16: RSTP configuration using Enterprise Device Manager.....	229
Viewing global RSTP information using EDM.....	229
Viewing RSTP port information using EDM.....	232
Viewing RSTP statistics using EDM.....	234
Graphing RSTP port statistics using EDM.....	235
Chapter 17: MSTP configuration using Enterprise Device Manager.....	237
Viewing global MSTP using EDM.....	238
Viewing CIST port information using EDM.....	241
Graphing CIST port statistics using EDM.....	243
Viewing MSTI bridge information using EDM.....	245
Inserting MSTI Bridges using EDM.....	247
Deleting MSTI Bridges using EDM.....	247
Viewing MSTI port information using EDM.....	247
Graphing MSTI port statistics using EDM.....	249
Chapter 18: Configuring ADAC using Enterprise Device Manager.....	251
Configuring ADAC globally using EDM.....	251
ADAC MAC address range configuration using EDM.....	253
Creating a ADAC MAC address range using EDM.....	253
Deleting MAC address ranges using EDM.....	254
ADAC port configuration using EDM.....	254
Viewing the ADAC configuration for ports using EDM.....	254
Configuring ADAC for specific ports using EDM.....	256
Chapter 19: Configuring LACP and VLACP using Enterprise Device Manager.....	261
Viewing LAG information using EDM.....	261

Link Aggregation Group configuration using EDM.....	263
Viewing LACP for LAG members using EDM.....	263
Configuring LACP for specific LAG members using EDM.....	264
LACP configuration for ports using EDM.....	267
Viewing the LACP configuration for ports using EDM.....	267
Configuring LACP for ports using EDM.....	269
Graphing port LACP statistics using EDM.....	272
Global VLACP configuration using EDM.....	273
Enabling global VLACP using EDM.....	273
Disabling global VLACP using EDM.....	274
VLACP configuration for ports using EDM.....	274
Viewing the VLACP configuration for ports using EDM.....	274
Configuring VLACP for specific ports using EDM.....	276

Chapter 1: New in this release

The following section details what is new in *Avaya Ethernet Routing Switch 4500 Configuration — VLANs, Spanning Tree, and MultiLink Trunking* (NN47205-501) for Release 5.5.

Features

See the following section for information about feature changes:

SLPP Guard

You can use Avaya's Split Multi-Link Trunking (SMLT) in combination with Simple Loop Prevention Protocol (SLPP) Guard to provide additional loop protection to protect wiring closets from erroneous connections. SMLT implementations provide an SLPP packet which helps prevent loops from occurring when switch clustering is implemented. When you enable SLPP Guard, this loop prevention mechanism is extended into and across multiple wiring closets. If the edge switch configured for SLPP Guard receives an SLPP packet on a port, the feature can immediately disable the port administratively, and generate appropriate log messages and SNMP traps.

 **Note:**

SLPP packets are generated only on switches that are configured with SLPP - for example ERS 5000 Series or ERS 8300. The ERS 4500 switches do not support SLPP. When you enable SLPP Guard on an ERS 4500, the switch must be connected to another Avaya switch that supports SLPP and SLPP must be enabled on that switch.

STP BPDU filtering ignore-self

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

New in this release

Chapter 2: Introduction

This document provides information you need to configure VLANs, Spanning Tree and MultiLink Trunking for the Avaya Ethernet Routing Switch 4500 Series.

ACLI command modes

ACLI provides the following command modes:

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

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

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

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

Command mode and sample prompt	Entrance commands	Exit commands
User EXEC 4526T>	No entrance command, default mode	exit or logout
Privileged EXEC 4526T#	enable	exit or logout
Global Configuration 4526T(config)#	configure	To return to Privileged EXEC mode, enter: end or exit To exit ACLI completely, enter:

Command mode and sample prompt	Entrance commands	Exit commands
		logout
Interface Configuration 4526T(config-if) #	From Global Configuration mode: To configure a port, enter: interface fastethernet <port number> To configure a VLAN, enter: interface vlan <vlan number>	To return to Global Configuration mode, enter: exit To return to Privileged EXEC mode, enter: end To exit ACLI completely, enter: logout

See *Avaya Ethernet Routing Switch 4500 Series Fundamentals* (NN47205-102).

Navigation

This document contains the following chapters:

- [VLAN Fundamentals](#) on page 15
- [MLT Fundamentals](#) on page 29
- [STP Fundamentals](#) on page 41
- [ADAC Fundamentals](#) on page 51
- [LACP and VLACP Fundamentals](#) on page 67
- [Configuring VLANs using ACLI](#) on page 73
- [Configuring MultiLink Trunking using ACLI](#) on page 89
- [Configuring Spanning Tree Protocol using ACLI](#) on page 101
- [Configuring ADAC using ACLI](#) on page 127
- [LACP and VLACP configuration using ACLI](#) on page 143
- [Configuring VLANs using Enterprise Device Manager](#) on page 155
- [Configuring MultiLink Trunking using Enterprise Device Manager](#) on page 199
- [Configuring Spanning Tree Protocol using Enterprise Device Manager](#) on page 211
- [RSTP configuration using Enterprise Device Manager](#) on page 229
- [MSTP configuration using Enterprise Device Manager](#) on page 237
- [Configuring ADAC using Enterprise Device Manager](#) on page 251
- [Configuring LACP and VLACP using Enterprise Device Manager](#) on page 261

Chapter 3: VLAN Fundamentals

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

Virtual Local Area Networks

The Avaya Ethernet Routing Switch 4500 Series supports up to 25 concurrent VLANs.

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

Setting up virtual LANs (VLAN) is a way to segment networks to increase network capacity and performance without changing the physical network topology ([Figure 1: Port-based VLAN](#) on page 15). With network segmentation, each switch port connects to a segment that is a single broadcast domain. When you configure a switch port to be a member of a VLAN, you add it to a group of ports (workgroup) that belong to one broadcast domain.

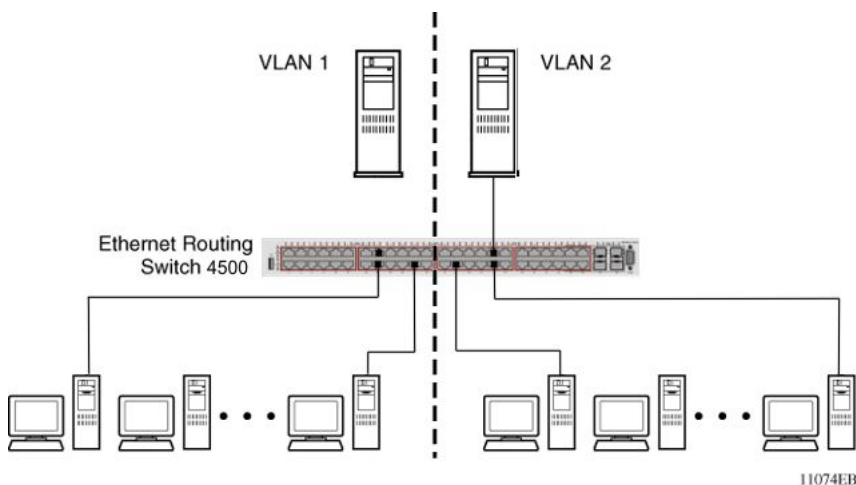


Figure 1: Port-based VLAN

With the Avaya Ethernet Routing Switch 4500 Series, you can assign ports to VLANs using the command line interface (CLI) or the Enterprise Device Manager (EDM). You can assign different ports (and associated devices) to different broadcast domains to provide network flexibility. You can reassign VLANs to accommodate network moves, additions, and changes, to eliminate the need to change physical cabling.

IEEE 802.1Q Tagging

The Avaya Ethernet Routing Switch 4500 Series operates in accordance with the IEEE 802.1Q tagging rules. Important terms used with the 32-bit 802.1Q tagging feature are

- **VLAN identifier (VID):** the 12-bit portion of the VLAN tag in the frame header that identifies an explicit VLAN. When other types of VLANs are enabled, the values enabled in the management interfaces can override this default value.
- **Port VLAN identifier (PVID):** a classification mechanism that associates a port with a specific VLAN. For example, a port with a PVID of 3 (PVID =3) assigns all untagged frames received on this port to VLAN 3.
- **Tagged frame:** a frame that contains the 32-bit 802.1q field (VLAN tag) and identifies the frame as belonging to a specific VLAN.
- **Untagged frame:** a frame that carries no VLAN tagging information in the frame header.
- **VLAN port members:** a group of ports that are all members of a particular VLAN. A port can be a member of one or more VLANs.
- **Untagged member:** a port configured as an untagged member of a specific VLAN. When an untagged frame exits the switch through an untagged member port, the frame header remains unchanged. When a tagged frame exits the switch through an untagged member port, the tag is stripped and the tagged frame is changed to an untagged frame.
- **Tagged member:** a port configured as a tagged member of a specific VLAN. When an untagged frame exits the switch through a tagged member port, the frame header changes to include the 32-bit tag associated with the ingress port PVID. When a tagged frame exits the switch through a tagged member port, the frame header remains unchanged (original VID remains).
- **User priority:** a three-bit field in the header of a tagged frame. The field is interpreted as a binary number, therefore has a value of 0 to 7. The tagged frame uses this field to carry the user-priority across bridged LANs where the individual LAN segments may be unable to signal priority information.
- **Port priority:** the priority level assigned to untagged frames received on a port. This value becomes the user priority for the frame. Tagged packets obtain their user priority from the value in the 32-bit 802.1Q frame header.
- **Unregistered packet:** a tagged frame that contains a VID if the receiving port is not a member of that VLAN.
- **Filtering database identifier (FID):** the specific filtering and forwarding database within the Avaya Ethernet Routing Switch 4500 Series switch that is assigned to each VLAN. Each VLAN has a filtering database, which is called independent VLAN learning (IVL). IVLs can have duplicate MAC addresses in different VLANs.

The default configuration settings for the Avaya Ethernet Routing Switch 4500 Series have all ports set as untagged members of VLAN 1 with all ports configured as PVID = 1. Every VLAN is assigned a unique VLAN identifier (VID) that distinguishes it from all other VLANs. In the

default configuration example shown in [Figure 2: Default VLAN Settings](#) on page 17, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID=1). Untagged packets enter and leave the switch unchanged.

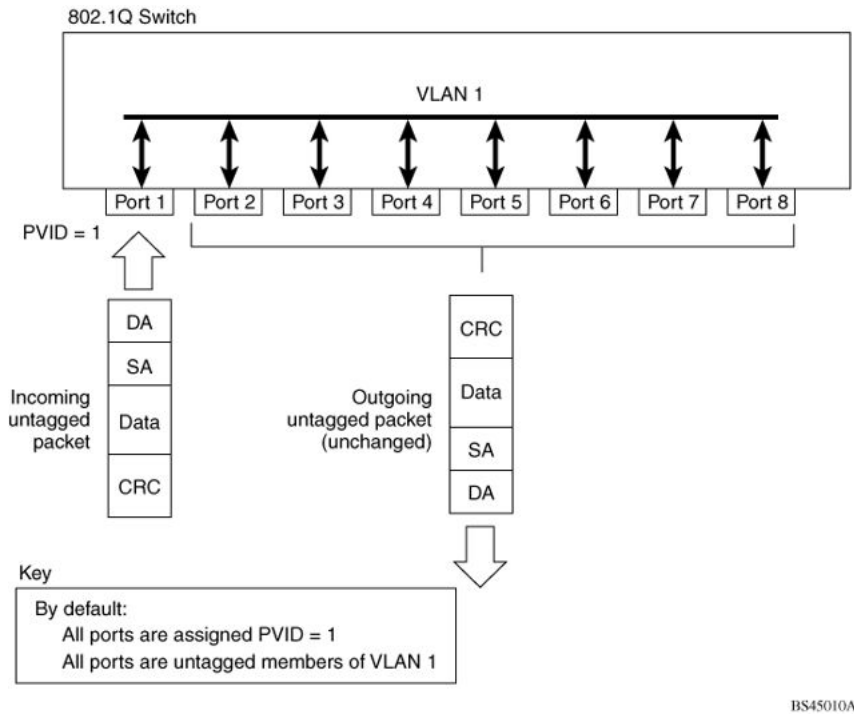


Figure 2: Default VLAN Settings

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

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

In [Figure 3: Port-based VLAN assignment](#) on page 17, untagged incoming packets are assigned directly to VLAN 2 (PVID = 2). Port 5 is as a tagged member of VLAN 2, and port 7 is an untagged member of VLAN 2.

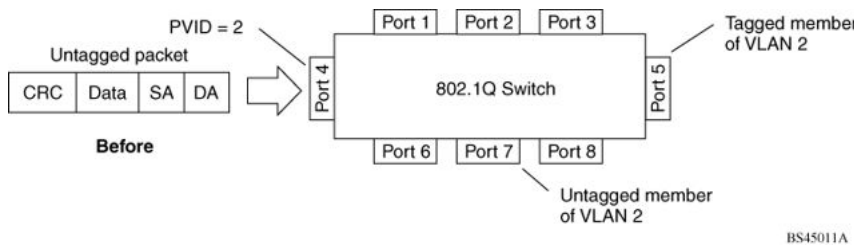


Figure 3: Port-based VLAN assignment

As shown in [Figure 4: 802.1Q tagging \(after port-based VLAN assignment\)](#) on page 18, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is a tagged

member of VLAN 2. The untagged packet remains unchanged as it leaves the switch through port 7, which is an untagged member of VLAN 2.

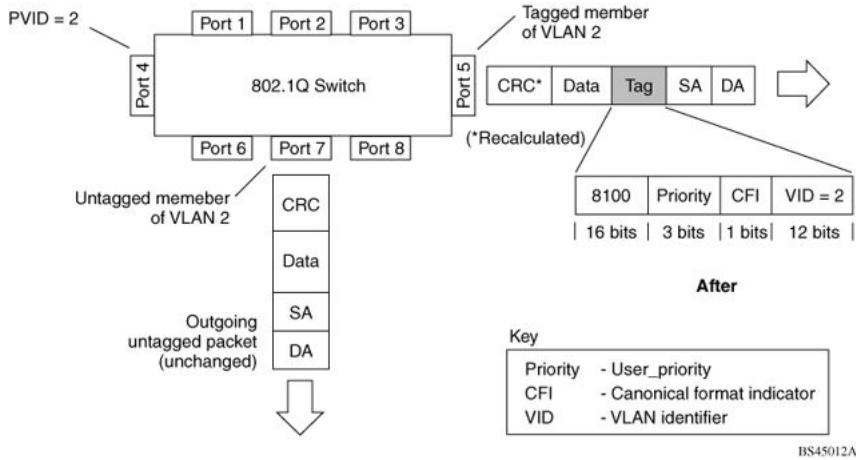


Figure 4: 802.1Q tagging (after port-based VLAN assignment)

In [Figure 5: Policy-based VLAN assignment](#) on page 18, untagged incoming packets are assigned to VLAN 3 (policy VLAN = 3, PVID = 2). Port 5 is a tagged member of VLAN 3, and port 7 is an untagged member of VLAN 3.

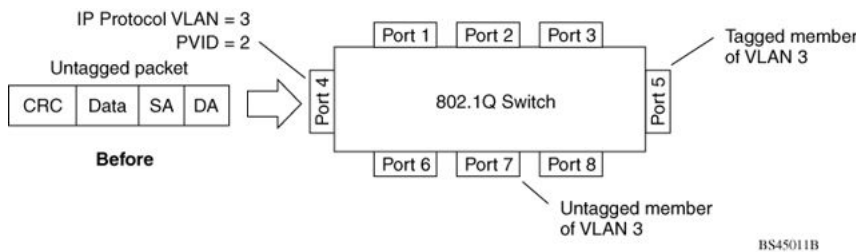


Figure 5: Policy-based VLAN assignment

As shown in [Figure 6: 802.1Q tagging \(after policy-based VLAN assignment\)](#) on page 19, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is a tagged member of VLAN 3. The untagged packet remains unchanged as it leaves the switch through port 7, which is an untagged member of VLAN 3.

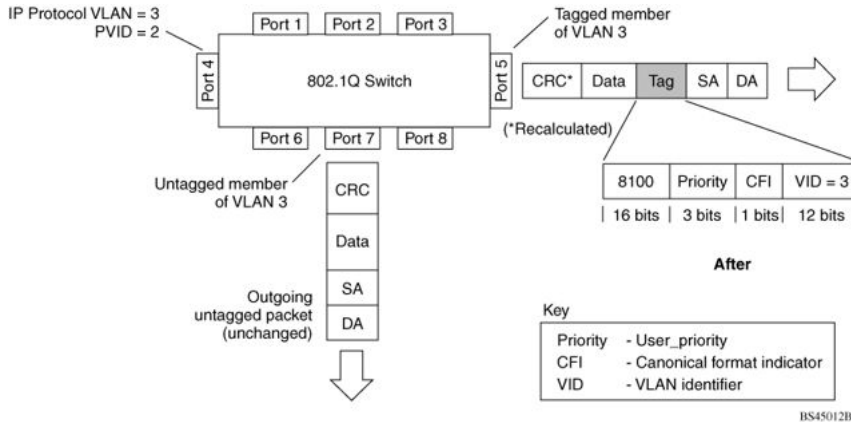


Figure 6: 802.1Q tagging (after policy-based VLAN assignment)

In [Figure 7: 802.1Q tag assignment](#) on page 19, tagged incoming packets are assigned directly to VLAN 2 because of the tag assignment in the packet. Port 5 is a tagged member of VLAN 2, and port 7 is an untagged member of VLAN 2.

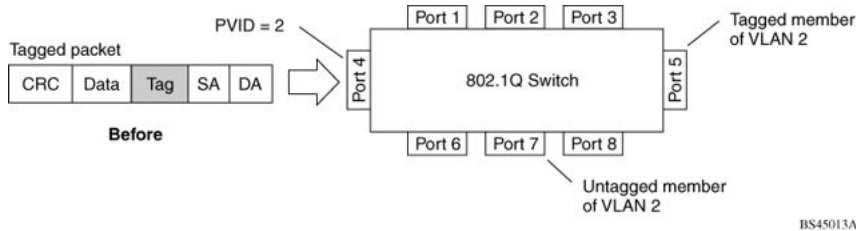


Figure 7: 802.1Q tag assignment

As shown in [Figure 8: 802.1Q tagging \(after 32-bit 802.1Q tag assignment\)](#) on page 20, the tagged packet remains unchanged as it leaves the switch through port 5, which as a tagged member of VLAN 2. However, the tagged packet is stripped (untagged) as it leaves the switch through port 7, which is an untagged member of VLAN 2.

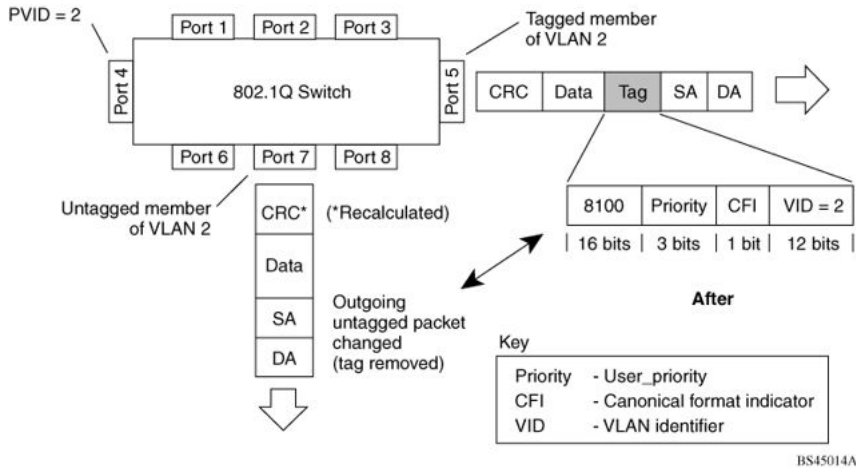


Figure 8: 802.1Q tagging (after 32-bit 802.1Q tag assignment)

In [Figure 9: 802.1Q tag assignment](#) on page 20, untagged incoming packets are assigned directly to a PVID of 2. Port 5 is a tagged member of PVID 2, and port 7 is an untagged member of PVID 2.

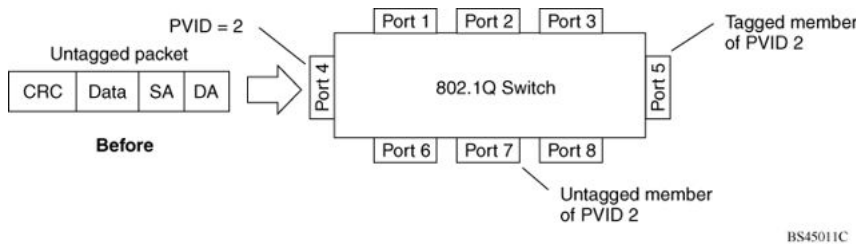


Figure 9: 802.1Q tag assignment

As shown in [Figure 10: 802.1Q tagging \(after 30-bit 802.1Q tag assignment\)](#) on page 21, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is a tagged member of PVID 2. The untagged packet remains unchanged as it leaves the switch through port 7, which is an untagged member of PVID 2.

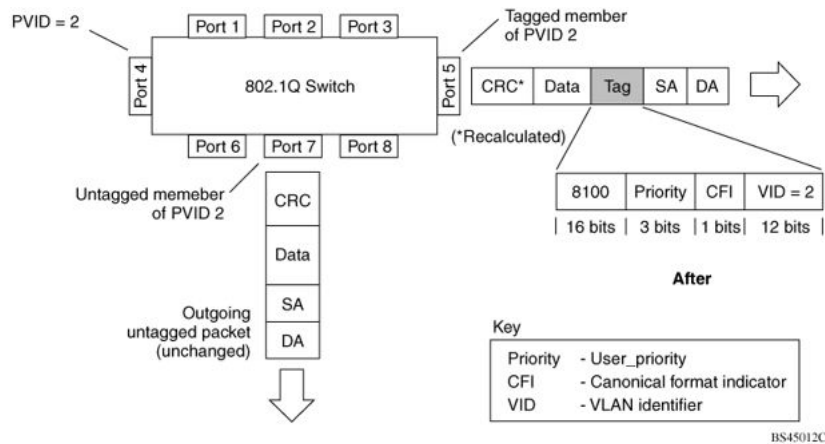


Figure 10: 802.1Q tagging (after 30-bit 802.1Q tag assignment)

VLANS Spanning Multiple Switches

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

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

VLANS spanning multiple 802.1Q tagged switches

[Figure 11: VLANS spanning multiple 802.1Q tagged switches](#) on page 22 shows VLANs spanning two Avaya Ethernet Routing Switch 4500 Series switches. The 32-bit 802.1Q tagging is enabled on S1, port 14 and on S2, port 13 for VLAN 1 and VLAN 2. Both ports are tagged members of VLAN 1 and VLAN 2.

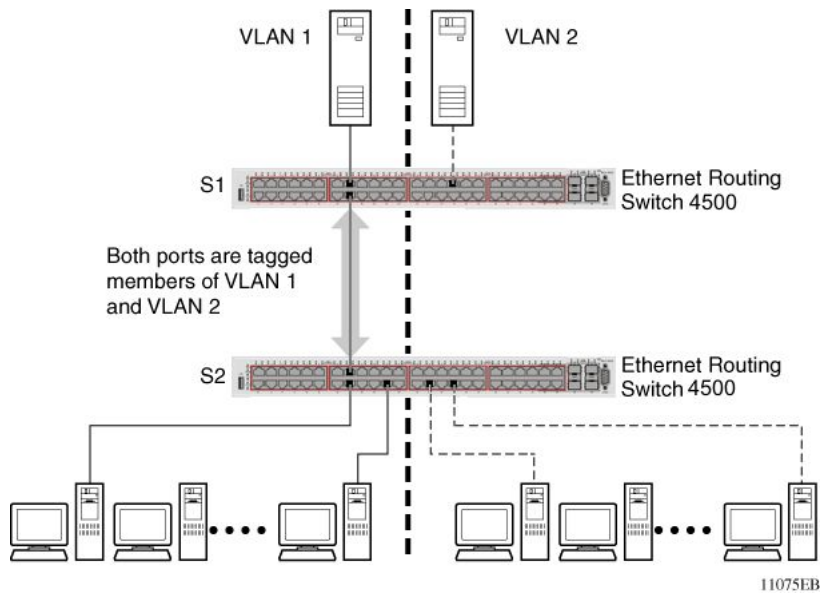


Figure 11: VLANs spanning multiple 802.1Q tagged switches

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

VLANs spanning multiple untagged switches

[Figure 12: VLANs spanning multiple untagged switches](#) on page 23 shows VLANs spanning multiple untagged switches. In this configuration, Switch S2 does not support 32-bit 802.1Q tagging and you must use a single switch port on each switch for each VLAN.

For this configuration to work properly, you must set spanning tree participation to Disabled (the STP is not supported across multiple LANs).

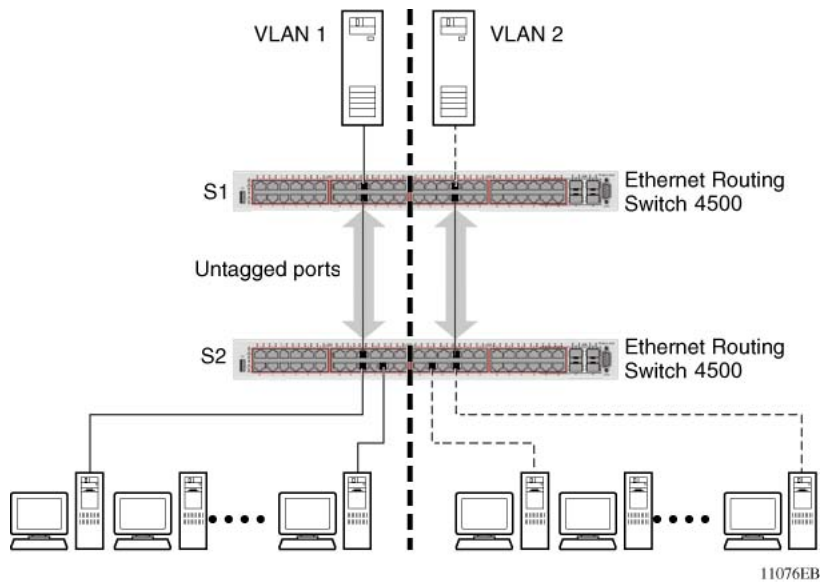


Figure 12: VLANs spanning multiple untagged switches

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

To connect multiple VLANs across switches with redundant links, you must disable the STP on all participating switch ports. [Figure 13: Possible problems with VLANs and Spanning Tree Protocol](#) on page 23 shows possible consequences of enabling the STP when you use VLANs between untagged (non-802.1Q tagged) switches.

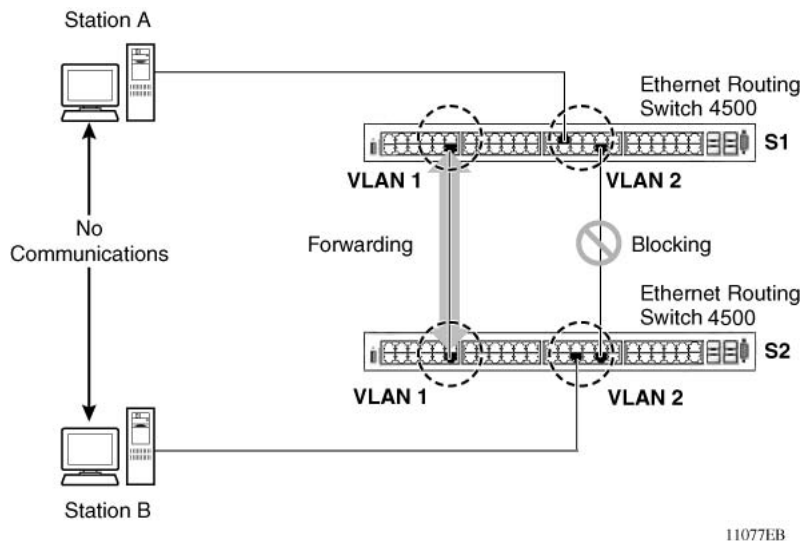


Figure 13: Possible problems with VLANs and Spanning Tree Protocol

As shown in [Figure 13: Possible problems with VLANs and Spanning Tree Protocol](#) on page 23, with STP enabled, only one connection between Switch S1 and Switch S2 forwards

traffic at any time. Communication fails between VLAN 2 of S1 and VLAN 2 of S2, blocking communications between Stations A and B.

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

VLAN Summary

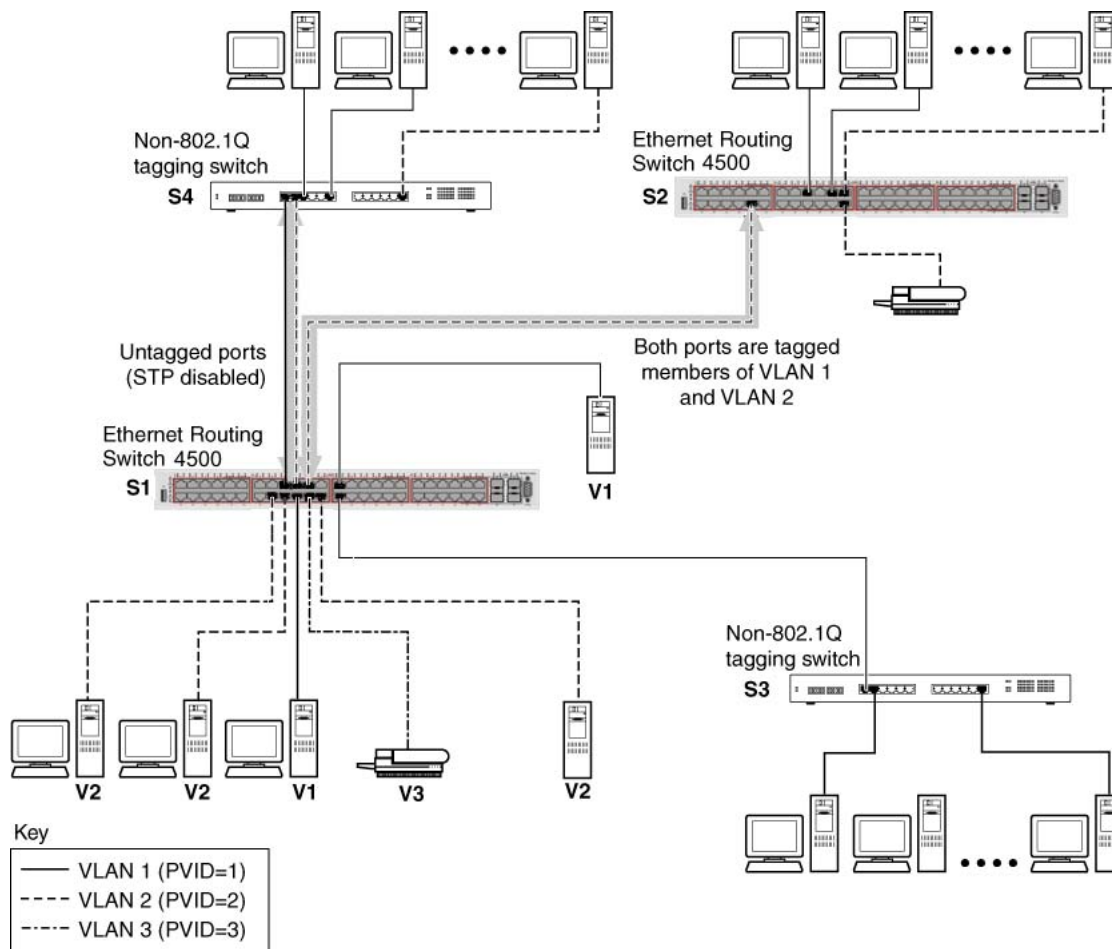
This section summarizes the VLAN examples discussed in the previous sections.

As shown in [Figure 14: VLAN configuration spanning multiple switches](#) on page 25, Switch S1 is configured with multiple VLANs:

- Ports 17, 20, 25, and 26 are in VLAN 1.
- Ports 16, 18, 19, 21, and 24 are in VLAN 2.
- Port 22 is in VLAN 3.

Because S4 does not support 32-bit 802.1Q tagging, you must use a single switch port on each switch for each VLAN (see [Figure 12: VLANs spanning multiple untagged switches](#) on page 23).

The connection to S2 requires only one link between the switches because S1 and S2 are both Avaya Ethernet Routing Switch 4500 Series switches that support 32-bit 802.1Q tagging (see [VLANs spanning multiple 802.1Q tagged switches](#) on page 21).



11079EB

Figure 14: VLAN configuration spanning multiple switches

VLAN Configuration Rules

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

- If a port is a trunk group member, all trunk members, except those belonging to a Link Aggregation Group (LAG), are added to or deleted from the VLAN.
- All ports involved in trunking must have the same VLAN configuration.
- VLANs do not depend on Rate Limiting settings.
- If a port is an Internet Gateway Management Protocol (IGMP) member on any VLAN, and you remove the port from a VLAN, the port IGMP membership is also removed.
- If you add a static router port to a different VLAN, you can configure the port as an IGMP member on that specific VLAN.

 **Important:**

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

VLAN Configuration Control

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

VLAN Configuration Control offers four options to control VLAN modification:

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

 **Important:**

Strict is the factory default setting.

- **Automatic:** Automatically add an untagged port to a new VLAN and automatically remove it from any previous VLAN membership. The PVID of the port automatically changes to the VID of the VLAN it joins. Because you first add the port to the new VLAN and then remove it from any previous membership, the Spanning Tree Group participation of the port remains enabled as long as the VLANs involved are in the same Spanning Tree Group.
- **AutoPVID:** This option functions in the same manner as previous AutoPVID functionality. When you add an untagged port to a new VLAN, you add the port to the new VLAN and the PVID assigned to the new VID without removing it from previous VLAN memberships. Using this option, an untagged port can have membership in multiple VLANs.
- **Flexible:** This option functions in a similar manner to disabling AutoPVID functionality. When you use this option, an untagged port can belong to an unlimited number of VLANs. Any new additions of an untagged port to a new VLAN does not change the PVID of that port.

VLAN Configuration Control applies only to ports with the tagging modes of **Untag All** and **Tag PVID Only**. VCC does not govern ports with the tagging modes of **Tag All** and **Untag PVID Only**. Ports with the tagging modes of **Tag All** and **Untag PVID Only** can belong to multiple VLANs regardless of VLAN Configuration Control settings and you must manually change their PVID.

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 port to flush out all addresses learned on the port

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

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

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.

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

Chapter 4: MLT Fundamentals

MultiLink trunks

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

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

Client-server configuration using MultiLink trunks

[Figure 15: Client/server configuration example](#) on page 30 shows an example of how you can use MultiLink Trunking in a client/server configuration. In this example, both servers connect directly to Switch S1. FS2 is connected through a trunk configuration. The switch-to-switch connections are through trunks.

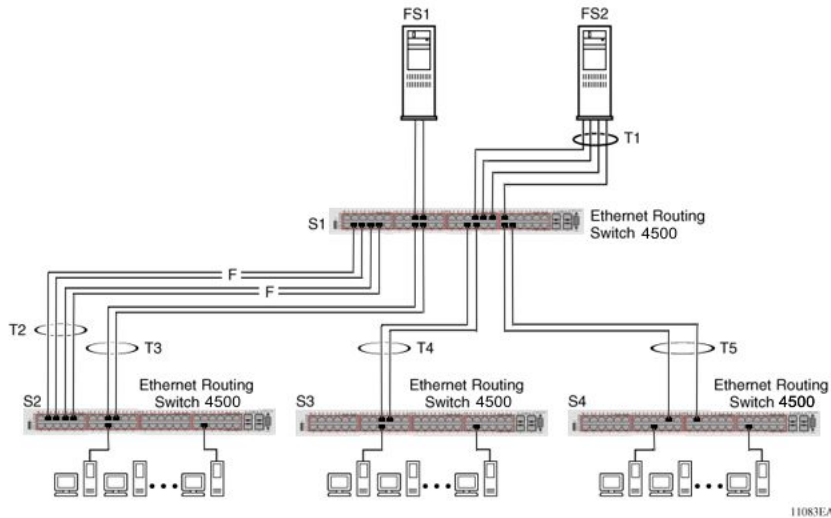


Figure 15: Client/server configuration example

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

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

Before Trunks are Configured

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

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

1. Read the configuration rules provided in the next section, [MultiLink Trunking Configuration Rules](#) on page 31.
2. Determine which switch ports (up to eight) are to become trunk members (the specific ports that make up the trunk). Each trunk requires a minimum of two ports.

! Important:

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

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

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

 **Important:**

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

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

 **Important:**

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

6. Consider how the addition of a trunk will affect existing VLANs.

MultiLink Trunking Configuration Rules

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

- Disabled ports can belong to MLTs. For traffic to flow to your configured MLT ports, be sure that you enable them (set to Enabled through the Port Configuration screen or through network management)..
- All trunk members must have the same VLAN configuration before you set the Trunk Status field on the Trunk Configuration screen to Enabled using ACLI.
- When you configure an active port in a trunk, the port becomes a trunk member when the Trunk Status field is Enabled. The spanning tree parameters for the port then change to reflect the new trunk settings.
- If you change the spanning tree participation of any trunk member to Enabled or Disabled, the spanning tree participation of all members of that trunk changes similarly.
- If you change the VLAN settings of any trunk member, the VLAN settings of all members of that trunk change similarly.
- A MLT/DMLT/LAG member can not be configured as a monitor port.
- A monitor port cannot monitor entire trunks; the monitor port can monitor trunk members.
- All trunk members must have identical Internet Gateway Management Protocol (IGMP) configurations.
- If you change the IGMP snooping configuration for any trunk member, the IGMP snooping settings for all trunk members change.
- Avaya recommends that you do not enable MAC Address Security on trunk ports.

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

MLT load-balancing

The Avaya Ethernet Routing Switch 4500 supports two modes of MLT load-balancing; Basic for layer 2 operation and Advanced for Layer 3 operation. You can configure this option using the `mlt <1-32> loadbalance` CLI command. You can also use the `show mlt hash-calc` CLI command to display the MLT hashing for a particular source or destination address.

The 4500 Series switch uses the following formula to perform MLT load-balancing:

- Mode 3 (basic) hash algorithm:

```
Index=DA[42:40]^DA[34:32]^DA[26:24]^DA[18:16]^DA[10:8]^DA[2:0]^VLAN[10
:
8]^VLAN[2:0]^Ethertype[10:8]^Ethertype[2:0]^SRC_MODID[2:0]^SRC_PORT_TG
ID[2:0]
```

- Mode 6 (advanced) hash algorithm:

```
Index=SIP[122:120]^SIP[114:112]^SIP[106:104]^SIP[98:96]^SIP[90:88]^SI
P[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_UDP_SPORT[10:8]^TCP_U
DP_SPORT[2:0]^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_UDP_DPORT[10:8
]^TCP_UDP_DPORT[2:0]
```

Index is the MLT/LAG link member index starting from zero.

Table 1: Formula variables

Variable	Definition
^	XOR operation on the specified number of bits in []
DA / SA	Destination or source MAC Address
SA	Source MAC Address
VLAN	VLAN tag

Variable	Definition
Ethertype	Ethernet Type Field
DIP / SIP	Destination or source IP Address
TCP_UDP_DPORT/ TCP_UDP_SPORT	Destination or source TCP or UDP port
SRC_MODID	ASIC system number identifier. Each ASIC inside the switch is using one ModuleID, starting from zero to the number of ASICs used by the switch; 24 or 26 port variants use a single ASIC, so in standalone mode their ModuleID is 0, while 48 or 50 port variants use 2 ASICs per switch. When a switch is part of a stack the ModuleIDs for the ASICs are calculated using the following formula $4 * (\text{StackUnitNumber} - 1) + \text{Local ASIC Number}$
SRC_PORT_TGID	Ingress port number or the trunk number (zero based). The port number is the ASIC port number, not the front panel port number. For the unshared ports on the 24/26 ports models the physical port number is the logical port number minus one. For the unshared ports on the 48/50 ports models, the physical port number for the first 24 ports is the logical port number minus one, for the front panel ports 25-48 the physical port number is the front panel port number (logical number) minus 25.

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

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

MLT Enable or Disable Whole Trunk

The MLT Enable or Disable Whole Trunk feature is user-configurable switch-wide. The feature is in a disabled state by default. When you the enable or disable MLT or DMLT groups, the operational state of the links that make up the bundle are not changed by default. When you disable MLT or DMLT groups, a traffic loop within a network can occur. The Avaya Ethernet Routing Switch 4500 supports the ability to change this operational mode using the MLT Enable or Disable Whole Trunk capability.

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

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

 **Important:**

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

Removal of MLT restrictions

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

Add and delete links from existing MultiLink trunks

You cannot add or remove ports from an Avaya Ethernet Routing Switch 4500 Series switch MLT, unless you first disable MLT. If you have disabled Whole Trunk functionality, then you should be aware that disabling MLT does not disable the ports assigned to the MLT. If the MLT is disabled with Whole Trunk functionality disabled then the ports form separate links and could create a network loop if depending on other network configurations.

How a MultiLink trunk reacts to losing distributed trunk members

A MultiLink trunk ([Figure 16: Loss of distributed trunk member](#) on page 35) can cover separate units in a stack configuration. If a unit in the stack becomes inactive due to loss of power or unit failure, the unaffected trunk members remain operational.

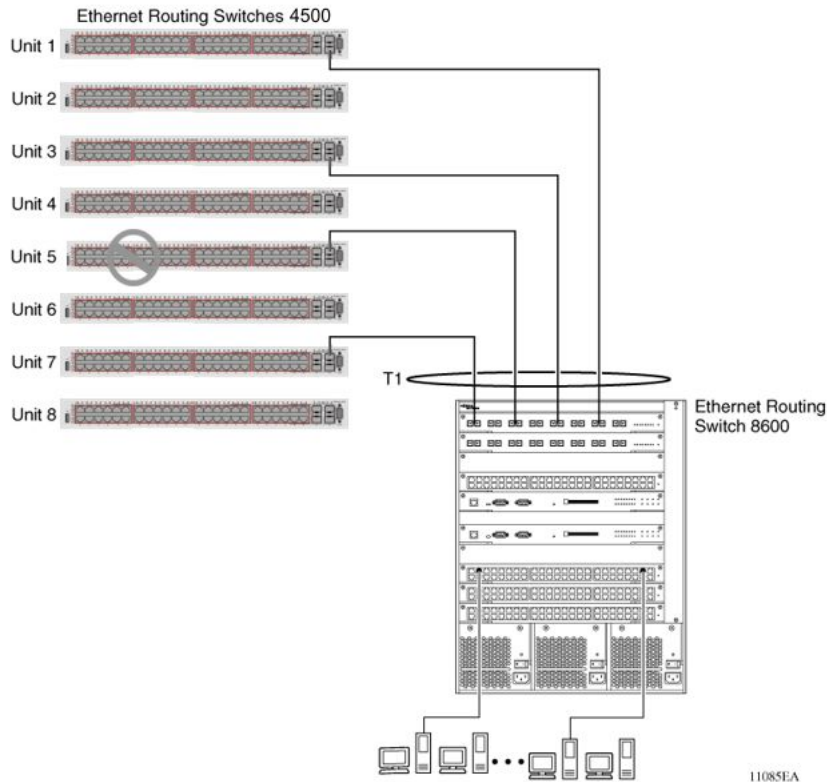


Figure 16: Loss of distributed trunk member

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

- VLAN configuration
- spanning tree configuration
- Port configuration
- IGMP configuration

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

Spanning Tree Considerations for MultiLink trunks

The spanning tree Path Cost parameter is recalculated based on the aggregate bandwidth of the trunk. For example, [Figure 17: Path Cost Arbitration](#) on page 36 shows a two-port trunk (T1) with two port members that operate at an aggregate bandwidth of 2 GB, with a comparable Path Cost of 1. Trunk 2 has two ports at 100 Mb/s with a Path Cost of 5.

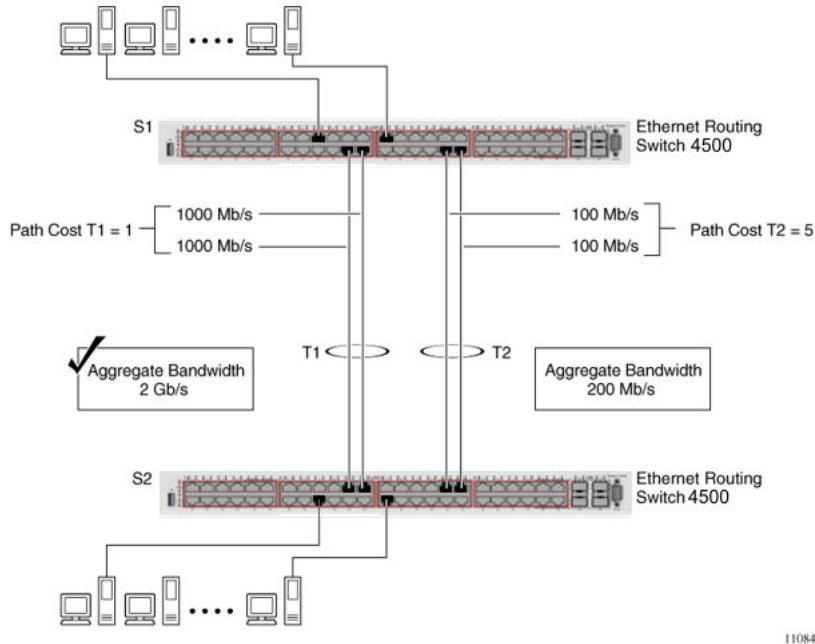


Figure 17: Path Cost Arbitration

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

! Important:

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

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

The switch can detect trunk member ports that are physically misconfigured. For example, in [Figure 18: Correctly Configured Trunk](#) on page 37, trunk member ports 2, 4, and 6 of Switch S1 are configured correctly to trunk member ports 7, 9, and 11 of Switch S2. The **show spanning-tree port** command output for each switch shows the port state field for each port in the Forwarding state.

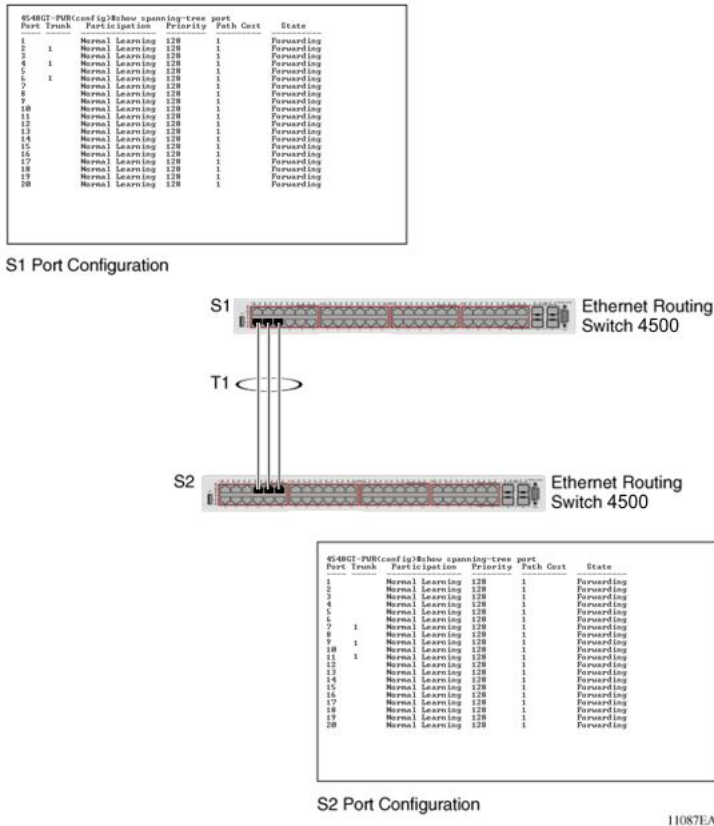


Figure 18: Correctly Configured Trunk

Important:

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

If trunk member port 11 of root Switch S2 is physically disconnected and then reconnected to port 13, the `show spanning-tree port` command output for Switch S1 changes to show port 6 in the Blocking state, [Figure 19: Detecting a Misconfigured Port](#) on page 38.

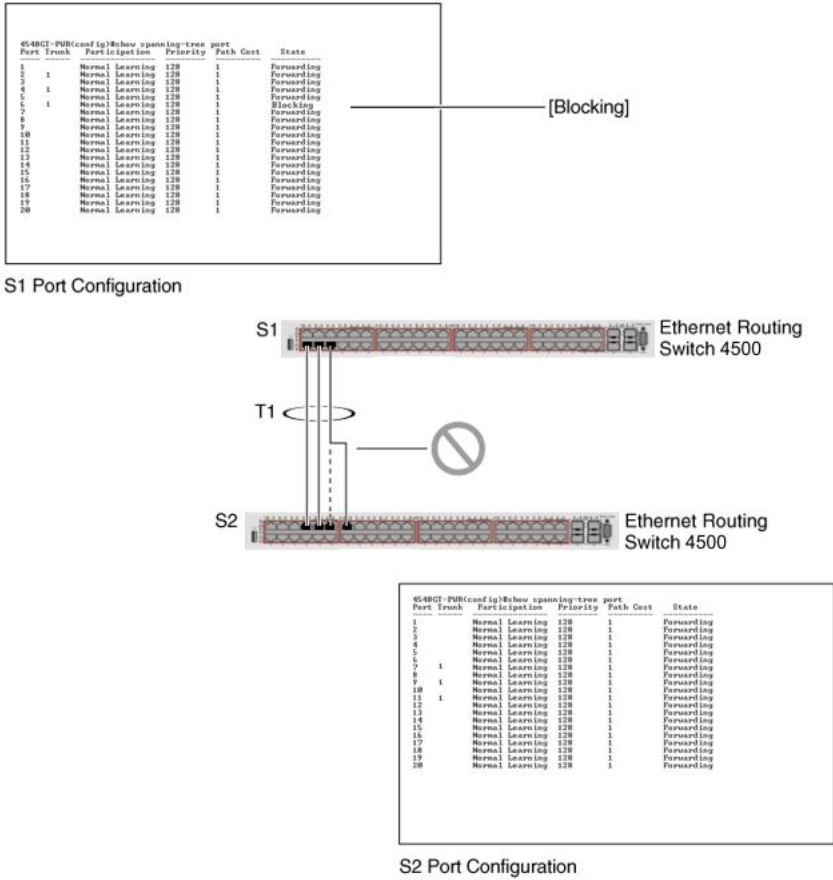


Figure 19: Detecting a Misconfigured Port

! Important:

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

Additional Tips About the MultiLink Trunking Feature

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

To change port membership in MultiLink Trunking, you must perform this procedure:

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

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

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

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

SLPP Guard

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

When you use the ERS4500 in combination with other Avaya switches that support Simple Loop Protection Protocol (SLPP) and Avaya's Switch Clustering (SMLT) - for example, ERS 5000 Series or ERS 8300 - the SLPP Guard feature provides additional network loop protection.

Because the ERS4500 does not support SLPP, the switch does not generate SLPP packets on ports that have SLPP Guard enabled, but when you enable SLPP Guard on switch ports, they can receive SLPP packets. When the system receives the SLPP packet it can generate a local log message, syslog message, and SNMP traps. When you enable SLPP Guard on a switch port and the switch receives an SLPP packet on that port, SLPP Guard can immediately disable the port administratively, for a predetermined interval.

For example: ERS4500 port 1 connects to ERS8300 port 1/1, the links are configured for SMLT, and a loop is created. With SLPP enabled on port 1/1, the ERS8300 transmits SLPP packets from that port. With SLPP Guard enabled on ERS4500 port 1, when ERS 4500 port 1 receives an SLPP packet the system automatically shuts ERS 4500 port 1 down, preventing the possibility of data looping between ERS4500 port 1 and ERS8300 port 1/1. After the predetermined interval expires, SLPP Guard re-enables the port. As an option, you can configure SLPP Guard to administratively disable the port indefinitely.

 **Note:**

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

Chapter 5: STP Fundamentals

Spanning Tree Protocol groups

The Avaya Ethernet Routing Switch 4500 Series supports the Spanning Tree Protocol (STP) as defined in IEEE 802.1D. The Spanning Tree Protocol detects and eliminates logical loops in a bridged or switched network. When multiple paths exist, the spanning tree algorithm configures the network so that a bridge or switch uses only the most efficient path. If that path fails, the protocol automatically reconfigures the network activate another path, thus sustaining network operations.

The Avaya Ethernet Routing Switch 4500 Series supports multiple spanning tree groups (STG). The Avaya Ethernet Routing Switch 4500 Series supports a maximum of eight STGs, either all in one stand-alone switch or across a stack. Multiple STGs provide multiple data paths, which can be used for load-sharing and redundancy. Enable load sharing between two switches using multiple STGs by configuring each path with a different VLAN and then assigning each VLAN to a separate STG. Each STG is independent. Each STG sends its own Bridge Protocol Data Units (BPDU), and you must independently configure each STG.

The STG, or bridge group, forms a loop-free topology that includes one or more virtual LANs (VLAN). The Avaya Ethernet Routing Switch 4500 Series supports multiple instances (eight) of STGs that run simultaneously.

The Avaya Ethernet Routing Switch 4500 Series supports a maximum of 256 VLANs. With a maximum of 8 STGs, on average, each STG can have 32 VLANs.

In the default configuration of the Avaya Ethernet Routing Switch 4500 Series, a single STG with the ID of 1 includes all ports on the switch. This STG is the default STG. Although you can add ports or delete ports from the default STG, you cannot delete the default STG (STG1) itself from the system. Also you cannot delete the default VLAN (VLAN1) from STG1.

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

Important:

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

You must create all other STGs, except the Default STG. To become active, you must enable each STG after its creation. Each STG is assigned an ID number from 2 to 8 (the Default STG

is assigned the ID number 1). Ports or VLANs are assigned to an active STG. However, a port that is not a member of a VLAN cannot join an STG.

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

Disable and delete an STG when you no longer need it. The procedure is to disable the STG, delete all VLAN and port memberships, and then delete the STG.

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

 **Important:**

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

STG Configuration Guidelines

This section provides important information about configuring STGs:

- You must create an STG must by performing these steps:
 - Create the STG.
 - Add the existing VLAN and port memberships.
 - Enable the STG.
- When you create a VLAN, that VLAN automatically belongs to STG 1, the default STG. If the VLAN is to be in another STG, move the VLAN by assigning it to another STG.
- You must move a newly created VLAN to an existing STG by performing these steps:
 - Create the VLAN.
 - Add the VLAN to an existing STG.
- You cannot move or delete VLAN1 from STG1.
- VLANs must be in a single STG; a VLAN cannot span multiple STGs. By confining VLANs within a single STG, you avoid problems with spanning tree blocking ports and loss of connectivity within the VLAN. When a VLAN spans multiple switches, the VLAN must be within the same spanning tree group (have the same STG ID) across all the switches.
- You cannot add a port that is a member of no VLAN to any STG. You must add the port must to a VLAN, and add that VLAN to the desired STG.
- Tagged ports can belong to more than one STG, but untagged ports can belong to only one STG.
- When a tagged port belongs to more than one STG, the egress BPDUs are tagged to distinguish the BPDUs of one STG from those of another STG.

- Because some STP-compliant devices do not support tagging, you can configure whether to send tagged or untagged BPDUs, even from tagged ports. The VLAN ID for the tagged BPDUs is 4000+STG ID.
- The default VLAN ID for tagged BPDUs is as follows:
 - 4001--STG1
 - 4002--STG2
 - 4003--STG3
 - 4004--STG4
 - 4005--STG5
 - 4006--STG6
 - 4007--STG7
 - 4008--STG8
- You can select a VLAN ID for tagged BPDUs for each STG. Valid VLAN IDs are 1 to 4094.
- Tagged BPDUs cannot use the same VID as an active VLAN.
- An untagged port cannot span multiple STGs.
- When you remove a port from a VLAN that belongs to an STG, that port is also removed from the STG. However, if that port belongs to another VLAN in the same STG, the port remains in the STG.
- As an example, assume that port 1 belongs to VLAN1, and that VLAN1 belongs to STG1. When you remove port 1 from VLAN1, port 1 is also removed from STG1. However, if port 1 belongs to both VLAN1 and VLAN2 and both VLANs belong to STG1, removing port 1 from VLAN1 does not remove port 1 from STG1 because VLAN2 is still a member of STG1.
- You must disable an STG before you can delete it.
- You can configure a unique multicast address for STGs 1 to 4 only.

Spanning Tree Fast Learning

Spanning Tree Fast Learning is an enhanced port mode supported by the Ethernet Routing Switch 4500 Series. If you enable Spanning Tree Fast Learning on a port with no other bridges, the port starts more quickly after a switch initialization or a spanning tree change. The port passes through the normal blocking and learning states before the forwarding state, but the hold times for these states is the bridge hello timer (2 seconds by default) instead of the bridge forward delay timer (15 seconds by default).

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

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

 **Important:**

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

STG port membership mode

The Avaya Ethernet Routing Switch 4500 supports two different STP port membership modes: normal and automatic. In the normal mode, when you assign a port to VLAN X and VLAN X is in STP group Y, the port does not automatically become a member of STP group Y. In automatic mode, when you assign a port to VLAN X and VLAN X is in STP group Y, the port automatically becomes a member of STP group Y.

802.1t path cost calculation

You can configure the switch to calculate the STG path cost using either the IEEE 802.1D standard or the IEEE 802.1t standard. The 802.1t standard is a maintenance extension to the 802.1D standard which provides more bits for spanning tree costs, thus provides a larger range of costs which can better support the higher speed links which can be supported on the Avaya Ethernet Routing Switch 4500. It is recommended to use 802.1t mode if using 10 Gigabit links and other switches in the network support 802.1t. The mode can be changed using the ACLI command, `spanning-tree cost-calc-mode`.

802.1D compliancy support

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

Rapid Spanning Tree Protocol

The standard Spanning Tree implementation in 4500 Series switches is based on IEEE 802.1D. This implementation results in a slow response to a topology change in the network (for example, a dysfunctional link in a network).

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

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

Multiple Spanning Tree Protocol

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

The 4500 switch uses RSTP and MSTP to achieve the following:

- Reduce converging time from 30 seconds to less than 2 seconds when a topology change occurs in the network (that is, the port goes up or down).
- Eliminate unnecessary flushing of the MAC database and flooding of traffic to the network with a new Topology Change mechanism.
- Obtain backward compatibility with other switches that run legacy 802.1D STP or Avaya MSTG (STP group 1 only).
- Under MSTP mode, simultaneously support eight instances of RSTP. Instance 0 or CIST is the default group, which includes default VLAN 1. Instances 1 to 7 are called MSTIs 1-7.
- Run Avaya MSTG, RSTP, or MSTP.

Interoperability with legacy STP

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

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

Differences in STP and RSTP port roles

RSTP is an enhanced version of STP. These two protocols have similar parameter sets.

[Table 2: Differences in port roles for STP and RSTP](#) on page 46 lists the differences in port roles for STP and RSTP. STP supports two port roles, while RSTP supports four port roles.

Table 2: Differences in port roles for STP and RSTP

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

Edged Port

RSTP supports the Edged Port parameter. When a port is connected to a nonswitch device such as a PC or a workstation, you must configure the port as an Edged port for fast convergence. An active Edged port goes directly to Forwarding state with no delay. An Edged port becomes a non-Edged port if it receives a BPDU.

Path cost values

RSTP and MSTP recommend new path cost values that support a wide range of link speeds. [Table 3: Recommended path cost values](#) on page 46 lists the recommended path cost values.

Table 3: Recommended path cost values

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

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

Rapid convergent

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

With RSTP and MSTP, information received on a port can be sent immediately if the port malfunctions, instead of waiting for the Maximum Age time.

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

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

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

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

Switch A is the Root.

Negotiation Process

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

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

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

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

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

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

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

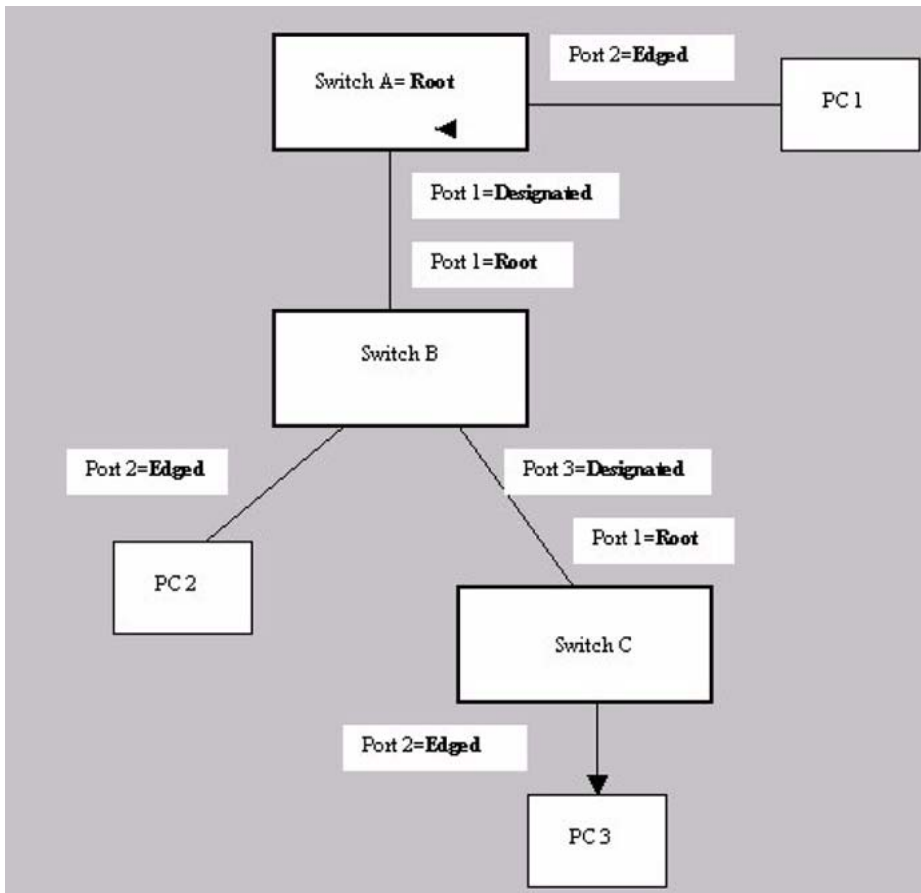


Figure 20: Negotiation process

The RSTP convergent time depends on how quickly the switch can exchange BPDUs during negotiation and the number of switches in the network. For a 4500 Series switch, the convergent time depends on the hardware platform and the number of active applications that run on the switch.

BPDU-Filtering

Ethernet Switches 4500 series support the BPDU-Filtering feature for STG, RSTP, and MSTP.

The Spanning Tree Protocol detects and eliminates logical loops in a bridged or switched network. Any bridge that participates in the spanning tree exchanges information with other

bridges using configuration messages known as Bridge Protocol Data Units (BPDU). Based on the BPDU information exchange, the bridge with the lowest bridge ID becomes the root. This process is called the root selection process.

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

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

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

 **Important:**

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

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

- The port is immediately put in the operational disabled state.
- A trap is generated and the following log message is written to the log:

```
BPDU received on port with BPDU-Filtering enabled. Port <x> has been disabled.
```

- The port timer starts.
- The port stays in the operational disabled state until the port timer expires.

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

You can enable and disable the BPDU-Filtering feature on a per-port basis. The BPDU-Filtering timer is user-configurable for each port and has a valid range of between 10 and 65 535 seconds. The port timer is disabled if it is configured as 0.

For details on configuring BPDU Filtering, see [Configuring STP BPDU filtering using ACLI](#) on page 101 and [Configuring STP BPDU filtering for specific ports using EDM](#) on page 212.

STP BPDU filtering ignore-self

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

Chapter 6: ADAC Fundamentals

Autodetection and Autoconfiguration of IP Phones

Ethernet Switch software supports Autodetection and Autoconfiguration (ADAC) of IP Phones. With ADAC, you can automatically configure the switch to support and prioritize IP Phone traffic.

When ADAC is enabled and an Avaya IP Phone is connected to the switch, the switch automatically configures the 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 ports) or is indirectly connected to the Call Server using a network uplink (through the Uplink ports).

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

- **Untagged-Frames-Basic:**

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

- **Untagged-Frames-Advanced:**

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

- **Tagged Frames:**

Use this mode when you want an advanced configuration and the IP Phones are sending tagged traffic. This mode provides the same configuration as the Untagged-Frames-Advanced mode, but with tagged frames. As with the Untagged-Frames-Advanced mode, ADAC creates a Voice VLAN that includes the Call Server or Uplink ports, as applicable, and all telephony ports. While Traffic prioritization is configured automatically, tagging and PVID settings are user configurable.

ADAC operation

The following sections provide detailed explanations of ADAC operation.

Auto-detection of IP Phones

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

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

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

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

The two methods of auto-detection are by MAC address or using LLDP (IEEE 802.1ab). Auto-detection by MAC address is based on using predefined MAC addresses to determine that the specified port is connected to an Avaya IP phone. For more information and the list of defined MAC address ranges, see [Auto-Detection by MAC address](#) on page 52.

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 54.

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

Auto-Detection by MAC address

When this feature is enabled on a port, the switch checks all MAC addresses of packets received on the port. If a received MAC address falls within the range of known Avaya IP Phone MAC addresses, ADAC determines that the specified port is connected to an Avaya IP Phone and initiates the required configuration. ADAC is supported for a maximum of 32 devices per port, but in most cases, there will be only one IP phone and one PC on each port. The ERS 4500 Series has a default range of MAC addresses configured to be recognized as Avaya IP Phones by ADAC.

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

Table 4: Default ADAC MAC address ranges

Lower End	Higher End
00-0A-E4-01-10-20	00-0A-E4-01-23-A7
00-0A-E4-01-70-EC	00-0A-E4-01-84-73
00-0A-E4-01-A1-C8	00-0A-E4-01-AD-7F
00-0A-E4-01-DA-4E	00-0A-E4-01-ED-D5
00-0A-E4-02-1E-D4	00-0A-E4-02-32-5B
00-0A-E4-02-5D-22	00-0A-E4-02-70-A9
00-0A-E4-02-D8-AE	00-0A-E4-02-FF-BD
00-0A-E4-03-87-E4	00-0A-E4-03-89-0F
00-0A-E4-03-90-E0	00-0A-E4-03-B7-EF
00-0A-E4-04-1A-56	00-0A-E4-04-41-65
00-0A-E4-04-80-E8	00-0A-E4-04-A7-F7
00-0A-E4-04-D2-FC	00-0A-E4-05-48-2B
00-0A-E4-05-B7-DF	00-0A-E4-06-05-FE
00-0A-E4-06-55-EC	00-0A-E4-07-19-3B
00-0A-E4-08-0A-02	00-0A-E4-08-7F-31
00-0A-E4-08-B2-89	00-0A-E4-09-75-D8
00-0A-E4-09-BB-9D	00-0A-E4-09-CF-24
00-0A-E4-09-FC-2B	00-0A-E4-0A-71-5A
00-0A-E4-0A-9D-DA	00-0A-E4-0B-61-29
00-0A-E4-0B-BB-FC	00-0A-E4-0B-BC-0F
00-0A-E4-0B-D9-BE	00-0A-E4-0C-9D-0D
00-13-65-FE-F3-2C	00-13-65-FF-ED-2B
00-15-9B-FE-A4-66	00-15-9B-FF-24-B5
00-16-CA-00-00-00	00-16-CA-01-FF-FF
00-16-CA-F2-74-20	00-16-CA-F4-BE-0F
00-17-65-F6-94-C0	00-17-65-F7-38-CF
00-17-65-FD-00-00	00-17-65-FF-FF-FF
00-18-B0-33-90-00	00-18-B0-35-DF-FF
00-19-69-83-25-40	00-19-69-85-5F-FF

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

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

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

Auto-Detection by LLDP (IEEE 802.1ab)

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

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

Detailed configuration example

The following commands provide a detailed configuration example.

- Default a device.
- Disable on port 5 MAC detection.

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

- Enable ADAC on port 5 and globally.

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

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

```
ERS 4500 (config) #adac voice-vlan 200
ERS 4500 (config) #adac uplink-port 10
ERS 4500 (config) #adac op-mode untagged-frames-advanced
```

- Verify that above settings were applied.

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

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

```
ERS4500 (config-if)#sho adac in 5
Port  Type      Auto   Oper   Auto
-----  -
5      T      Enabled  Enabled  Applied      No Change  Untag FVID Only
```

Auto-Configuration of IP Phones

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

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

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

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

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

- auto-detect becomes disabled on the port
- the ports operational state becomes disabled

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

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

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

Initial user settings

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

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

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



Important:

The ADAC feature automatically creates and manages the Voice-VLAN on the switch. Manually configuring the Voice-VLAN causes issues with ADAC operation.

You must also ensure that voice traffic entering the Uplink port is tagged with the Voice VLAN ID. This configuration must be made on all switches on the path to the Call Server.

Port Restrictions

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

Call Server ports must not be:

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

Uplink ports must not be:

- a Monitor Port in port mirroring
- a Telephony port

- an EAP port
- the Call Server port

Telephony ports must not be:

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

Operating modes

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

- [QoS Settings](#) on page 57
- [Untagged-Frames-Basic operating mode](#) on page 57
- [Untagged-Frames-Advanced operating mode](#) on page 58
- [Tagged-Frames operating mode](#) on page 60

QoS Settings

ADAC QoS configuration is applied to:

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

Untagged-Frames-Basic operating mode

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

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

- Configure the IP Phones to send untagged frames.
- Connect only IP Phones to a port. (You cannot connect a device that is not an Avaya IP Phone to the same port.)
- Ensure that the Filter Unregistered Frames option is set to disabled on the ADAC-enabled ports (or that the ports belong to at least one VLAN).

Untagged-Frames-Basic QoS configuration

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

Autoconfiguration performs the following:

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

DSCP to 0x2E is the default for ADAC. If you configure 802.1AB (LLDP) MED Network Policy to use a different DSCP marking, this marking is used by ADAC.

- creates a policy containing the above

Untagged-Frames-Basic VLAN configuration

In the Untagged-Frames-Basic operating mode, Autoconfiguration also performs the following VLAN configuration:

Tagging of Telephony ports is set to Untagged.

Untagged-Frames-Advanced operating mode

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

- Configure the IP Phones to send untagged frames.
- Connect only IP Phones to a port. (You cannot connect a device that is not an Avaya IP Phone to the same port.)
- Ensure that Filter Unregistered Frames option is set to disabled on the ADAC-enabled ports (or that the ports belong to at least one VLAN).
- Specify the Voice-VLAN ID and either the Call Server port or the Uplink port, as applicable.
- If the switch is not directly connected to the Call Server, ensure that the telephony packets coming from the Call Server through the Uplink port are tagged with the Voice-VLAN ID.

Untagged-Frames-Advanced QoS configuration

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

Table 5: Untagged-Frames-Advanced QoS configuration

For traffic coming from:	Autoconfiguration does the following:
Telephony ports	<ul style="list-style-type: none"> creates an Unrestricted Interface with all Telephony ports (each time a new Telephony port is detected, it will be added to this interface) creates an IP Filter (all fields set to Ignore) and an IP Filter Group uses Premium Service (transmit frame, update DSCP to 0x2E, Drop Precedence to Loss Sensitive, Update Priority to 6) DSCP to 0x2E is the default for ADAC. If you configure 802.1AB (LLDP) MED Network Policy to use a different DSCP marking, this marking is used by ADAC. creates a policy containing all of the above
Call Server ports	adds the Call Server port to the interface group created for Telephony ports
Uplink ports	<ul style="list-style-type: none"> creates an Unrestricted Interface containing the Uplink port creates a Layer 2 Filter, with EtherType IP, VLAN set to ID of the Voice-VLAN and Tagged (all other fields set to Ignore) uses Premium Service creates a policy containing all of the above

Untagged-Frames-Advanced VLAN configuration

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

Table 6: Untagged-Frames-Advanced VLAN configuration

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

Port type	Membership	Tagging	PVID
			Auto-PVID setting is ignored.)

Tagged-Frames operating mode

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

- Configure the IP Phones to send tagged frames with the ID of the Voice-VLAN.
- Connect at least one Avaya IP Phone to a telephony port. (In this mode, other devices can be connected to the same port; for example, when a PC is connected directly to the IP phone.)
- Ensure that the Filter Unregistered Frames option is set to disabled on the ADAC-enabled ports. (Otherwise, no source MAC address can be learned for incoming packets tagged with the Voice VLAN ID, meaning that no phone can be detected.)
- Specify the Voice-VLAN ID and either the Call Server port or the Uplink port, as applicable.
- If the switch is not directly connected to the Call Server, ensure that the telephony packets coming from the Call Server through the Uplink port are tagged with the Voice-VLAN ID.

Tagged-Frames QoS configuration

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

Table 7: Tagged-Frames QoS configuration

For traffic coming from:	Autoconfiguration does the following:
Telephony ports	<ul style="list-style-type: none"> • creates an Unrestricted Interface (Call Server interface ID will be a member of this interface group) • creates an IP Filter (all fields set to Ignore) and an IP Filter Group • uses Premium Service • creates a policy containing all of the above
IP Phones and Uplink ports	<ul style="list-style-type: none"> • create an Unrestricted Interface containing all Telephony ports and Uplink ports • create a Layer 2 Filter, with EtherType IP, VLAN set to ID of the Voice-VLAN and Tagged (all other fields set to Ignore) • use Premium Service • create a policy containing all of the above

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

Tagged-Frames VLAN configuration

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

Table 8: Tagged-Frames VLAN configuration

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

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

Dynamic VLAN Autoconfiguration

Important:

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

The following describes the details of the ADAC VLAN configuration:

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

automatically by ADAC follow the rules of the Flexible mode, regardless of the current value of VCC. Any settings that you manually make on ADAC ports follow the current VCC mode, similar to a non-ADAC port.

ADAC and stacking

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

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

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

This same scenario also occurs for the Uplink port.

Lost Call Server Port or Uplink Port

Beginning with release 5.4, the Avaya Ethernet Routing Switch 4500 maintains ADAC operation if the designated call server or uplink ports become unreachable. This allows the switch to maintain any current communications between end devices located on the switch.

ADAC Uplink port as part of trunk

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

Uplink port as part of MLT in a stack

The Uplink port can be part of an MLT. If the unit containing the Uplink port in a stack is removed from the stack, the lowest port from the same MLT becomes the new Uplink port.

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

ADAC and LACP enabled on an Uplink port

To set an Uplink port as LACP-enabled, you must first configure and enable Link Aggregation Control Protocol (LACP) on the port, and then you can set the port as the Uplink port.

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

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

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

Any changes to the LAG mode, from active to passive or from passive to active, have no effect on ADAC.

Disabling LACP on an Uplink port

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

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

Uplink port as part of LACP in a stack

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

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

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

ADAC and EAP configuration

ADAC and Extensible Authentication Protocol (EAP) are mutually exclusive on the Call Server port and the Uplink port.

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

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

To enable ADAC on an EAP port, you must perform the following:

1. On the switch, globally enable support for non-EAP MAC addresses. (In ACLI, use the `eap multihost allow-non-eap-enable` command.)
2. On each telephony port, enable support for non-EAP MAC addresses. (In ACLI, use the `eap multihost port <port> allow-non-eap-enable` command.)
3. On each telephony port, enable EAP Multihost. (In ACLI, use the `eap multihost port <port> enable` command.)
4. On the telephony ports, ensure that Guest VLAN is disabled. (In ACLI, use the `show eap guest-vlan` command.)
5. On the switch, enable EAP globally. (In ACLI, use the `eap enable` command.)
6. Configure and enable ADAC on the ports.

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

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

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

ADAC User Restrictions

After ADAC is enabled, you cannot:

- erase the Voice-VLAN
- remove auto-configured ports from Voice-VLAN

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

You can:

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

Adding the Voice-VLAN to another STG

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

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

Disabling ADAC

Disabling the ADAC feature means the deletion of all configurations (except as noted in [ADAC User Restrictions](#) on page 64), including the following:

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

ADAC management

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

Chapter 7: LACP and VLACP Fundamentals

IEEE 802.3ad Link Aggregation

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

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

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

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

Link aggregation employs the following principles and concepts:

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

The network manager can control the determination and binding directly by manipulating the state variables of Link Aggregation (for example, Keys). In addition, automatic

determination, configuration, binding, and monitoring can occur by using a Link Aggregation Control Protocol (LACP).

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

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

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

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

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

Link aggregation rules

The 4500 Series switch link aggregation groups operate under the following rules:

- Link aggregation groups are formed using LACP.
- All ports in a link aggregation group must connect to the same far-end system.
- All ports in a link aggregation group must operate in full-duplex mode.
- You must configure all ports in a link aggregation group to the same port speed.
- All ports in a link aggregation group must be in the same VLANs.
- In stack mode, ports in a link aggregation group can be on different units to form a distributed LAG (DLAG).
- LACPDU are transmitted and received on all ports in the link aggregation group.
- Link aggregation is compatible with the Spanning Tree Protocol (STP).
- Link aggregation groups must be in the same STP groups.
- STP BPDUs are transmitted and received only on the first link in the group.
- A maximum of 32 link aggregation groups are supported.
- A maximum of 8 active links are supported per LAG.
- Unlimited standby links are supported for each LAG (for example, if a switch or stack has one LAG, you can configure all non active LAG link ports as standby ports for that LAG).
- The MLT/LAG is a logical port. The STP protocol is computing the topology using this logical port, not on individual MLT/LAG member ports. The logical port is represented by

the first MLT/LAG port. The STP events related to MLT/LAG are logged using the first MLT/LAG port.

The maximum number of LAGs is 32, and the maximum number of active links for each group is 8. With Link Aggregation, you can configure more than 8 links in one LAG. The first eight high-priority links are active links, and together, they form a trunk group. The fifth low-priority link remains in standby mode. When an active link goes down, the standby link becomes active and is added to the trunk group. For more information, see [LACP and VLACP configuration using ACLI](#) on page 143 and [Configuring LACP and VLACP using Enterprise Device Manager](#) on page 261.

The failover process is as follows:

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

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

VLACP

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

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

Virtual LACP (VLACP) overview

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

[Figure 21: Problem description \(1 of 2\)](#) on page 70 provides an illustration of these limitations. While the Enterprise networks shown can connect their aggregated Ethernet trunk groups through a service provider network connection (for example, through a VPN), far-end failures cannot be signaled with Ethernet-based functions that operate end-to-end through the service provider cloud.

In [Figure 21: Problem description \(1 of 2\)](#) on page 70, the MLT (between Enterprise switches S1 and S2) extends through the service provider (SP) network.

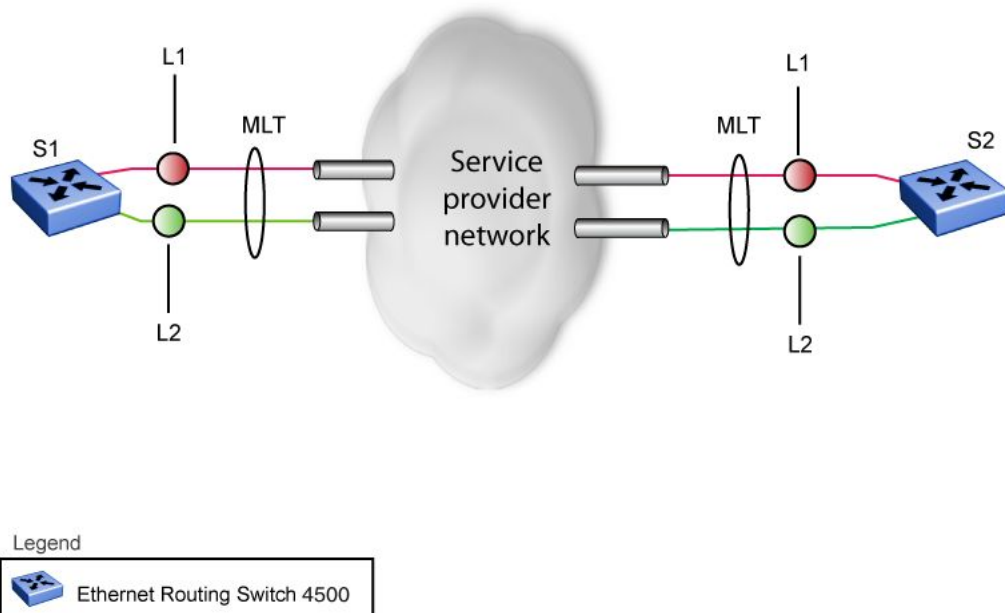


Figure 21: Problem description (1 of 2)

As shown in [Figure 22: Problem description \(2 of 2\)](#) on page 71, 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.

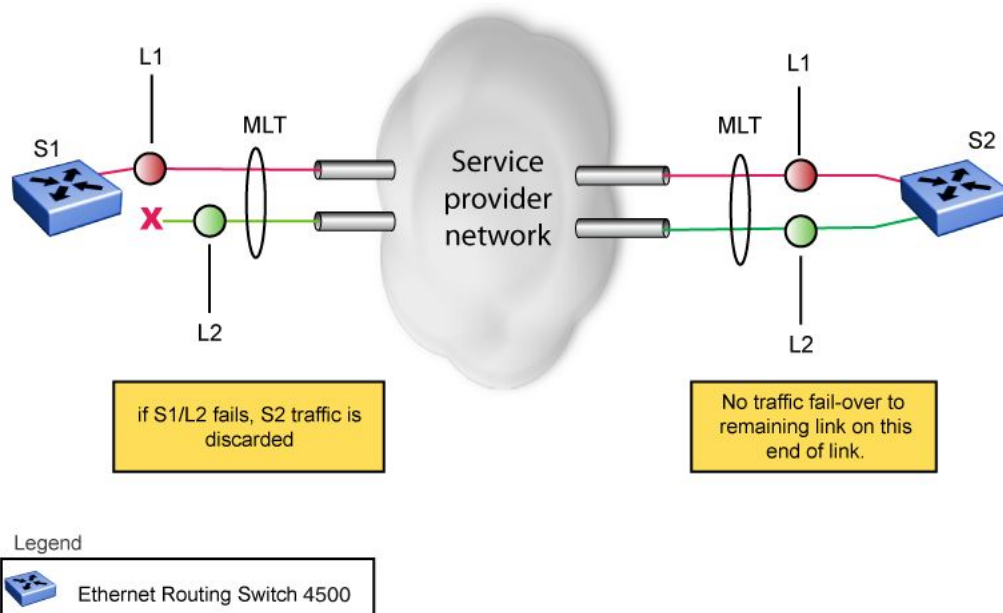


Figure 22: Problem description (2 of 2)

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

Avaya has developed an extension to LACP, which is called Virtual LACP (VLACP). This extension can provide an end-to-end failure detection mechanism. With VLACP, far-end failures can be detected allowing an MLT to fail over properly when end-to-end connectivity is not guaranteed for certain links in an aggregation group. VLACP prevents the failure scenario shown in [Figure 22: Problem description \(2 of 2\)](#) on page 71.

Prior to Release 5.5, when you used VLACP, the switch could not detect certain types of unidirectional communication outage. With the addition to the software of two new VLACP Protocol Data Unit (PDU) subtypes, DOWN and HOLD, the switch manages certain operational situations better. For example:

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

VLACP features

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

- VLACP is configured per port. A port can be an individual port or a member of an MLT.
- When you set VLACP parameters for a trunk port, the settings are applied to all trunk members.
- For VLACP to operate properly, there must be a logical point-to-point connection (Layer 2 tunnel) between the two endpoints.
- VLACP does not work for point-to-multipoint connections.
- On each port that has VLACP enabled, VLACPDUs are sent periodically. If VLACPDUs are not received on a particular link, that link is taken down after a configurable timeout period.
- For the current software release, VLACP is supported on Ethernet interfaces only.
- VLACP can run independently as a port-to-port protocol or on top of MLT or LACP protocol.
- VLACP packets are untagged because they operate at the port level and not the VLAN level.
- The Destination Mac Address used in VLACPDUs is configurable. The MAC Address must be a multicast MAC Address so that it is always flooded. This allows the exchange of VLACPDUs from end to end.

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

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

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

Troubleshooting

Error logs are created for the following failures and errors:

- An incorrect PDU, such as wrong destination MAC addresses received
- An inability to enable VLACP on a port due to unallowable Destination MAC addresses
- A port index that is out of range
- A port was blocked by VLACP (a log message is also generated when the port is unblocked)

Chapter 8: Configuring VLANs using ACLI

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

Displaying VLAN information

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

Procedure steps

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

```
show vlan [type {port | protocol-ipEther2 | protocol-ipx802.3 |
protocol-ipx802.2 | protocol-ipxSnap | protocol-ipxEther2 |
protocol-decEther2 | protocol-snaEther2 | protocol-Netbios |
protocol-xnsEther2 | protocol-vinesEther2 | protocol-ipv6Ether2
| protocol-Userdef |protocol-RarpEther2} [protocol-sna802.2]]
[vid <1-4094>]
```

Variable Definitions

Variable	Value
vid <1-4094>	Enter the number of the VLAN to display.
type	Enter the type of VLAN to display: <ul style="list-style-type: none">• port - port-based• protocol - protocol-based (see following list)
Protocol parameter	Description
protocol-ipEther2	Specify an ipEther2 protocol-based VLAN.
protocol-ipx802.3	Specify an ipx802.3 protocol-based VLAN.
protocol-ipx802.2	Specify an ipx802.2 protocol-based VLAN.

Variable	Value
protocol-ipxSnap	Specify an ipxSnap protocol-based VLAN.
protocol-ipxEther2	Specify an ipxEther2 protocol-based VLAN.
protocol-decEther2	Specify a decEther2 protocol-based VLAN.
protocol-snaEther2	Specify an snaEther2 protocol-based VLAN.
protocol-Netbios	Specify a NetBIOS protocol-based VLAN.
protocol-xnsEther2	Specify an xnsEther2 protocol-based VLAN.
protocol-vinesEther2	Specify a vinesEther2 protocol-based VLAN.
protocol-ipv6Ether2	Specify an ipv6Ether2 protocol-based VLAN.
protocol-Userdef	Specify a user-defined protocol-based VLAN.
protocol-RarpEther2	Specify a RarpEther2 protocol-based VLAN.
protocol-sna802.2	Specify a sna802.2 VLAN.

Displaying VLAN interface information

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

Procedure steps

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

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

Displaying port membership in VLANs

Use the following procedure to display port membership in VLANs.

Procedure steps

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

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

Displaying the management VLAN

Use the following procedure to display the management VLAN.

Procedure steps

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

```
show vlan mgmt
```

Configuring the management VLAN

Use the following procedure to configure the management VLAN.

Procedure steps

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

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

Deleting the management VLAN IP address

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

Procedure steps

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

```
default ip address
```



Note:

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

Resetting the management VLAN

Use the following procedure to reset the management VLAN.

Procedure steps

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

```
default vlan mgmt
```

Creating VLANs

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

Procedure steps

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


```
vlan create <1-4094> [name <line>] type {port | protocol-  
decEther2 | protocol-ipEther2 | protocol-ipv6Ether2 | protocol-  
ipx802.2 | protocol-ipx802.3 | protocol-ipxEther2 | protocol-  
ipxSnap | protocol-Netbios | protocol-RarpEther2 | protocol-  
sna802.2 | protocol-snaEther2 | protocol-vinesEther2 |  
protocol-xnsEther2 | protocol-Userdef <4096-65534> }
```



Important:

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

Variable Definitions

Variable	Value
<1-4094>	Enter as an individual VLAN ID to create a single VLAN or enter as a range of VLAN IDs to create multiple VLANs simultaneously.  Note: VLAN ID values 4001 through 4008 are reserved and cannot be used.
name <line>	Specifies a unique alphanumeric name for an individual VLAN. Do not enter a value for this parameter when you are creating multiple VLANs simultaneously.
type	Enter the type of VLAN to create: <ul style="list-style-type: none"> • port - port-based • protocol - protocol-based (see following list)
protocol-decEther2	Specify a decEther2 protocol-based VLAN.
protocol-ipEther2	Specify an ipEther2 protocol-based VLAN.
protocol-ipv6Ether2	Specify an ipv6Ether2 protocol-based VLAN.
protocol-ipx802.2	Specify an ipx802.2 protocol-based VLAN.
protocol-ipx802.3	Specify an ipx802.3 protocol-based VLAN.
protocol-ipxEther2	Specify an ipxEther2 protocol-based VLAN.
protocol-ipxSnap	Specify an ipxSnap protocol-based VLAN.
protocol-Netbios	Specify a NetBIOS protocol-based VLAN.
protocol-sna802.2	Specify an sna802.2 protocol-based VLAN.
protocol-snaEther2	Specify an snaEther2 protocol-based VLAN.
protocol-xnsEther2	Specify an xnsEther2 protocol-based VLAN.
protocol-vinesEther2	Specify a vinesEther2 protocol-based VLAN.
protocol-Userdef <4096-65534>	Specify a user-defined protocol-based VLAN.

Deleting a VLAN

Use the following procedure to delete a VLAN.

Procedure steps

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

```
vlan delete <1-4094>
```



Important:

VLAN 1 cannot be deleted.

Variable Definitions

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

Removing a MAC address from allowed flooding

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

Procedure steps

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

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

Configuring VLAN name

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

Procedure steps

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

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

Configuring automatic PVID

Use the following procedure to enable automatic PVID.

Procedure steps

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

```
auto-pvid
```

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

Configuring port VLAN settings

Use the following procedure to configure port VLAN settings.


Procedure steps

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

```
vlan ports [<portlist>] [tagging {enable | disable | tagAll |  
untagAll | tagPvidOnly | untagPvidOnly}] [pvid <1-4094>]
```

```
[filter-untagged-frame {enable | disable}] [filter-
unregistered-frames {enable | disable}] [priority <0-7>] [name
<line>]
```

Variable Definitions

Variable	Value
<portlist>	Enter the port numbers to be configured for a VLAN.
tagging {enable disable tagAll untagAll tagPvidOnly untagPvidOnly}	Enables or disables the port as a tagged VLAN member for egressing packet.
pvid <1-4094>	Sets the PVID of the port to the specified VLAN.
filter-untagged-frame {enable disable}	Enables or disables the port to filter received untagged packets.
filter-unregistered-frames {enable disable}	Enables or disables the port to filter received unregistered packets. Enabling this feature on a port means that any frames with a VID to which the port does not belong to are discarded.
priority <0-7>	Sets the port as a priority for the switch to consider as it forwards received packets.
name <line>	Enter the name you want for this port.  Important: This option can only be used if a single port is specified in the <portlist>.

Configuring VLAN member ports


Use the following procedure to add or remove VLAN member ports.

Procedure steps

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


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

Variable Definitions

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

Configuring VLAN Configuration Control

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

VLAN Configuration Control offers four options for controlling VLAN modification:

- Strict
- Automatic
- AutoPVID
- Flexible

 **Important:**

Strict is the factory default setting.

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

To configure VCC using ACLI, see the following commands:

Displaying VLAN Configuration Control settings

Use the following procedure to display VLAN Configuration Control settings.

Procedure steps

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

```
show vlan configcontrol
```

Modifying VLAN Configuration Control

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

Procedure steps

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

```
vlan configcontrol <vcc_option>
```

Variable Definitions

Variable	Value
<vcc_option>	This parameter denotes the VCC option to use on the switch. The valid values are: <ul style="list-style-type: none">• automatic: Changes the VCC option to Automatic.• autopvid: Changes the VCC option to AutoPVID.• flexible: Changes the VCC option to Flexible.• strict: Changes the VCC option to Strict. This is the default VCC value.

Managing MAC address forwarding database table

 **Note:**

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

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

- [Displaying the MAC address forwarding table](#) on page 83
- [Configuring aging time for unseen MAC addresses](#) on page 84
- [Setting aging time for unseen MAC addresses to default](#) on page 84
- [Clearing the MAC address table on a VLAN](#) on page 85
- [Clearing the MAC address table](#) on page 85
- [Clearing the MAC address table on a FastEthernet interface](#) on page 86
- [Clearing the MAC address table on a trunk](#) on page 86
- [Removing a single address from the MAC address table](#) on page 87

Displaying the MAC address forwarding table

Use the following procedure to 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 steps

To display the MAC address forwarding table, use the following command from Privileged EXEC mode:

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

Variable Definitions

Variable	Value
vid <1-4094>	Enter the number of the VLAN for which you want to display the forwarding database. Default is to display the management VLAN's database.
aging-time	Display the time in seconds after which an unused entry is removed from the forwarding database.
address <H.H.H>	Display a specific MAC address if it exists in the database. Enter the MAC address you want displayed.
port <portlist>	Specify ports.

Configuring aging time for unseen MAC addresses

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

Procedure steps

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

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

Variable Definitions

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

Setting aging time for unseen MAC addresses to default

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

Procedure steps

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

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

Clearing the MAC address table

Use the following procedure to clear the MAC address table.

Prerequisites

Log on to the Privileged EXEC mode.

Procedure steps

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

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

Clearing the MAC address table on a VLAN

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

Prerequisites

Log on to the Privileged EXEC mode.

Procedure steps

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

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

Variable definition

Use the information in the following table to complete this procedure.

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

Clearing the MAC address table on a FastEthernet interface

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

Prerequisites

Log on to the Privileged EXEC mode.

Procedure steps

To clear the MAC address table on a FastEthernet interface, use the following command.

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

Variable definition

Use the information in the table to complete this procedure.

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

Clearing the MAC address table on a trunk

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

Prerequisites

Log on to the Privileged EXEC mode.

Procedure steps

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

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

Variable definition

Use the information in the table to complete this procedure.

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

Removing a single address from the MAC address table

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

Prerequisites

Log on to the Privileged EXEC mode.

Procedure steps

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

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

Variable definition

Use the information in the table to complete this procedure.

Configuring VLANs using ACLI

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

Chapter 9: Configuring MultiLink Trunking using ACLI

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

Configuring a Multi Link Trunk using ACLI

Use the following procedure to configure a MLT.

Procedure steps

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

```
mlt <id> [name <trunkname>] [enable | disable] [member <portlist>] [learning {disable | fast | normal}] [bpdu {all-ports | single-port}] [loadbalance <advance|basic>
```

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

Variable Definitions

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

Variable	Value
loadbalance	Specifies the type of MLT load balancing. <ul style="list-style-type: none">• advance—performs hashing based on layer2 criteria• basic—performs hashing based on layer3 criteria

Displaying MLT configuration using ACLI

Use the following procedure to display MLT configuration and utilization.

Procedure steps

To display MLT configuration and utilization, use the following command from Privileged EXEC mode:

```
show mlt [utilization] <1-32>
```

Viewing IP address-based MLT hashing information using ACLI

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

Procedure steps

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

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

Variable definitions

The following table defines parameters that you can enter with the **show mlt hash-calc <1-32> dest-ip <ip-add> src-ip <ip-add>** command.

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

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

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

```
ERS4500#show mlt hash-calc 1 dest-ip 172.16.2.1 src-ip
172.16.2.5
% MLT trunk is disabled.
```

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

```
ERS4500#show mlt hash-calc 1 dest-ip 172.16.2.1 src-ip
172.16.2.5
% MLT links are all down.
```

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

```
ERS4500#show mlt hash-calc 1 dest-ip 172.16.2.1 src-ip
172.16.2.5
Hash Calc: 1/24
```

Viewing MAC address-based MLT hashing using ACLI

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

Procedure steps

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

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

Variable definitions

The following table defines parameters that you can enter with the `show mlt hash-calc <1-32> dest-mac <h:h:h> src-mac <h:h:h>` command.

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

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

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

```
ERS4500#show mlt hash-calc 1 dest-mac 00-13-49-4b-04-74 src-
mac 00-1D-42-36-EC-40
% MLT trunk is disabled.
```

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

```
ERS4500#show mlt hash-calc 1 dest-mac 00-13-49-4b-04-74 src-
mac 00-1D-42-36-EC-40
% MLT links are all down.
```

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

```
ERS4500#show mlt hash-calc 1 dest-mac 00-13-49-4b-04-74 src-
mac 00-1D-42-36-EC-40
% You must use dest-ip and src-ip when MLT load-balancing
mode is advanced.
```

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

```
ERS4500#show mlt hash-calc 1 dest-mac 00-13-49-4b-04-74 src-
mac 00-1D-42-36-EC-40
% Hash Calc: 2/23
```

Displaying STG MLT properties using ACLI

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

Procedure steps

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

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

Configuring STP participation for MLTs using ACLI

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

Procedure steps

To set STP participation for MLTs, use the following command from Global Configuration mode:

```
mlt spanning-tree <1-32> [stp <1-8 | all > learning {disable | normal | fast}]
```

Variable Definitions

Variable	Value
<1 - 32>	Specify the ID of the MLT to associate with the STG.
stp <1 - 8 all >	Specify the spanning tree group.
learning {disable normal fast}	Specify the STP learning mode: <ul style="list-style-type: none"> • disable: disables learning • normal: sets the learning mode to normal • fast: sets the learning mode to fast

Enabling all ports shutdown in the MLT using ACLI

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

Prerequisites

Log on to the Global Configuration mode.

Procedure steps

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

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

Disabling MLT Enable or Disable Whole Trunk feature using ACLI

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

Prerequisites

Log on to the Global Configuration mode.

Procedure steps

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

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

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

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

Prerequisites

Log on to the Privileged EXEC mode.

Procedure steps

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

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

Job aid

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

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

Selecting an SLPP Guard Ethernet type using ACLI

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

Important:

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

Prerequisites

Log on to the GlobalConfiguration mode in ACLI.

Procedure steps

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

```
slpp-guard ethertype <0x1-0xffff>
```

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

```
default slpp-guard ethertype
```


Variable definitions

Variable	Value
<0x1-0xffff>	Specifies a hexadecimal value ranging from 0x1 to 0xffff. Use the prefix 0x to type the hexadecimal value.

Configuring SLPP Guard using ACLI

Use this procedure to configure SLPP Guard for switch ports.

Prerequisites

Log on to the FastEthernet Interface Configuration mode in ACLI.

Note:

SLPP packets are generated only on switches that are configured with SLPP - for example ERS 5000 Series or ERS 8300. The ERS 4500 switches do not support SLPP. When you enable SLPP Guard on an ERS 4500, the switch must be connected to another Avaya switch that supports SLPP and SLPP must be enabled on that switch.

Procedure steps

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

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

Variable definitions

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

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

Viewing the SLPP Guard status using ACLI

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

Prerequisites

Log on to the User EXEC mode in ACLI.

Procedure steps

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

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

Variable definitions

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

Job aid: show eapol multihost command output

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

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

 **Note:**

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

Chapter 10: Configuring Spanning Tree Protocol using ACLI

Configuring STP operation mode using ACLI

Use the following procedure to set the STP operational mode to STG (Avaya Multiple Spanning Tree Protocol), RSTP (802.1w Rapid Spanning Tree Protocol), or MSTP (802.1s Multiple Spanning Tree Protocol).

Procedure steps

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

```
spanning-tree op-mode {stpg | rstp | MSTP}
```

Configuring STP BPDU filtering using ACLI

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

Procedure steps

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

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

Variable Definitions

Variable	Value
port <portlist>	Specifies the ports affected by the command.
enable	Enables STP BPDU Filtering on the specified ports. The default value is disabled.
timeout <10-65535 0 >	When BPDU filtering is enabled, this indicates the time (in seconds) during which the port remains disabled after it receives a BPDU. The port timer is disabled if this value is set to 0. The default value is 120 seconds.

Configuring STP BPDU filtering ignore-self using ACLI

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

Prerequisites

Log on to the Global Configuration mode in ACLI.

Procedure steps

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

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

Variable definitions

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

Viewing the STP BPDU Filtering ignore-self status using ACLI

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

Prerequisites

Log on to the Privileged EXEC mode in ACLI.

Procedure steps

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

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

Creating and Managing STGs using ACLI

To create and manage Spanning Tree Groups, you can refer to the Command Line Interface commands listed in this section. Depending on the type of Spanning Tree Group that you want to create or manage, the command mode needed to execute these commands can differ.

In the following commands, the omission of any parameters that specify a Spanning Tree Group results in the command operating against the default Spanning Tree Group (Spanning Tree Group 1).

To configure STGs using ACLI, see the following:

Configuring path cost calculation using ACLI

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

Procedure steps

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

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

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

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

Configuring STG port membership using ACLI

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

Procedure steps

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

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

Displaying spanning tree configuration information using ACLI

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

Procedure steps

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

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

Variable Definitions

Variable	Value
stp <1-8>	Display specified Spanning Tree Group configuration; enter the number of the group to be displayed.
config port vlans	Display spanning tree configuration for <ul style="list-style-type: none">• config: the specified (or default) Spanning Tree Group• port: the ports within the Spanning Tree Group• vlans: the VLANs that are members of the specified Spanning Tree Group

Variable	Value
cost-calc-mode	Display the STG port membership mode.
op-mode	Display the STP operational mode (STG, RSTP, or MSTP).
port-mode	Display the STG port membership mode.

Creating a spanning tree group using ACLI

Use the following procedure to create a spanning tree group.

Procedure steps

To create a spanning tree group, use the following command from Global Configuration mode:

```
spanning-tree stp <1-8> create
```

Deleting a spanning tree group using ACLI

Use the following procedure to delete a spanning tree group.

Procedure steps

To delete a spanning tree group, use the following command from Global Configuration mode:

```
spanning-tree stp <1-8> delete
```

Enabling a spanning tree group using ACLI

Use the following procedure to enable a spanning tree group.

Procedure steps

To enable a spanning tree group, use the following command from Global Configuration mode:

```
spanning-tree stp <1-8> enable
```

Disabling a spanning tree group using ACLI

Use the following procedure to disable a spanning tree group.

Procedure steps

To disable a spanning tree group, use the following command from Global Configuration mode:

```
spanning-tree stp <1-8> disable
```

Configuring STP values by STG using ACLI

Use the following procedure to configure STP values by STG.

Procedure steps

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

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

Variable Definitions

Variable	Value
stp <1-8>	Specify the Spanning Tree Group; enter the STG ID.
forward-time <4-30>	Enter the forward time of the STG in seconds; the range is from 4–30, and the default value is 15.
hello-time <1-10>	Enter the hello time of the STG in seconds; the range is from 1–10, and the default value is 2.
max-age <6-40>	Enter the max-age of the STG in seconds; the range is from 6–40, and the default value is 20.

Variable	Value
priority {0000 1000 2000 3000 ... E000 F000}	Set the spanning tree priority (in Hex); if 802.1T compliant, this value must be a multiple of 1000.
tagged-bpdu {enable disable}	Set the BPDU as tagged or untagged. The default value for Spanning Tree Group 1 (default group) is untagged; the default for the other groups is tagged.
tagged-bpdu-vid <1-4094>	Set the VLAN ID (VID) for the tagged BPDU. The default value is from 4001–4008 for STG 1–8, respectively.
mcast-address <H.H.H>	Set the spanning tree multicast address.
add-vlan <1-4094>	Add a VLAN to the Spanning Tree Group.
remove-vlan <1-4094>	Remove a VLAN from the Spanning Tree Group.

Restoring default spanning tree value for a STG using ACLI

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

Procedure steps

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

```
default spanning-tree [stp <1-8>] [forward-time] [hello-time]
[max-age] [priority] [tagged-bpdu] [multicast-address]
```

Variable Definitions

Variable	Value
stp <1-8>	Disable the Spanning Tree Group; enter the STG ID.
forward-time	Set the forward time to the default value of 15 seconds.
hello-time	Set the hello time to the default value of 2 seconds.
max-age	Set the maximum age time to the default value of 20 seconds.
priority	Set spanning tree priority (in Hex); if 802.1T compliant, this value must be a multiple of 0x1000.

Variable	Value
tagged-bpdu	Set the tagging to the default value. The default value for Spanning Tree Group 1 (default group) is untagged; the default for the other groups is tagged.
multicast-address	Set the spanning tree multicast MAC address to the default.

Setting STP and STG participation using ACLI


Use the following procedure to set the Spanning Tree Protocol (STP) and multiple Spanning Tree Group (STG) participation for the ports within the specified Spanning Tree Group.

Procedure steps

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

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

Variable Definitions

Variable	Value
port <portlist>	Enable the spanning tree for the specified port or ports; enter port or ports you want enabled for the spanning tree.  Important: If you omit this parameter, the system uses the port number you specified when you issued the interface command to enter the Interface Configuration mode.
stp <1-8>	Specify the spanning tree group; enter the STG ID.
learning {disable normal fast}	Specify the STP learning mode: <ul style="list-style-type: none"> • disable: disables FastLearn mode • normal: changes to normal learning mode • fast: enables FastLearn mode
cost <1-65535>	Enter the path cost of the spanning tree; range is from 1–65535.

Variable	Value
[priority {00 10 < F0}	Set the spanning tree priority for a port as a hexadecimal value.

Setting default spanning tree values for ports using ACLI


Use the following procedure to set the spanning tree values for the ports within the specified Spanning Tree Group to the factory default settings.

Procedure steps

To set default values, use the following command from Interface Configuration mode:

```
default spanning-tree [port <portlist>] [stp <1-8>] [learning]
[cost] [priority]
```

Variable Definitions

Variable	Value
port <portlist>	Enable spanning tree for the specified port or ports; enter port or ports to be set to factory spanning tree default values.  Important: If this parameter is omitted, the system uses the port number specified when the interface command was used to enter Interface Configuration mode.
stp <1-8>	Specify the Spanning Tree Group to set to factory default values; enter the STG ID. This command places the port into the default STG. The default value for STG is 1.
learning	Set the spanning tree learning mode to the factory default value. The default value for learning is Normal mode.
cost	Set the path cost to the factory default value. The default value for path cost depends on the type of port.
priority	Set the priority to the factory default value. The default value for the priority is 0x8000.

Disable spanning tree for a port using ACLI


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

Procedure steps

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

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

Variable Definitions

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

STP 802.1D compliancy support configuration using ACLI

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

Enabling STP 802.1D compliancy support using ACLI

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

Prerequisites

Log on to the Global Configuration mode in ACLI.

Procedure steps

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

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

Disabling STP 802.1D compliancy support using ACLI

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

Prerequisites

Log on to the Global Configuration mode in ACLI.

Procedure steps

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

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

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

Viewing STP 802.1D compliancy support status using ACLI

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

Prerequisites

Log on to the User EXEC mode in ACLI.

Procedure steps

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

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

Job aid: show spanning-tree 802dot1d-port-compliance command output

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

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

Figure 23: show spanning-tree 802dot1d-port-compliance command output

STP 802.1t cost calculation support configuration using ACLI

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

Enabling STP 802.1t cost calculation support using ACLI

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

Prerequisites

Log on to the Global Configuration mode in ACLI.

Procedure steps

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

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

Disabling STP 802.1t cost calculation support using ACLI

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

Prerequisites

Log on to the Global Configuration mode in ACLI.

Procedure steps

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

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

Viewing STP 802.1t cost calculation status using ACLI

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

Prerequisites

Log on to the Privileged EXEC mode in ACLI.

Procedure steps

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

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

Job aid: show spanning-tree cost-calc-mode command output

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

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

Managing RSTP using ACLI

This section contains the following procedures:

Configuring RSTP parameters using ACLI

Use the following procedure to set the RSTP parameters which include forward delay, hello time, maximum age time, default path cost version, bridge priority, transmit holdcount, and version for the bridge.

Procedure steps

To configure RSTP parameters, use the following command in Global Configuration mode:

```
spanning-tree rstp [ forward-time <4 - 30>] [hello-time <1 - 10>] [max-age <6 - 40>] [pathcost-type {bits16 | bits32}] [priority {0000|1000|2000| ...| F000}] [tx-holdcount <1 - 10>] [version {stp-compatible | rstp}]
```

Variable Definitions

Variable	Value
forward-time <4- 30>	Set the RSTP forward delay for the bridge in seconds; the default is 15.
hello-time <1- 10>	Set the RSTP hello time delay for the bridge in seconds; the default is 2.

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

Configuring RSTP parameters per port using ACLI

Use the following procedure to set the RSTP parameters, which include path cost, edge-port indicator, learning mode, point-to-point indicator, priority, and protocol migration indicator on the single or multiple port.

Procedure steps

To configure RSTP parameters, use the following command from Interface Configuration mode:

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

Variable Definitions

Variable	Value
port <portlist>	Filter on list of ports.
cost <1 - 200000000>	Set the RSTP path cost on the single or multiple ports; the default is 200000.
edge-port {false true}	Indicate whether the single or multiple ports are assumed to be edge ports. This parameter sets the Admin value of edge port status; the default is false.
learning {disable enable}	Enable or disable RSTP on the single or multiple ports; the default is enable.

Variable	Value
p2p {auto force-false force-true}	Indicate whether the single or multiple ports are to be treated as point-to-point links. This command sets the Admin value of P2P Status; the default is force-true.
priority {00 10 ... F0}	Set the RSTP port priority on the single or multiple ports; the default is 80.
protocol-migration {false true}	Force the single or multiple port to transmit RSTP BPDUs when set to true, while operating in RSTP mode; the default is false.

Displaying RSTP bridge-level configuration details using ACLI

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

Procedure steps

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

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

Variable Definitions

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

Displaying RSTP port-level configuration details using ACLI

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

Procedure steps

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

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

Variable Definitions

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

Configuring RSTP SNMP traps using ACLI

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

The following events are generated:

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

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

Enable RSTP SNMP traps using ACLI

Use the following procedure to enable RSTP SNMP traps.

Procedure steps

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

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

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

Reset RSTP SNMP traps settings to default using ACLI

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

Procedure steps

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

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

Settings are returned to default values.

Verifying RSTP SNMP traps settings using ACLI

Use the following procedure to verify RSTP SNMP traps settings.

Procedure steps

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

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

Job aid: Verifying RSTP SNMP traps output

```
#show spanning-tree rstp config
Stp Priority (hex):      8000
Stp Version:           Rstp Mode
Bridge Max Age Time:   20 seconds
Bridge Hello Time:     2 seconds
Bridge Forward Delay Time: 15 seconds
```

```
Tx Hold Count:          3
Path Cost Default Type: 32-bit
STP Traps:              Enabled
```

Managing MSTP using ACLI

This section contains the following procedures:

Configuring MSTP parameters for CIST Bridge using ACLI

Use the following procedure to set the MSTP parameters, which include maximum hop count, maximum number of instances allowed, forward delay time, hello time, maximum age time, default path cost version, priority, transmit hold count, and version for the CIST Bridge.

Procedure steps

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

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

Variable Definitions

Variable	Value
max-hop <100 - 4000>	Set the MSTP maximum hop count for the CIST bridge; the default is 2000.
forward-time <4 - 30>	Set the MSTP forward delay for the CIST bridge in seconds; the default is 15.
max-age <6 - 40>	Set the MSTP maximum age time for the CIST bridge in seconds; the default is 20.
pathcost-type {bits16 bits32}	Set the MSTP default path cost version; the default is bits32.
priority {0000 1000 2000 ... F000}	Set the MSTP bridge priority for the CIST Bridge; the default is 8000.

Variable	Value
tx-holdcount<1 - 10>	Set the MSTP Transmit Hold Count; the default is 3.
version {stp-compatible rstp MSTP}	Set the MSTP version for the CIST Bridge; the default is MSTP.
add-vlan <1 - 4094>	Add a VLAN to the CIST bridge.
remove-vlan <1 - 4094>	Remove the specified VLAN from the CIST bridge.

Configuring MSTP parameters for Common Spanning Tree using ACLI

Use the following procedure to set the MSTP parameters, which include path cost, hello time, edge-port indicator, learning mode, point-to-point indicator, priority, and protocol migration indicator on the single or multiple ports for the Common Spanning Tree.

Procedure steps

To configure MSTP parameters, use the following command from Interface Configuration mode:

```
spanning-tree MSTP [port <portlist>] [cost <1 - 200000000>]
[edge-port {false | true}][hello-time <1 - 10>] [learning
{disable | enable}][p2p {auto | force-false | force-true}]
[priority {00 | 10 | < | F0}] [protocol-migration {false |
true}][instance-specific <1-7>]
```

Variable Definitions

Variable	Value
port <portlist>	Enter a list or range of port numbers.
cost <1 - 200000000>	Set the MSTP path cost on the single or multiple ports for the CIST; the default is 200000.
hello-time <1 - 10>	Set the MSTP hello time on the single or multiple ports for the CIST; the default is 2.
edge-port {false true}	Indicate whether the single or multiple ports are assumed to be edge ports. This parameter sets the Admin value of edge port status; the default is false.
learning {disable enable}	Enable or disable MSTP on the single or multiple ports; the default is enable.

Variable	Value
p2p {auto force-false force-true}	Indicate whether the single or multiple ports are treated as point-to-point links. This command sets the Admin value of P2P Status; the default is force-true.
priority {00 10 ... F0}	Set the MSTP port priority on the single or multiple ports; the default is 80.
protocol-migration {false true}	Force the single or multiple ports to transmit MSTP BPDUs when set to true, while operating in MSTP mode; the default is false.
instance-specific <1-7>	Set the MSTP instance-specific configuration in a range from 1–7 (filter on the MSTP instance).

Configuring MSTP region parameters using ACLI

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

Procedure steps

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

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

Variable Definitions

Variable	Value
[config-id-sel <0 - 255>]	Set the MSTP config ID selector; the default is 0.
[region-name <1 - 32 chars>]	Set the MSTP region name; the default is the bridge MAC address.
[region-version <0 - 65535>]	Set the MSTP region version; the default is 0.

Configuring MSTP parameters for bridge instance using ACLI

Use the following procedure to set the MSTP parameters, which include forward delay time, hello-time, maximum hop count, priority, and VLAN mapping for the bridge instance.

Procedure steps

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

```
spanning-tree MSTP MSTI <1 - 7> [priority{0000|1000|...|F000}]
[add-vlan <vid>] [remove-vlan <vid>] [enable]
```

Variable Definitions

Variable	Value
<1 - 7>	Filter on MSTP instance.
priority {0000 1000 ... F000}	Set the MSTP priority for the bridge instance; the default is 8000.
add-vlan <1 - 4094>	Map the specified Vlan and MSTP bridge instance.
remove-vlan <1 - 4094>	Unmap the specified Vlan and MSTP bridge instance.
enable	Enable the MSTP bridge instances.

Disabling a MSTP bridge instance using ACLI

Use the following procedure to disable a MSTP bridge instance.

Procedure steps

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

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

Deleting a MSTP bridge instance using ACLI

Use the following procedure to delete a MSTP bridge instance.

Procedure steps

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

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

Displaying MSTP status by selected bridge using ACLI

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

Procedure steps

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

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

Variable Definitions

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

Displaying MSTP CIST port information using ACLI

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

Procedure steps

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

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

Variable Definitions

Variable	Value
<portlist>	Enter a list or range of port numbers.
config	Display the MSTP CIST port information maintained by every port of the Common Spanning Tree.
role	Display MSTP CIST related port role information maintained by every port.
statistics	Display the MSTP CIST Port statistics maintained by every port.

Displaying MSTP MSTI settings using ACLI

Use the following procedure to display MSTP MSTI settings.

Procedure steps

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

```
show spanning-tree MSTP MSTI [config] [statistics] [port
{config | role | statistics}] <1 - 7>
```

Variable Definitions

Variable	Value
config	Display the MSTP instance-specific configuration and the VLAN mapping port.
statistics	Display MSTP instance-specific statistics.
port {config role statistics}	Display MSTP instance-specific port information:

Variable	Value
	<ul style="list-style-type: none">• config: Display MSTI port configuration• role: Display MSTI port role information• statistics: Display MSTI port statistics
<1 - 7>	Specify the MSTI instance for which to display the statistics.

Chapter 11: Configuring ADAC using ACLI

You can configure ADAC-related settings using ACLI.

Configuring ADAC globally using ACLI

Use the following procedure to configure ADAC for a switch.

Procedure steps

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

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

Variable Definitions

The following table defines optional parameters that can enter with the `adac [enable] [op-mode <untagged-frames-basic | untagged-frames-advanced| tagged-frames>] [traps enable] [voice-vlan <1-4094>] [uplink-port <portlist>] [call-server-port <portlist>]` command.

Variable	Value
enable	Enables ADAC on the switch.
op-mode <untagged-frames-basic untagged-frames-advanced tagged-frames >	Sets the ADAC operation mode to one of the following:

Variable	Value
	<ul style="list-style-type: none"> • 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.
<code>traps enable</code>	Enables ADAC trap notifications.
<code>voice-vlan <1-4094></code>	Sets the Voice VLAN ID. The assigned VLAN ID must not previously exist.
<code>uplink-port <portlist></code>	Configures a maximum of 8 ports as Uplink ports.
<code>call-server-port <portlist></code>	Configures a maximum of 8 ports as Call Server ports.

Disabling ADAC globally using ACLI

Use the following procedure to disable ADAC for a switch.

Procedure steps

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

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

Variable Definitions

The following table defines optional parameters that can enter with the `no adac [enable] [traps enable] [voice-vlan] [uplink-port] [call-server-port]` command.

Variable	Value
<code>enable</code>	Disables ADAC on the switch.

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

Restoring default ADAC settings using ACLI

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

Procedure steps

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

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

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

Variable Definitions

The following table defines optional parameters that you can enter with the **default adac [enable] [op-mode] [traps enable] [voice-vlan] [uplink-port] [call-server-port]** command.

Variable	Value
enable	Restores the default ADAC administrative state (disabled).
call-server-port	Restores the default Call Server port (none).
op-mode	Restores the default ADAC operation mode (Untagged Frames Basic).
traps enable	Restores the default state for ADAC notifications (enabled).
uplink-port	Restores the default Uplink port (none).

Variable	Value
voice-vlan	Restores the default Voice-VLAN ID (none).

Configuring per port ADAC settings using ACLI

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

Procedure steps

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

```
adac [port <portlist>] {[enable] [tagged-frames-pvid (<1-4094>|no-change)] [tagged-frames-tagging (tagAll|tagPvidOnly|untagPvidOnly|no-change)] }
```

Variable Definitions

The following table defines optional parameters that you can enter with the `adac [port <portlist>] {[enable] [tagged-frames-pvid (<1-4094>|no-change)] [tagged-frames-tagging (tagAll|tagPvidOnly|untagPvidOnly|no-change)] }` command.

Variable	Value
port <portlist>	Ports to which to apply the ADAC configuration.
enable	Enables ADAC on the port or ports listed.
tagged-frames-pvid <1-4094> no-change	Sets Tagged-Frames PVID on the port or ports listed. Use no-change to keep the current setting.
tagged-frames-tagging tagAll tagPvidOnly untagPvidOnly no-change	Sets Tagged-Frames Tagging to <ul style="list-style-type: none"> • tagAll • tagPvidOnly • untagPvidOnly Use no-change to keep the current setting.

Disable ADAC settings per port using ACLI

Use the following procedure to disable ADAC settings per port.

Procedure steps

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

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

Variable Definitions

The following table defines optional parameters that you can enter with the `no adac [port <portlist>] [enable]` command.

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

Configuring per port ADAC defaults for a specified port using ACLI

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

Procedure steps

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

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

Variable Definitions

The following table defines optional parameters that you can enter with the `default adac [port <portlist>] [enable] [tagged-frames-pvid] [tagged-frames-tagging]` command.

Variable	Value
port <portlist>	Ports on which to apply the ADAC defaults.
enable	Restores the port to the default ADAC state: Disabled.
tagged-frames-pvid	Restores Tagged-Frames PVID on the port or ports to the default setting: no-change.
tagged-frames-tagging	Restores Tagged-Frames Tagging to default setting: Untag PVID Only.

Configuring the autodetection method using ACLI

Use the following procedure to configure the autodetection method, by MAC address or using LLDP (IEEE 802.1ab).

Procedure steps

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

```
adac detection [port <port-list>] {[mac][lldp]}
```

Variable Definitions

Variable	Value
port <portlist>	Specifies the port or ports for which to set the detection mode.

Variable	Value
mac	Enables MAC-based detection. The default setting is MAC enabled.
lldp	Enables LLDP (802.1ab) detection. The default setting is LLDP enabled.

Disabling autodetection using ACLI

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

Procedure steps

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

```
no adac detection [port <port-list>] {[mac][lldp]}
```

Variable Definitions

Variable	Value
port <portlist>	Specifies the port or ports for which to disable the detection mode.
mac	Disables the MAC address detection mode.
lldp	Disables the LLDP detection mode.

Setting autodetection method to default using ACLI

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

Procedure steps

To return to default, use the following command from Interface Configuration mode:

```
default adac detection [port <port-list>] {[mac][lldp]}
```

Variable Definitions

Variable	Value
port <portlist>	Specifies the port or ports to be returned to the default; both MAC and LLDP are enabled.
mac	MAC is enabled by default.
lldp	LLDP is enabled by default.

Configuring autodetection for a specified port using ACLI

Use the following procedure to enable autodetection on specified ports.

Procedure steps

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

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

Disabling autodetection on specified ports using ACLI

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

Procedure steps

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

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

Restoring default ADAC setting for ports using ACLI

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

Procedure steps

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

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

Adding a range of MAC addresses for autodetection using ACLI

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

Procedure steps

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

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

Deleting a range of MAC addresses used by autodetection using ACLI

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

Procedure steps

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

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

Resetting supported MAC address ranges using ACLI

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

Procedure steps

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

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

Displaying global ADAC settings for a device using ACLI

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

Procedure steps

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

```
show adac
```

Displaying ADAC settings per port using ACLI

Use the following procedure to display ADAC settings per port.

Procedure steps

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

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

Displaying configured ADAC MAC ranges using ACLI

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

Procedure steps

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

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

Displaying detection mechanism configured per port using ACLI

Use the following procedure to display the detection mechanism configured per port.

Procedure steps

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

```
show adac detection interface [<interface-type>][<interface-id>]
```

ADAC UFA configuration example

[Figure 24: ADAC UFA configuration example](#) on page 139 shows an example of ADAC configured in Untagged-Frames-Advanced (UFA) op-mode. (Call-server-port is used in this example, because the server is directly connected to the 4500 series switch.)

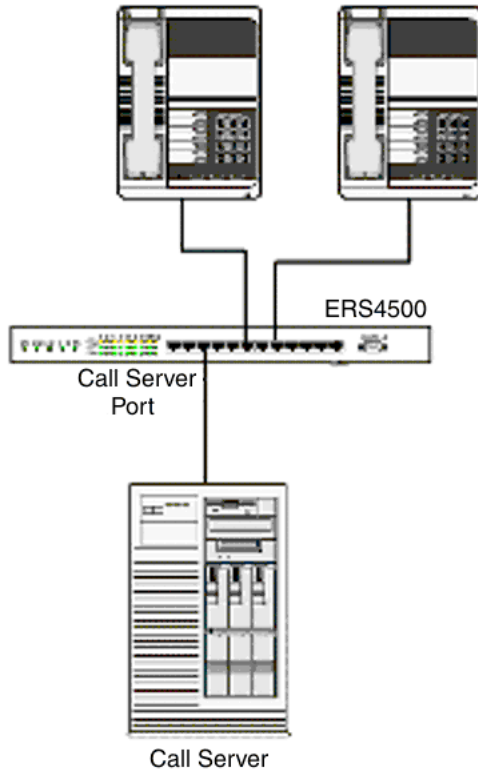


Figure 24: ADAC UFA configuration example

Auto-Configuration (AC) is applied for call-server-port and telephony ports. On telephony ports, AC is applied only when Avaya IP Phones are detected. (Autodetection is based on MAC Address.) VLAN configuration is made according to the selected op-mode (UFA):

- Telephony port:
 - Membership = remove from all other VLANs, and add to Voice-VLAN (since there is no reason for the port to be member of more than the Voice VLAN)
 - Tagging = Untagged
 - PVID = Voice-VLAN
- Call Server port:
 - Membership = add to Voice-VLAN
 - Tagging = Untagged
 - PVID = Voice-VLAN

To configure the example shown in [Figure 24: ADAC UFA configuration example](#) on page 139, you must perform the following tasks:

1. Configure the call-server port.
2. Configure voice-VLAN.
3. Configure Untagged-Frames-Advanced (UFA) op-mode.
4. Enable ADAC on all ports to which IP phones connect.
5. Configure IP phones to send untagged traffic.

ADAC ACLI configuration commands

The following section describes the detailed ACLI commands required to carry out the configuration shown in [Figure 24: ADAC UFA configuration example](#) on page 139.

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

Verifying new ADAC settings

The following section includes commands used to view ADAC configuration settings and the expected responses for each.

Auto configuration settings

```
(config)#show adac interface 7,16,24
```

Port	Auto-Detection	Auto-Configuration
7	Disabled	Applied
16	Enabled	Applied
24	Enabled	Applied

VLAN settings

```
(config)#show vlan
```

Id	Name	Type	Protocol	User	PID	Active	IVL/SVL	Mgmt	---
1	VLAN #1		Port	None	0x0000	Yes	IVL		Yes
Port Members: 1-15,17-23									
2	Voice_VLAN		Port	None	0x0000	Yes	IVL		No
Port Members: 7,16,24									

```
(config)#show vlan interface info 7,16,24
```

Filter	Filter	Port	Frames	Frames	PVID	PRI	Tagging	Name
Untagged	Unregistered							
7	No	Yes	2	0	UntagAll		Port 7	
16	No	Yes	2	0	UntagAll		Port 16	
24	No	Yes	2	0	UntagAll		Port 24	

ADAC settings

```
ERS4500#show running-config module adac
```

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

```
ERS4500#show running-config verbose module adac
```

```
! Embedded ASCII Configuration Generator Script
! Base model = Ethernet Routing Switch 4524GT
! Base Software version = v5.4.0.074
! Stack info:
!Unit# Switch Model      Pluggable Pluggable Pluggable Pluggable SW Version
!          Port          Port          Port          Port
!-----
!1      4524GT          (21) None (22) None (23) None (24) None v5.4.0.074
!2      4526GTX        (21) None (22) None (23) None (24) None v5.4.0.074
!          (25) None (26) None
!
! Displaying all switch parameters
!=====
enable
configure terminal
!
! *** ADAC ***
!
no adac enable
no adac mac-range-table
interface FastEthernet ALL
adac detection port 1/1-24,2/1-26 mac
adac detection port 1/1-24,2/1-26 lldp
exit
adac mac-range-table low-end 00-0A-E4-01-10-20 high-end 00-0A-E4-01-23-A7
adac mac-range-table low-end 00-0A-E4-01-70-EC high-end 00-0A-E4-01-84-73
adac mac-range-table low-end 00-0A-E4-01-A1-C8 high-end 00-0A-E4-01-AD-7F
```

Configuring ADAC using ACLI

```
adac mac-range-table low-end 00-0A-E4-01-DA-4E high-end 00-0A-E4-01-ED-D5
adac mac-range-table low-end 00-0A-E4-02-1E-D4 high-end 00-0A-E4-02-32-5B
adac mac-range-table low-end 00-0A-E4-02-5D-22 high-end 00-0A-E4-02-70-A9
adac mac-range-table low-end 00-0A-E4-02-D8-AE high-end 00-0A-E4-02-FF-BD
adac mac-range-table low-end 00-0A-E4-03-87-E4 high-end 00-0A-E4-03-89-0F
adac mac-range-table low-end 00-0A-E4-03-90-E0 high-end 00-0A-E4-03-B7-EF
adac mac-range-table low-end 00-0A-E4-04-1A-56 high-end 00-0A-E4-04-41-65
adac mac-range-table low-end 00-0A-E4-04-80-E8 high-end 00-0A-E4-04-A7-F7
adac mac-range-table low-end 00-0A-E4-04-D2-FC high-end 00-0A-E4-05-48-2B
adac mac-range-table low-end 00-0A-E4-05-B7-DF high-end 00-0A-E4-06-05-FE
adac mac-range-table low-end 00-0A-E4-06-55-EC high-end 00-0A-E4-07-19-3B
adac mac-range-table low-end 00-0A-E4-08-0A-02 high-end 00-0A-E4-08-7F-31
adac mac-range-table low-end 00-0A-E4-08-B2-89 high-end 00-0A-E4-09-75-D8
adac mac-range-table low-end 00-0A-E4-09-BB-9D high-end 00-0A-E4-09-CF-24
adac mac-range-table low-end 00-0A-E4-09-FC-2B high-end 00-0A-E4-0A-71-5A
adac mac-range-table low-end 00-0A-E4-0A-9D-DA high-end 00-0A-E4-0B-61-29
adac mac-range-table low-end 00-0A-E4-0B-BB-FC high-end 00-0A-E4-0B-BC-0F
adac mac-range-table low-end 00-0A-E4-0B-D9-BE high-end 00-0A-E4-0C-9D-0D
adac mac-range-table low-end 00-13-65-FE-F3-2C high-end 00-13-65-FF-ED-2B
adac mac-range-table low-end 00-15-9B-FE-A4-66 high-end 00-15-9B-FF-24-B5
adac mac-range-table low-end 00-16-CA-00-00-00 high-end 00-16-CA-01-FF-FF
adac mac-range-table low-end 00-16-CA-F2-74-20 high-end 00-16-CA-F4-BE-0F
adac mac-range-table low-end 00-17-65-F6-94-C0 high-end 00-17-65-F7-38-CF
adac mac-range-table low-end 00-17-65-FD-00-00 high-end 00-17-65-FF-FF-FF
adac mac-range-table low-end 00-18-B0-33-90-00 high-end 00-18-B0-35-DF-FF
adac mac-range-table low-end 00-19-69-83-25-40 high-end 00-19-69-85-5F-FF
adac voice-vlan 101
no adac call-server-port
adac uplink-port 2/25,2/26
adac op-mode tagged-frames
adac enable
```

Chapter 12: LACP and VLACP configuration using ACLI

Configuring LACP using ACLI

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

Displaying LACP settings using ACLI

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

Procedure steps

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

```
show lacp system
```

Displaying per port LACP configuration information using ACLI

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

Procedure steps

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

```
show lacp port [<portList> | aggr <1-65535>]
```

Variable Definitions

Variable	Value
<portList>	Enter the specific ports for which to display LACP information.
aggr <1-65535>	Enter the Aggregator value to display ports that are members of it.

Displaying LACP port statistics using ACLI

Use the following procedure to display LACP port statistics.

Procedure steps

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

```
show lacp stats [<portList> | aggr <1-65535>]
```

Variable Definitions

Variable	Value
<portList>	Enter the specific ports for which to display LACP information.
aggr <1-65535>	Enter the Aggregator value to display ports that are members of it.

Clearing LACP port statistics using ACLI

Use the following procedure to clear LACP port statistics.

Procedure steps

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


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

Displaying port debug information using ACLI

Use the following procedure to display port debug information.

Procedure steps

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

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

Displaying LACP aggregators or LACP trunks using ACLI

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

Procedure steps

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

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

Configuring LACP system priority using ACLI

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

Procedure steps

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

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

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

```
default lacp system-priority
```

Enabling port aggregation mode using ACLI

Use the following procedure to enable the port aggregation mode.

Procedure steps

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

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

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

```
default lacp aggregation
```

Disabling port aggregation mode using ACLI

Use the following procedure to disable the port aggregation mode.

Procedure steps

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

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

Configuring administrative LACP key using ACLI

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

Procedure steps

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

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

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

```
default lacp key
```

Variable Definitions

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

Configuring LACP mode of operation using ACLI

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

Procedure steps

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

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

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

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

Variable Definitions

Variable	Value
port <portList>	The ports for which the LACP mode is to be set.
{active passive off}	<p>The type of LACP mode to set for the port. The LACP modes are:</p> <ul style="list-style-type: none"> • active—The port will participate as an active Link Aggregation port. Ports in active mode send LACPDUs periodically to the other end to negotiate for link aggregation. • passive—The port will participate as a passive Link Aggregation port. Ports in passive mode send LACPDUs only when the configuration is changed or when its link partner communicates first. • off — The port does not participate in Link Aggregation. <p>LACP requires at least one end of each link to be in active mode.</p>

Configuring per port LACP priority using ACLI

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

Procedure steps

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

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

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

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

Variable Definitions

Variable	Value
port <portList>	The ports for which to configure LACP priority.
<0-65535>	The priority value to assign.

Configuring LACP periodic transmission timeout interval using ACLI

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

Procedure steps

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

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

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

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

Variable Definitions

Variable	Value
port <portList>	The ports for which to configure the timeout interval.
{long short}	Specify the long or short timeout interval.

Configuring VLACP using ACLI

To configure VLACP using ACLI, refer to the following procedures:



Important:

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

Enabling VLACP using ACLI

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

Procedure steps

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

```
vlacp enable
```

Configuring multicast MAC address for VLACP using ACLI

Use the following procedure to set the multicast MAC address used by the device for VLACPDU's.

Procedure steps

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

```
vlacp macaddress <macaddress>
```

Configuring VLACP parameters per port using ACLI

Use the following procedure to configure VLACP parameters per port.



Procedure steps

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

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

Variable Definitions

Variable	Value
<slot/port>	Specifies the slot and port number.
enable	Enables VLACP.
timeout <long/short>	<p>Specifies whether the timeout control value for the port is a long or short timeout.</p> <ul style="list-style-type: none"> • long— sets the port timeout value to: (timeout-scale value) × (slow-periodic-time value). • short— sets the port's timeout value to: (timeout-scale value) × (fast-periodic-time value). <p>For example, if the timeout is set to short while the timeout-scale value is 5 and the fast-periodic-time value is 500 ms, the timer expires after 2500 ms. Default is long.</p>
fast-periodic-time <integer>	<p>Specifies the number of milliseconds between periodic VLACPDU transmissions using short timeouts.</p> <p>The range is 400-20000 milliseconds. Default is 500.</p>

Variable	Value
<code>slow-periodic-time</code> <code><integer></code>	<p>Specifies the number of milliseconds between periodic VLACPDU transmissions using long timeouts.</p> <p>The range is 10000-30000 milliseconds. Default is 30000.</p>
<code>timeout-scale</code> <code><integer></code>	<p>Sets a timeout scale for the port, where $\text{timeout} = (\text{periodic time}) \times (\text{timeout-scale})$.</p> <p>The range is 1-10. Default is 3.</p> <p> Note:</p> <p>When you use fast-timers, you do not use a timeout-scale of 1, because this breaks the link continuity from service due to the time taken to transmit VLACPDU and for the partner to provide a corresponding response. Avaya recommends that you set the minimum timeout-scale to 3.</p> <p>Avaya also recommends that you use the minimum setting of 5 for the timeout-scale when using the fast-periodic-timer of 500 ms.</p>
<code>funcmac-addr</code> <code><mac></code>	<p>Specifies the address of the far-end switch/stack configured to be the partner of this switch/stack. If none is configured, any VLACP-enabled switch communicating with the local switch through VLACP PDUs is considered to be the partner switch.</p> <p> Note:</p> <p>VLACP has only one multicast MAC address, configured using the <code>vlacp macaddress</code> command, which is the Layer 2 destination address used for the VLACPDUs. The port-specific <code>funcmac-addr</code> parameter does not specify a multicast MAC address, but instead specifies the MAC address of the switch or stack to which this port is sending VLACPDUs. You are not always required to configure <code>funcmac-addr</code>. 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.</p> <p>If you want an intermediate switch to drop VLACP packets, configure the <code>funcmac-addr</code> parameter to the desired destination MAC address. With <code>funcmac-addr</code> configured, the intermediate switches do not misinterpret the VLACP packets.</p>

Variable	Value
ethertype <hex>	Sets the VLACP protocol identification for this port. Defines the ethertype value of the VLACP frame. The range is 8101-81FF. Default is 8103.

Disabling VLACP using ACLI

Use the following procedure to disable VLACP for a device.

Procedure steps

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

```
no vlacp enable
```

Resetting multicast MAC address for VLACP to default using ACLI

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

Procedure steps

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

```
no vlacp macaddress
```

Disabling VLACP on a port using ACLI

Use the following procedure to disable VLACP on a port.

Procedure steps

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


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

Variable Definitions

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

Displaying VLACP status using ACLI

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

Procedure steps

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

```
show vlacp
```

Displaying VLACP configuration details for ports using ACLI

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

Procedure steps

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

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

Among other properties, the **show vlacp interface** command displays a column called `HAVE PARTNER`, with possible values of `yes` or `no`.

If `HAVE PARTNER` is `yes` when `ADMIN ENABLED` and `OPER ENABLED` are `true`, then that port has received VLACPDUs from a port, and those PDUs were recognized as valid, according to the interface settings.

If `HAVE PARTNER` is `no` when `ADMIN ENABLED` and `OPER ENABLED` are `true`, then that port did not yet receive any VLACPDUs.

If `HAVE PARTNER` is `no` when `ADMIN ENABLED` is `true` and `OPER ENABLED` is `FALSE`, then the partner for that port is down (that port received at least one correct VLACPDU, but did not receive additional VLACPDUs within the configured timeout period). In this case VLACP blocks the port.

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

As long as the VLACP functional address for a specific interface is not changed when using the `(config-if)# vlacp port x funcmac-addr H.H.H` command, the MAC address is displayed as `00:00:00:00:00:00`. The MAC address used for sending VLACP PDUs for an interface is the global VLACP MAC address (`01:80:c2:00:11:00`). The VLACP global destination MAC can be 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`.

Chapter 13: Configuring VLANs using Enterprise Device Manager

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

VLAN management using EDM

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

Viewing VLAN information using EDM

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



Procedure steps

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

Variable definitions

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

Variable	Value
Id	Indicates the VLAN ID for the VLAN.
Name	Indicates the name of the VLAN.
IfIndex	Indicates the interface index.
Type	Indicates the VLAN type as defined by the policy used to define the VLAN port membership. Values include: <ul style="list-style-type: none">• byPort—VLAN by Port• byIpSubnet—VLAN by IP subnet• byProtocolId—VLAN by Protocol ID• bySrcMac—VLAN by source MAC address• byDstMcast—VLAN by destination MultiCast

Variable	Value
	<ul style="list-style-type: none"> • bySvlan—VLAN by stacked VLAN • byIds—VLAN by VLAN IDs • byPortIp—VLAN by port type IP • byPortEvpn—VLAN by EVPN port type • byPortDefault—VLAN by default port type
PortMembers	Indicates the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met.
StgId	<p>Indicates the STG to which the selected VLAN belongs.</p> <p> Important: This column is available only when the switch is operating in the STG mode. Avaya Ethernet Routing Switch 4500 Series does not support multiple STGs when operating in the STG mode.</p>
MstpInstance	<p>Indicates the MSTP instance associated with the VLAN. Values include:</p> <ul style="list-style-type: none"> • none • cist • msti-1-7 <p> Important: This column is available only when the switch is operating in the MSTP mode.</p>
ProtocolId	<p>Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is <i>byProtocolId</i>. Values include:</p> <ul style="list-style-type: none"> • ip • ipx802dot3 • ipx802dot2 • ipxSnap • ipxEthernet2 • decLat • sna802dot2 • snaEthernet2 • netBios • xns • vines

Variable	Value
	<ul style="list-style-type: none"> • ipv6 • usrDefined • rarp
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN.
Encap	Indicates the encapsulation type for user defined protocol based VLANs only. Values include: <ul style="list-style-type: none"> • ethernet2 • llc • snap By default there is no value in this cell.
MacAddress	Indicates the MAC address associated with the VLAN.
Routing	Indicates whether routing is enabled (true) or disabled (false) for the VLAN.

Modifying an existing VLAN in STG mode using EDM

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

Prerequisites

Select avayaStpg for the Spanning Tree administration mode.

Procedure steps

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

OR


Deselect ports to remove them from the VLAN.

9. Click **Ok**.

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

Variable definitions

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

Variable	Value
Id	Indicates the ID for the VLAN. This is a read-only value.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
IfIndex	Indicates the interface index. This is a read-only value.
Type	Indicates the type of VLAN: byPort. This is a read-only value. Values include: <ul style="list-style-type: none"> • byPort—VLAN by Port • byProtocolId—VLAN by Protocol ID
PortMembers	Specifies the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.
StgId	Specifies the STG to associate with the selected VLAN or VLANs. This is a read-only value. <p> Important: This column is available only when the Spanning Tree administration operating mode is avayaSTG mode, when the operating mode is MSTP or RSTP, this column is not available.</p>
ProtocolId	Specifies the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is <i>byProtocolId</i> . Values include: <ul style="list-style-type: none"> • ip • ipx802dot3 • ipx802dot2 • ipxSnap • ipxEthernet2 • decLat • sna802dot2

Variable	Value
	<ul style="list-style-type: none"> • snaEthernet2 • netBios • xns • vines • ipv6 • usrDefined • rarp
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN. This is a read-only value.
Encap	Indicates the encapsulation type for user defined protocol based VLANs only. This is a read-only value. Values include: <ul style="list-style-type: none"> • ethernet2 • llc • snap • all • notapplicable By default there is no value in this cell.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Specifies whether routing is enabled (true) or disabled (false) for the VLAN.

Modifying an existing VLAN in RSTP mode using EDM

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

Prerequisites

Select RSTP for the Spanning Tree administration mode.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
 2. Double-click **VLANs**.
 3. In the work area, click the **Basic** tab.
 4. To select a VLAN to edit, click the VLAN ID.
 5. In the VLAN row, double-click the cell in the **Name** column.
 6. Type a character string to assign a unique name to the VLAN.
 7. In the VLAN row, double-click the cell in the **PortMembers** column.
 8. Select ports to add to the VLAN.
- OR**
- Deselect ports to remove them from the VLAN.
9. Click **Ok** .
 10. In the VLAN row, double-click the cell in the **Routing** column.
 11. Select a value from the list—**true** to enable routing for the VLAN, or **false** to disable routing for the VLAN .
 12. Click **Apply** .

Variable definitions

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

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

Variable	Value
	<ul style="list-style-type: none"> • byPort—VLAN by Port • byProtocolId—VLAN by Protocol ID
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	<p>Specifies the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is <i>byProtocolId</i>. Values include:</p> <ul style="list-style-type: none"> • ip • ipx802dot3 • ipx802dot2 • ipxSnap • ipxEthernet2 • decLat • sna802dot2 • snaEthernet2 • netBios • xns • vines • ipv6 • usrDefined • rarp
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN. This is a read-only value.
Encap	<p>Indicates the encapsulation type for user defined protocol based VLANs only. This is a read-only value. Values include:</p> <ul style="list-style-type: none"> • ethernet2 • llc • snap • all • notapplicable <p>By default there is no value in this cell.</p>
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.

Variable	Value
Routing	Specifies whether routing is enabled (true) or disabled (false) for the VLAN.

Modifying an existing VLAN in MSTP mode using EDM

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

Prerequisites


Select MSTP for the Spanning Tree administration mode.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
 2. Double-click **VLANs**.
 3. In the work area, click the **Basic** tab.
 4. To select a VLAN to edit, click the VLAN ID.
 5. In the VLAN row, double-click the cell in the **Name** column.
 6. Type a character string to assign a unique name to the VLAN.
 7. In the VLAN row, double-click the cell in the **PortMembers** column.
 8. Select ports to add to the VLAN.
- OR**
- Deselect ports to remove them from the VLAN.
9. Click **Ok** .
 10. In the VLAN row, double-click the cell in the **MstpInstance** column, if the switch is in MSTP mode.
 11. Select a value from the list.
 12. In the VLAN row, double-click the cell in the **Routing** column.
 13. Select a value from the list—**true** to enable routing for the VLAN, or **false** to disable routing for the VLAN .
 14. Click **Apply** .

Variable definitions

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

Variable	Value
Id	Indicates the ID for the VLAN. This is a read-only value.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
IfIndex	Indicates the interface index. This is a read-only value.
Type	Indicates the type of VLAN: byPort. This is a read-only value. Values include: <ul style="list-style-type: none"> • byPort—VLAN by Port • byProtocolId—VLAN by Protocol ID
PortMembers	Specifies the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.
MstpInstance	The MSTP instance associated with the VLAN. Values include: <ul style="list-style-type: none"> • none • cist • msti-1-7 <p> Important: This column is available only when the Spanning Tree administration operating mode is MSTP, when the operating mode is avayaSTG or RSTP, this column is not available .</p>
ProtocolId	Specifies the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is <i>byProtocolId</i> . Values include: <ul style="list-style-type: none"> • ip • ipx802dot3 • ipx802dot2 • ipxSnap • ipxEthernet2 • decLat • sna802dot2 • snaEthernet2 • netBios • xns • vines • ipv6

Variable	Value
	<ul style="list-style-type: none"> • usrDefined • rarp
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN. This is a read-only value.
Encap	<p>Indicates the encapsulation type for user defined protocol based VLANs only. This is a read-only value. Values include:</p> <ul style="list-style-type: none"> • ethernet2 • llc • snap • all • notapplicable <p>By default there is no value in this cell.</p>
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Specifies whether routing is enabled (true) or disabled (false) for the VLAN.

Creating a VLAN in STP mode using EDM

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

Prerequisites

Select avayaStpg for the Spanning Tree administration mode.

Procedure steps

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

OR

Accept the default ID for the VLAN.

6. In the Name dialog box, type a value.

OR

Accept the default name for the VLAN.

7. In the **Type** section, click a radio button.
8. Click **Insert**.
9. In the VLAN row, double-click the cell in the **PortMembers** column.
10. Select ports to add to the VLAN.

OR


Deselect ports to remove them from the VLAN.

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

Variable definitions

Use the data in this table to modify the create VLAN in STG mode.

Variable	Value
Id	Specifies the ID for the VLAN.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
Type	Indicates the type of VLAN. This is a read-only value. Values include: <ul style="list-style-type: none"> • byPort—VLAN by Port • byProtocolId—VLAN by Protocol ID
PortMembers	Specifies the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.
StgId	Specifies the STG to associate with the selected VLAN or VLANs. This is a read-only value.

Variable	Value
	<p> Important: This column is available only when the Spanning Tree administration operating mode is avayaSTG mode, when the operating mode is MSTP or RSTP, this column is not available.</p>
ProtocolId	<p>Specifies the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is <i>byProtocolId</i>. Values include:</p> <ul style="list-style-type: none"> • ip • ipx802dot3 • ipx802dot2 • ipxSnap • ipxEthernet2 • decLat • sna802dot2 • snaEthernet2 • netBios • xns • vines • ipv6 • usrDefined • rarp
UserDefinedPid	<p>Indicates the user defined protocol identifier for a protocol based VLAN. This is a read-only value.</p>
Encap	<p>Indicates the encapsulation type for user defined protocol based VLANs only. This is a read-only value. Values include:</p> <ul style="list-style-type: none"> • ethernet2 • llc • snap • all • notapplicable <p>By default there is no value in this cell.</p>
MacAddress	<p>Indicates the MAC address associated with the VLAN. This is a read-only value.</p>
Routing	<p>Specifies whether routing is enabled (true) or disabled (false) for the VLAN.</p>

Creating a VLAN in RSTP mode using EDM

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

Prerequisites

Select RSTP for the Spanning Tree administration mode.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. Click **Insert**.
5. In the Id dialog box, type a value.
OR
Accept the default ID for the VLAN.
6. In the Name dialog box, type a value.
OR
Accept the default name for the VLAN.
7. Click **Insert**.
8. In the VLAN row, double-click the cell in the **PortMembers** column.
9. Select ports to add to the VLAN.
OR
Deselect ports to remove them from the VLAN.
10. Click **Ok** .
11. In the VLAN row, double-click the cell in the **Routing** column.
12. Select a value from the list—**true** to enable routing for the VLAN, or **false** to disable routing for the VLAN .
13. Click **Apply** .

Variable definitions

Use the data in this table to modify the create a VLAN in RSTP mode.

Variable	Value
Id	Specifies the ID for the VLAN.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
Type	Indicates the type of VLAN. This is a read-only value. Values include: <ul style="list-style-type: none"> • byPort—VLAN by Port • byProtocolId—VLAN by Protocol ID
PortMembers	Specifies the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.
ProtocolId	Specifies the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is <i>byProtocolId</i> . Values include: <ul style="list-style-type: none"> • ip • ipx802dot3 • ipx802dot2 • ipxSnap • ipxEthernet2 • decLat • sna802dot2 • snaEthernet2 • netBios • xns • vines • ipv6 • usrDefined • rarp
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN. This is a read-only value.
Encap	Indicates the encapsulation type for user defined protocol based VLANs only. This is a read-only value. Values include:

Variable	Value
	<ul style="list-style-type: none"> • ethernet2 • llc • snap • all • notapplicable <p>By default there is no value in this cell.</p>
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Specifies whether routing is enabled (true) or disabled (false) for the VLAN.

Creating a VLAN in MSTP mode using EDM

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

Prerequisites

Select MSTP for the Spanning Tree administration mode.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. Click **Insert**.
5. In the Id dialog box, type a value.
OR
Accept the default ID for the VLAN.
6. In the Name dialog box, type a value.
OR
Accept the default name for the VLAN.
7. Click the **MstpInstance** box arrow.

8. Select a value from the list.
9. Click **Insert**.
10. In the VLAN row, double-click the cell in the **PortMembers** column.
11. Select ports to add to the VLAN.

OR


Deselect ports to remove them from the VLAN.

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

Variable definitions

Use the data in this table to modify the create a VLAN in MSTP mode.

Variable	Value
Id	Specifies the ID for the VLAN.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
IfIndex	Indicates the interface index. This is a read-only value.
Color	Specifies the color code for the VLAN. The VLAN Manager graphical user interface tool uses the value of this object to select a color when it draws this VLAN on the screen. Values range from 0 to 31.
Type	Indicates the type of VLAN. This is a read-only value. Values include: <ul style="list-style-type: none"> • byPort—VLAN by Port • byProtocolId—VLAN by Protocol ID
PortMembers	Specifies the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.
MstpInstance	The MSTP instance associated with the VLAN. Values include: <ul style="list-style-type: none"> • none • cist • msti-1-7

Variable	Value
	 Important: This column is available only when the Spanning Tree administration operating mode is MSTP, when the operating mode is avayaSTG or RSTP, this column is not available.
ProtocolId	Specifies the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is <i>byProtocolId</i> . Values include: <ul style="list-style-type: none"> • ip • ipx802dot3 • ipx802dot2 • ipxSnap • ipxEthernet2 • decLat • sna802dot2 • snaEthernet2 • netBios • xns • vines • ipv6 • usrDefined • rarp
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN. This is a read-only value.
Encap	Indicates the encapsulation type for user defined protocol based VLANs only. This is a read-only value. Values include: <ul style="list-style-type: none"> • ethernet2 • llc • snap • all • notapplicable By default there is no value in this cell.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Specifies whether routing is enabled (true) or disabled (false) for the VLAN.

Deleting a VLAN using EDM

Use this procedure to delete a VLAN.

Procedure steps

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

VLAN IPv4 address management using EDM

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

VLAN IPv4 address management using EDM navigation

- [Viewing VLAN IPv4 address information using EDM](#) on page 172
- [Assigning an IPv4 address to a using EDM](#) on page 173
- [Deleting an IPv4 address from a VLAN using EDM](#) on page 174

Viewing VLAN IPv4 address information using EDM

Use this procedure to display IPv4 addresses associated with VLANs.

Procedure steps

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

3. In the work area, click the **Basic** tab.
4. To select a VLAN to edit, click the VLAN ID.
5. On the toolbar, click **IP**.
6. In the work area, click the **IP Address** tab.

Variable definitions

Use the data in this table to help you understand the IPv4 address display.

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

Assigning an IPv4 address to a using EDM

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

Procedure steps

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

11. Click **Insert** .
12. Click **Apply** .

Variable definitions

Use the data in this table to assign an IPv4 address to a VLAN.

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

Deleting an IPv4 address from a VLAN using EDM

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

Procedure steps

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

Configuring DHCP for a VLAN using EDM

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

Procedure steps

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

OR

Clear the **Enable** check box to disable DHCP for the VLAN.

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

OR

Clear the **AlwaysBroadcast** check box to disable the broadcast of DHCP reply packets for the VLAN.

11. Select the **Option82Enabled** check box to enable DHCP option 82 for the VLAN.

OR

Clear the **Option82Enabled** check box to disable DHCP option 82 for the VLAN.

12. In the **ClearCounters** section, click a radio button.
13. Click **Apply** .

Variable definitions

Use the data in this table to configure DHCP for a VLAN.

Variable	Value
Enable	Enables or disables DHCP for the VLAN.
MinSec	Specifies the minimum period of time (in seconds) before a DHCP packet received on this VLAN, is forwarded to the destination device. Values range from 0 to 65535 seconds.
Mode	Specifies the type of DHCP packets this VLAN supports. Values include: <ul style="list-style-type: none"> • none—all received DHCP and BOOTP packets are dropped • bootp—only BOOTP packets are supported • dhcp—only DHCP packets are supported • both—DHCP and BOOTP packets are supported
AlwaysBroadcast	When selected, broadcasts DHCP reply packets from the VLAN to the DHCP client.
Option82Enabled	When selected, enables DHCP option 82 for the VLAN.
ClearCounters	Clears the DHCP counters. <ul style="list-style-type: none"> • clear—resets the DHCP counters to 0 and sets the counter clear time to the current system up time value. • dummy—the read-only default value.
CounterClearTime	Indicates the time the DHCP counters for this VLAN were last reset to 0.

Configuring RIP for a VLAN using EDM

Use this procedure to configure Routing Information Protocol (RIP) for a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN to edit, click the VLAN ID.
5. On the toolbar, click **IP**.
6. In the work area, click the **RIP** tab.
7. In the **Poison** section, click a radio button.
8. Select the **DefaultSupply** check box to enable ABC for the VLAN.
OR
Clear the **DefaultSupply** check box to disable ABC for the VLAN .
9. Select the **DefaultListen** check box to enable ABC for the VLAN.
OR
Clear the **DefaultListen** check box to disable ABC for the VLAN .
10. Select the **AutoAggregateEnable** check box to enable ABC for the VLAN.
OR
Clear the **AutoAggregateEnable** check box to disable ABC for the VLAN .
11. Select the **AdvertiseWhenDown** check box to enable ABC for the VLAN.
OR
Clear the **AdvertiseWhenDown** check box to disable ABC for the VLAN .
12. In the Cost dialog box, type a value.
13. Click **Apply** .

Variable definitions

Use the data in this table to configure RIP for a VLAN.

Variable	Value
Poison	Enables or disables the operation of poison reverse on this VLAN. The default is disabled.

Variable	Value
DefaultSupply	Enables or disables the advertising of default routes on this VLAN.
DefaultListen	Enables or disables listening for default rout advertisements on this VLAN.
AutoAggregateEnable	Enables or disables automatic aggregation on this VLAN.
AdvertiseWhenDown	Enables or disables the sending of advertisements from this VLAN when the VLAN is down.
Cost	Specifies the RIP cost for this VLAN. Values range from 1 to 15.

Graphing OSPF statistics for a VLAN using EDM

Use this procedure to display a graphical representation of OSPF statistics for a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN, click the VLAN ID.
5. On the toolbar, click **IP**.
6. In the work area, click the **OSPF Stats** tab.
7. Select a **Poll Interval** from the list on the toolbar.
8. To select statistics to graph, click a statistic type row under one of the displayed columns.
9. Click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

VLAN IPv6 interface management using EDM

Use the information in this section to configure and manage IPv6 interfaces for a VLAN.

VLAN IPv6 interface management using EDM navigation

- [Viewing IPv6 interface information for a VLAN using EDM](#) on page 179
- [Adding an IPv6 interface to a VLAN using EDM](#) on page 180
- [Deleting an IPv6 interface from a VLAN using EDM](#) on page 182

Viewing IPv6 interface information for a VLAN using EDM

Use this procedure to display existing IPv6 interface information for a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN, click the VLAN ID.
5. On the toolbar, click **IPv6**.
6. In the work area, click the **IPv6 Interface** tab.

Variable definitions

Use the data in this table to help you understand the VLAN IPv6 interface display.

Variable	Value
IfIndex	Identifies a physical interface or a logical interface (VLAN). For a VLAN, it is the Ifindex of the VLAN.
Identifier	Indicates the IPv6 address interface identifier, which is a binary string of up to 8 octets in network byte order.
IdentifierLength	Indicates the length of the interface identifier in bits.
Descr	Indicates a text string containing information about the interface. The network management system also sets this string.

Variable	Value
VlanId	Identifies the Virtual LAN associated with the entry. This value corresponds to the lower 12 bits in the IEEE 802.1Q VLAN tag.
Type	Indicates Unicast, the only supported type.
ReasmMaxSize(MTU)	Indicates the MTU for this IPv6 interface. This value must be same for all the IP addresses defined on this interface. The default value is 1280.
PhysAddress	Indicates the media-dependent physical address. The range is 0 through 65535. For Ethernet, this is a MAC address.
AdminStatus	Indicates whether the administration status of the interface is enabled (true) or disabled (false). The default is enabled (true).
OperStatus	Indicates whether the operation status of the interface is up or down.
ReachableTime	Indicates the time (3600000 ms) that a neighbor is considered reachable after receiving a reachability confirmation.
RetransmitTime	Indicates the retransmit time, which is the time (3600000 ms) between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.
MulticastAdminStatus	Indicates the multicast status as either True or False.

Adding an IPv6 interface to a VLAN using EDM

Use this procedure to add an IPv6 interface to a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN, click the VLAN ID.
5. On the toolbar, click **IPv6**.

6. In the work area, click the **IPv6 Interface** tab.
7. On the toolbar, click **Insert** .
8. In the Identifier dialog box, type a value.
9. In the Descr dialog box, type a value.
10. In the ReasmMaxSize(MTU) dialog box, type a value.
11. Select the **AdminStatus** check box to enable the interface administration status for the VLAN.

OR

Clear the **AdminStatus** check box to disable the interface administration status for the VLAN .

12. In the ReachableTime dialog box, type a value.
13. In theRetransmitTime dialog box, type a value.
14. Click **Insert** .
15. Click **Apply** .

Variable definitions

Use the data in this table to help you understand the VLAN IPv6 interface display.

Variable	Value
Identifier	Specifies the IPv6 address interface identifier, which is a binary string of up to 8 octets in network byte order.
Descr	Specifies a text string containing information about the interface. The network management system also sets this string.
ReasmMaxSize(MTU)	Specifies the MTU for this IPv6 interface. This value must be same for all the IP addresses defined on this interface. The default value is 1280.
AdminStatus	Specifies whether the administration status of the interface is enabled (true) or disabled (false). The default is enabled (true).
ReachableTime	Specifies the time (3600000 ms) that a neighbor is considered reachable after receiving a reachability confirmation.
RetransmitTime	Specifies the retransmit time, which is the time (3600000 ms) between retransmissions of neighbor solicitation messages to a

Variable	Value
	neighbor when resolving the address or when probing the reachability of a neighbor.

Deleting an IPv6 interface from a VLAN using EDM

Use this procedure to remove an IPv6 interface from a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN, click the VLAN ID.
5. On the toolbar, click **IPv6**.
6. In the work area, click the **IPv6 Interface** tab.
7. To select an interface to delete, click the IfIndex.
8. On the toolbar, click **Delete** .

VLAN IPv6 address management using EDM

Use the information in this section to configure and manage IPv6 addresses for a VLAN.

VLAN IPv6 address management using EDM navigation

- [Viewing IPv6 address information for a VLAN using EDM](#) on page 182
- [Adding an IPv6 address to a VLAN using EDM](#) on page 184
- [Deleting an IPv6 address from a VLAN using EDM](#) on page 185

Viewing IPv6 address information for a VLAN using EDM

Use this procedure to display existing IPv6 address information for a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN, click the VLAN ID.
5. On the toolbar, click **IPv6**.
6. In the work area, click the **IPv6 Addresses** tab.

Variable definitions

Use the data in this table to help you understand the VLAN IPv6 address display.

Variable	Value
IfIndex	Indicates of the VLAN.
Addr	Indicates the VLAN IPv6 address.
AddrLen	Indicates the VLAN IPv6 prefix length.
Type	Indicates the VLAN IPv6 address type. Values include: <ul style="list-style-type: none"> • unicast • anycast
Origin	Indicates the origin of the VLAN IPv6 address. Values include: <ul style="list-style-type: none"> • other • manual • dhcp • linklayer • random
Status	Indicates the status of the VLAN IPv6 address. Values include: <ul style="list-style-type: none"> • preferred • deprecated • invalid • inaccessible • unknown

Variable	Value
	<ul style="list-style-type: none"> • tentative • duplicate
Created	Indicates the value of the system up time when this address was created. A value of 0 indicates that this address was created before the last network management subsystem initialization.
LastChanged	Indicates the value of the system up time when this address was last updated. A value of 0 indicates that this address was updated before the last network management subsystem initialization.

Adding an IPv6 address to a VLAN using EDM

Use this procedure to add an IPv6 address to a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN, click the VLAN ID.
5. On the toolbar, click **IPv6**.
6. In the work area, click the **IPv6 Addresses** tab.
7. In the **Addr** box, type an IPv6 address.
8. In the **AddrLen** box, type the IPv6 prefix length.
9. In the **Type** section, click a radio button.
10. Click **Insert**.
11. Click **Apply** .

Variable definitions

Use the data in this table to add an IPv6 address to a VLAN.

Variable	Value
Addr	Specifies the VLAN IPv6 address.
AddrLen	Specifies the VLAN IPv6 prefix length.

Variable	Value
Type	Specifies the VLAN IPv6 address type. Values include: <ul style="list-style-type: none"> • unicast • anycast

Deleting an IPv6 address from a VLAN using EDM

Use this procedure to remove an IPv6 address from a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN, click the VLAN ID.
5. On the toolbar, click **IPv6**.
6. In the work area, click the **IPv6 Addresses** tab.
7. To select an address to delete, click the **Index**.
8. On the toolbar, click **Delete**.

VLAN configuration for ports using EDM

Use the information in this section to view and configure VLAN membership for specific ports.

VLAN configuration for ports using EDM navigation

- [Viewing VLAN membership port information using EDM](#) on page 186
- [Configuring VLAN membership ports using EDM](#) on page 187

Viewing VLAN membership port information using EDM

Use this procedure to display the VLAN membership information for switch ports.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **VLANs**.
3. Click the **Ports** tab.

Variable definitions

Use the data in the following table to help you understand the VLAN port membership display.

Variable	Value
Index	Indicates the switch position in the stack and the port number. This is a read-only value.
VlanIds	Indicates the VLAN IDs of which this port is a member. This is a read-only value.
DiscardUntaggedFrames	<p>Indicates how untagged frames received on this port are processed.</p> <ul style="list-style-type: none"> • true—untagged frames are discarded by the forwarding process • false—untagged frames are assigned to the VLAN specified by the VLAN ID. <p>This column applies to trunk ports only.</p>
FilteredUnregisteredFrame	<p>Indicates how unregistered frames received on this port are processed.</p> <ul style="list-style-type: none"> • true—unregistered frames are discarded by the forwarding process • false—unregistered frames are assigned to the VLAN specified by the VLAN ID. <p>This column applies to access ports only.</p>
DefaultVlanId	Indicates the VLAN ID assigned to untagged and unregistered frames received on a port.
PortPriority	Indicates the port priority for the switch to consider as it forwards received packets. Values range from 0 to 7.

Variable	Value
Tagging	Indicates the type of VLAN port. Values include: <ul style="list-style-type: none"> • untagAll (access) • tagAll (trunk) • untagPvidOnly • tagPvidOnly If the port is a trunk port, the port is often a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN.

Configuring VLAN membership ports using EDM

Use this procedure to configure VLAN membership for one or more switch ports.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **VLANs**.
3. Click the **Ports** tab.
4. To select a port to edit, click the port row.
5. In the port row, double-click the cell in the **DiscardUntaggedFrames** column.
6. Select a value from the list—**true** to discard untagged frames for the port, or **false** to accept untagged frames for the port.
7. In the port row, double-click the cell in the **FilteredUnregisteredFrame** column.
8. Select a value from the list—**true** to discard unregistered frames for the port, or **false** to process unregistered frames normally for the port.
9. In the port row, double-click the cell in the **DefaultVlanId** column.
10. Type a value for the default VLAN ID.
11. In the port row, double-click the cell in the **PortPriority** column.
12. Select a value from the list.
13. In the port row, double-click the cell in the **Tagging** column.
14. Select a value from the list.

15. You can repeat steps **5** through **14** to configure VLAN memberships for additional ports.
16. Click **Apply** .

Variable definitions

Use the data in the following table to configure VLAN membership for one or more switch ports.

Variable	Value
Index	Indicates the switch position in the stack and the port number. This is a read-only value.
VlanIds	Indicates the VLAN IDs of which this port is a member. This is a read-only value.
DiscardUntaggedFrames	<p>Specifies how untagged frames received on this port are processed.</p> <ul style="list-style-type: none"> • true—untagged frames are discarded by the forwarding process • false—untagged frames are assigned to the VLAN specified by the VLAN ID. <p>This column applies to trunk ports only.</p>
FilteredUnregisteredFrame	<p>Specifies how unregistered frames received on this port are processed.</p> <ul style="list-style-type: none"> • true—unregistered frames are discarded by the forwarding process • false—unregistered frames are assigned to the VLAN specified by the VLAN ID. <p>This column applies to access ports only.</p>
DefaultVlanId	Specifies the VLAN ID assigned to untagged and unregistered frames received on a port.
PortPriority	Specifies the port priority for the switch to consider as it forwards received packets. Values range from 0 to 7.
Tagging	<p>Specifies the type of VLAN port. Possible values are:</p> <ul style="list-style-type: none"> • untagAll (access) • tagAll (trunk) • untagPvidOnly • tagPvidOnly

Variable	Value
	If the port is a trunk port, the port is often a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN.

Selecting VLAN configuration control using EDM

Use the following procedure to select configuration control for a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **VLANs**.
3. In the work area, click the **Settings** tab.
4. In the ManagementVlanID dialog box, type a value.
5. In the **VlanConfigControl** section, click a radio button.
6. On the toolbar, click **Apply**.

Variable Definitions

Use the data in this table to select VLAN configuration control.

Variable	Value
ManagementVlanId	Specifies the identifier of the management VLAN. Values range from 1 to 4094.
VlanConfigControl	Specifies the VLAN configuration control options. The available options are: <ul style="list-style-type: none"> • automatic—This selection automatically adds an untagged port to a new VLAN and automatically removes it from any previous VLAN membership. The PVID of the port is automatically changed to the VID of the VLAN it joins. Since the port is first added to the new VLAN and then removed from any previous membership, the Spanning Tree Group participation of the port is not disabled as long as the VLANs involved are in the same Spanning Tree Group. • autopvid—This selection functions in the same manner as previous AutoPVID functionality. When an untagged port is added to a new VLAN, the port is added to the new VLAN and

Variable	Value
	<p>the PVID assigned to the new VID without removing it from any previous VLAN memberships. Using this option, an untagged port can have membership in multiple VLANs.</p> <ul style="list-style-type: none"> • flexible—This selection functions in a similar manner to disabling AutoPVID functionality. When this option is used, an untagged port can belong to an unlimited number of VLANs. Any new additions of an untagged port to a new VLAN does not change the PVID of that port. • strict—The factory default, this selection restricts the addition of an untagged port to a VLAN if it is already a member of another VLAN. To add an untagged port to a new VLAN, the switch administrator must remove the port from all other VLANs of which it is a member before adding it to the new VLAN. The PVID of the port is changed to the new VID to which it was added.

Enabling AutoPVID using EDM

Use this procedure to automatically assign a port VLAN ID to any port by enabling the AutoPVID functionality on the switch.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Chassis**.
4. In the work area, click the **System** tab.
5. In the AutoPVID section, click the enabled radio button.
6. Click **Apply**.

Port configuration for VLANs using EDM

Use the information in this section to view and configure specific ports for VLAN membership.

Port configuration for VLANs using EDM navigation

- [Viewing port VLAN membership information using EDM](#) on page 191
- [Configuring ports for VLAN membership using EDM](#) on page 192

Viewing port VLAN membership information using EDM

Use this procedure to display the VLAN membership information for switch ports.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis** .
3. In the Chassis tree, double-click **Ports** .
4. Click the **VLAN** tab.

Variable definitions

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

Variable	Value
Index	Indicates the switch position in the stack and the port number. This is a read-only value.
VlanIds	Indicates the VLAN IDs of which this port is a member. This is a read-only value.
DiscardUntaggedFrames	Indicates how untagged frames received on this port are processed. <ul style="list-style-type: none"> • true—untagged frames are discarded by the forwarding process • false—untagged frames are assigned to the VLAN specified by the VLAN ID. This column applies to trunk ports only.
FilteredUnregisteredFrame	Indicates how unregistered frames received on this port are processed.

Variable	Value
	<ul style="list-style-type: none"> • true—unregistered frames are discarded by the forwarding process • false—unregistered frames are assigned to the VLAN specified by the VLAN ID. <p>This column applies to access ports only.</p>
DefaultVlanId	Indicates the VLAN ID assigned to untagged and unregistered frames received on a port.
PortPriority	Indicates the port priority for the switch to consider as it forwards received packets. Values range from 0 to 7.
Tagging	<p>Indicates the type of VLAN port. Possible values are:</p> <ul style="list-style-type: none"> • untagAll (access) • tagAll (trunk) • untagPvidOnly • tagPvidOnly <p>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.</p>

Configuring ports for VLAN membership using EDM

Use this procedure to configure one or more switch ports for VLAN membership.

Procedure steps

1. From the navigation tree, double-click **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 **FilteredUnregisteredFrame** 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. You can repeat steps **5** through **15** to configure VLAN memberships for additional ports.
17. Click **Apply** .

Variable definitions

Use the data in the following table to configure ports for VLAN membership.

Variable	Value
Index	Indicates the switch position in the stack and the port number. This is a read-only value.
VlanIds	Indicates the VLAN IDs of which this port is a member. This is a read-only value.
DiscardUntaggedFrames	<p>Specifies how untagged frames received on this port are processed.</p> <ul style="list-style-type: none"> • true—untagged frames are discarded by the forwarding process • false—untagged frames are assigned to the VLAN specified by the VLAN ID. <p>This column applies to trunk ports only.</p>
FilteredUnregisteredFrame	<p>Specifies how unregistered frames received on this port are processed.</p> <ul style="list-style-type: none"> • true—unregistered frames are discarded by the forwarding process • false—unregistered frames are assigned to the VLAN specified by the VLAN ID. <p>This column applies to access ports only.</p>
DefaultVlanId	Specifies the VLAN ID assigned to untagged and unregistered frames received on a port.
PortPriority	Specifies the port priority for the switch to consider as it forwards received packets. Values range from 0 to 7.
Tagging	Specifies the type of VLAN port. Possible values are:

Variable	Value
	<ul style="list-style-type: none"> • untagAll (access) • tagAll (trunk) • untagPvidOnly • tagPvidOnly <p>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.</p>

MAC address table management using EDM

Use the information in this section to manage the MAC address table by clearing entries.



Important:

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

MAC address table management using EDM navigation



Important:

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

- [Flushing the MAC address table using EDM](#) on page 194
- [Flushing FastEthernet interface-based MAC addresses from the MAC address table using EDM](#) on page 195
- [Flushing VLAN-based MAC addresses from the MAC address table using EDM](#) on page 195
- [Flushing trunk-based MAC addresses from the MAC address table using EDM](#) on page 196
- [Flushing a specific MAC address from the MAC address table using EDM](#) on page 196

Flushing the MAC address table using EDM

Use the following procedure to clear all MAC addresses from the MAC address table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. In the work area, click the **MAC Flush** tab.
4. Select the **FlushMacAddrTableAll** check box.
5. On the toolbar, click **Apply**.

Flushing FastEthernet interface-based MAC addresses from the MAC address table using EDM

Use the following procedure to clear FastEthernet interface-based MAC addresses from the MAC address table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. On the work area, click the **MAC Flush** tab.
4. Click the **FlushMacAddrTableByPortList** elipsis (...).
5. Select one or more specific ports.

OR

Click **ALL** to select all the ports.

6. Click **Ok**.
7. On the toolbar, click **Apply**.

Flushing VLAN-based MAC addresses from the MAC address table using EDM

Use the following procedure to clear VLAN-based MAC addresses from the MAC address table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. On the work area, click the **MAC Flush** tab.
4. In the FlushMacAddrTableByVlan dialog box, type a VLAN ID ranging from 1 to 4094.
5. On the toolbar, click **Apply**.

Flushing trunk-based MAC addresses from the MAC address table using EDM

Use the following procedure to clear trunk-based MAC addresses from the MAC address table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. On the work area, click the **MAC Flush** tab.
4. In the FlushMacAddrTableByTrunk dialog box, type a trunk value ranging from 1 to 6.
5. On the toolbar, click **Apply**.

Flushing a specific MAC address from the MAC address table using EDM

Use the following procedure to remove a single specific MAC address from the MAC address table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.

3. On the work area, click the **MAC Flush** tab.
4. In the FlushMacAddrTableByAddress dialog box, type a MAC address.
5. On the toolbar, click **Apply**.

Chapter 14: Configuring MultiLink Trunking using Enterprise Device Manager

This chapter provides information you can use to create and manage Multi Link Trunks using Enterprise Device Manager (EDM).

MLT configuration using EDM

Use the information in this section to create a MultiLink Trunk (MLT) and to modify existing MLT port memberships.

MLT configuration using EDM navigation

- [Viewing MLT configurations using EDM](#) on page 199
- [Creating an MLT using EDM](#) on page 200
- [Modifying MLT port memberships using EDM](#) on page 202


Viewing MLT configurations using EDM

Use this procedure to display MLT configuration information.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **Multi Link Trunks** tab.

Variable Definitions

Variable	Value
Id	Indicates the number of the MLT (assigned consecutively). Displays the vlan based on port selected.
PortType	Indicates the port type. Values include: <ul style="list-style-type: none"> • access • trunk
Name	Indicates a unique alphanumeric identifier for the MLT.
PortMembers	Indicates the switch or stack ports to assign to the MLT.
VlanIds	Indicates the VLAN identifier. Displays the vlan based on port selected.
Loadbalance (Mode)	Indicates the mode of load balancing. Options are basic and advanced.
Enable	Indicates whether the MLT is enabled (true) or disabled (false) .  Important: You cannot enable an MLT if trunk port members are enabled for LACP.

Creating an MLT using EDM

Create an MLT to form a link from the switch to another switch or server.

Procedure steps


1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **Multi Link Trunks** tab.
4. To select a trunk to create, click the trunk **Id**.
5. In the trunk row, double-click the cell in the **Name** column.
6. In the box, type a name for the MLT.

OR

Accept the default MLT name.

7. In the trunk row, double-click the cell in the **PortMembers** column.
8. From the list , select ports to add to the trunk.
9. Click **Ok**.
10. In the trunk row, double-click the cell in the **Loadbalance(Mode)** column.
11. From the list, select a load balancing mode.
12. In the trunk row, double-click the cell in the **Enable** column.
13. From the list, select a value—**true** to enable the MLT, or **false** to disable the MLT.
14. You can repeat steps **4** through **13** to create additional MLTs.
15. Click **Apply**.

Variable Definitions

Variable	Value
Id	Specifies the number of the MLT (assigned consecutively). Displays the vlan based on port selected.
PortType	Specifies the port type. Values include: <ul style="list-style-type: none"> • access • trunk
Name	Specifies a unique alphanumeric identifier for the MLT.
PortMembers	Specifies the switch or stack ports to assign to the MLT.
VlanIds	Specifies the VLAN identifier. Displays the vlan based on port selected.
Loadbalance (Mode)	Specifies the mode of load balancing. Options are basic and advanced.
Enable	Enables (true) or disables (false) the MLT. <p> Important: You cannot enable an MLT if trunk port members are enabled for LACP.</p>

Modifying MLT port memberships using EDM


Modify MLT port memberships to change configuration parameters for an existing MLT.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **Multi Link Trunks** tab.
4. To select a trunk to modify, click the trunk **Id** of an existing trunk.
5. In the trunk row, double-click the cell in the **Enable** column.
6. From the list box, select **false** to disable the MLT.
7. Click **Apply**.
8. In the trunk row, double-click the cell in the **Name** column.
9. In the box, edit the MLT name as required.
10. In the trunk row, double-click the cell in the **PortMembers** column.
11. From the list box, select ports to add to or remove from the trunk.
12. Click **Ok**.
13. In the trunk row, double-click the cell in the **Loadbalance(Mode)** column.
14. From the list box, select a load balancing mode.
15. You can repeat steps **4** through **14** to modify additional MLTs.
16. Click **Apply**.

Variable Definitions

Variable	Value
Id	Specifies the number of the MLT (assigned consecutively). Displays the vlan based on port selected.
PortType	Indicates the port type. Values include: <ul style="list-style-type: none"> • access • trunk

Variable	Value
Name	Specifies a unique alphanumeric identifier for the MLT.
PortMembers	Specifies the switch or stack ports to assign to the MLT.
VlanIds	Specifies the VLAN identifier. Displays the vlan based on port selected.
Loadbalance (Mode)	Specifies the mode of load balancing. Options are basic and advanced.
Enable	Enables (true) or disables (false) the MLT.  Important: You cannot enable an MLT if trunk port members are enabled for LACP.

Viewing MLT utilization using EDM

Use this procedure to display MLT utilization information.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, click **MLT/LACP**.
3. In the work area, click the **MLT Utilization** tab.

Variable definition

Variable	Value
Id	Displays the MLT ID.
PortIfIndex	Displays the port number.
TrafficType	Displays the traffic type.
TrafficLast5Min	Displays MLT utilization for the last 5 minutes.
TrafficLast30Min	Displays MLT utilization for the last 30 minutes.
TrafficLast1Hour	Displays MLT utilization for the last hour.

Graphing MLT statistics using EDM

Use the following procedure to display and graph MLT interface statistics.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **Multi Link Trunks** tab.
4. Select an MLT row.
5. Click **Graph**.
6. Click the **Interface** tab.
7. Click the **Poll Interval** box.
8. From the list, select a poll interval time.
9. Click **Clear Counters**.
10. To select statistics to graph, click a row under one of the available column headings.
11. Click a **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.
12. To return to the MultiLink Trunks-Graph, Interface work area, click **Close**.

Variable definitions

Use the data in this table to help you understand MLT statistics.

Variable	Value
Poll Interval	Specifies the time interval in seconds, minutes, or hours that the switch polls the interface for MLT statistics. Located on menu bar.
InMulticastPkts	Indicates the number of packets delivered to this MLT that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.
OutMulticastPkts	Indicates the total number of packets that higher-level protocols requested be transmitted, and that were addressed to a

Variable	Value
	multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
InBroadcastPkts	Indicates the number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
OutBroadcastPkts	Indicates the total number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.
HCInOctets	Indicates the total number of octets received on the MLT interface, including framing characters.
HCOctets	Indicates the total number of octets transmitted out of the MLT interface, including framing characters.
HCInUcastPkts	Indicates the number of packets delivered by this MLT to a higher MLT that were not addressed to a multicast or broadcast address at this sublayer.
HCOctetsUcastPkts	Indicates the number of packets that high-level protocols requested be transmitted that were not addressed to a multicast address at this MLT. This total number includes those packets discarded or unsent.
HCInMulticastPkt	Indicates the number of packets delivered to this MLT that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.
HCOctetsMulticast	Indicates the total number of packets that high-level protocols requested be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
HCInBroadcastPkt	Indicates the number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
HCOctetsBroadcast	Indicates the total number of packets that high-level protocols requested be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.

Graphing MLT Ethernet error statistics using EDM

Use the following procedure to view and graph MLT Ethernet error statistics.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **MultiLink Trunks** tab.
4. Select an MLT row.
5. Click **Graph**.
6. Click the **Ethernet Errors** tab.
7. Click the **Poll Interval** box.
8. From the list, select a poll interval time.
9. Click **Clear Counters**.
10. To select error statistics to graph, click a row under one of the available column headings.
11. Click a **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.
12. To return to the MultiLink Trunks-Graph, Ethernet Errors work area, click **Close**.

Variable definitions

Use the data in this table to help you understand MLT Ethernet error statistics.

Variable	Value
Poll Interval	Specifies the time interval in seconds, minutes, or hours that the switch polls the interface for MLT Ethernet error statistics. Located on menu bar.
AlignmentErrors	Indicates a count of frames received on a particular MLT that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
FCSErrors	Indicates a count of frames received on an MLT that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3

Variable	Value
	Layer Management, counted exclusively according to the error status presented to the LLC.
IMacTransmit Error	Indicates a count of frames for which transmission on a particular MLT fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object.
IMacReceive Error	Indicates a count of frames for which reception on a particular MLT fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object. The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted.
CarrierSense Error	Indicates the number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular MLT. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
FrameTooLong	Indicates a count of frames received on a particular MLT that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
SQETestError	Indicates a count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular MLT. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
Deferred Transmiss	Indicates a count of frames for which the first transmission attempt on a particular MLT is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollFrames	Indicates a count of successfully transmitted frames on a particular MLT for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object.

Variable	Value
MultipleColl Frames	Indicates a count of successfully transmitted frames on a particular MLT for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	Indicates the number of times that a collision is detected on a particular MLT later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
ExcessiveCollis	Indicates a count of frames for which transmission on a particular MLT fails due to excessive collisions.

Selecting an SLPP Guard Ethernet type using EDM

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

 **Important:**

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

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **SLPP**.
3. In the work area, click the **Global** tab.
4. Type a value in the **SlppGuardEtherType** box.
5. On the toolbar, click **Apply**.

Configuring SLPP Guard using EDM

Use this procedure to configure SLPP Guard for switch ports.

 **Note:**

SLPP packets are generated only on switches that are configured with SLPP - for example ERS 5000 Series or ERS 8300. The ERS 4500 switches do not support SLPP. When you

enable SLPP Guard on an ERS 4500, the switch must be connected to another Avaya switch that supports SLPP and SLPP must be enabled on that switch.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **SLPP**.
3. In the work area, click the **SLPP Guard** tab.
4. To select a specific switch port, click an **IfIndex**.
5. In the IfIndex row, double-click the cell in the **Enabled** column.
6. Select a value from the list—**true** to enable SLPP Guard, **false** to disable SLPP Guard.
7. In the IfIndex row, double-click the cell in the **Timeout** column.
8. Type a value in the **Timeout** box.
9. On the toolbar, click **Apply**.

Variable definition

Variable	Value
IfIndex	Specifies the port on which to configure SLPP Guard.
Enable	Enables (true) or disables (false) SLPP Guard for the port.
Timeout	Specifies the time period, in seconds, for which SLPP Guard disables the port. After the timeout period expires, the switch re-enables the port. The timeout value can be 0 or a value ranging from 10 to 65535. With a value of 0, the port remains disabled until it is manually re-enabled. The default Timeout value is 60 seconds.
Status	Displays the SLPP Guard status for the port.
TimerCount	Indicates the time, in seconds, that elapses after SLPP Guard disables a port. When the TimerCount value equals the Timeout value, the switch re-enables the port.

Viewing the SLPP Guard configuration using EDM

Use this procedure to display SLPP Guard configuration information for switch ports.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **SLPP**.
3. In the work area, click the **SLPP Guard** tab.

Variable definition

Variable	Value
IfIndex	Indicates the port for which the SLPP Guard information is displayed.
Enable	Enables (true) or disables (false) SLPP Guard for the port.
Timeout	Specifies the time period, in seconds, for which SLPP Guard disables the port. After the timeout period expires, the switch re-enables the port. The timeout value can be 0 or a value ranging from 10 to 65535. With a value of 0, the port remains disabled until it is manually re-enabled. The default Timeout value is 60 seconds.
Status	Displays the SLPP Guard status for the port.
TimerCount	Indicates the time, in seconds, that elapses after SLPP Guard disables a port. When the TimerCount value equals the Timeout value, the switch re-enables the port.

Chapter 15: Configuring Spanning Tree Protocol using Enterprise Device Manager

This chapter describes how you can configure the Spanning Tree Protocol (STP) and Spanning Tree Groups (STGs) using Enterprise Device Manager (EDM).

Navigation

- [Configuring the STP mode using EDM](#) on page 211
- [Configuring STP BPDU filtering for specific ports using EDM](#) on page 212
- [Configuring STG globally using EDM](#) on page 213
- [STG configuration using EDM](#) on page 215
- [Moving a VLAN between STGs using EDM](#) on page 221
- [Viewing STG Status using EDM](#) on page 221
- [STG port membership management using EDM](#) on page 222
- [Port STG membership configuration using EDM](#) on page 225

Configuring the STP mode using EDM

Use the following procedure to configure the STP operational mode.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **Globals**.
4. Choose the STP mode in the **SpanningTreeAdminMode** field.

5. On the toolbar, click **Apply**.

A warning message appears reminding you that you must reset the switch for the change to take effect.

6. Click **Yes**.
7. Click **Close**.

For information about resetting the switch, see [Resetting the switch using EDM](#) on page 212.

Resetting the switch using EDM

Use the following procedure to reset the switch.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Chassis**.
4. On the work area, click the **System** tab.
5. In the ReBoot section, click the **reboot** radio button.
6. Click **Apply**.

Configuring STP BPDU filtering for specific ports using EDM

Use this procedure to configure STP BPDU filtering for one or more ports.

You can configure STP BPDU filtering in either STG, RSTP, or MSTP operational mode.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. On the work area, click the **STP BPDU-Filtering** tab.

5. To select a port to edit, click the port index.
6. In the port row, double-click the cell in the **AdminEnabled** column.
7. Select a value from the list—**true** to enable STP BPDU filtering for the port, or **false** to disable STP BPDU filtering for the port.
8. In the port row, double-click the cell in the **Timeout** column.
9. Type a value in the dialog box.
10. You can repeat steps **5** through **9** to configure STP BPDU filtering for additional ports.
11. On the toolbar, click **Apply**.

Variable Definitions

Variable	Value
rcPortIndex	Indicates the switch and port number.
AdminEnabled	Enables and disables BPDU filtering on the port.
OperEnabled	Indicates the current operational status of BPDU filtering on the port: true (enabled) or false (disabled).
Timeout	When BPDU filtering is enabled, this indicates the time (in 1/100 seconds) during which the port remains disabled after it receives a BPDU. The port timer is disabled if this value is set to 0. The default value is 12000 (120 seconds).
TimerCount	Displays the time remaining for the port to stay in the disabled state after receiving a BPDU.

Configuring STG globally using EDM

Use the following procedure to configure the STG for the switch.

Prerequisites

Select `avayaStpg` for the Spanning Tree administration mode.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. In the work area, click the **Globals** tab.
5. In the **SpanningTreePathCostCalculationMode** section, click a radio button.
6. In the **SpanningTreePortMode** section, select a radio button.
7. In the **SpanningTreeAdminCompatibility** section, select the **port802dot1dLearning** check box to enable 8021d compliancy support.

OR

In the **SpanningTreeAdminCompatibility** section, clear the **port802dot1dLearning** check box to disable 8021d compliancy support.

8. Click **Apply**.

Variable Definitions

Variable	Value
<code>SpanningTreePathCostCalculationMode</code>	<p>Specifies the spanning-tree path cost calculation mode. Values include:</p> <ul style="list-style-type: none"> • <code>ieee802dot1dCompatible</code> • <code>ieee802dot1tCompatible</code> <p>You can select <code>ieee802dot1dCompatible</code> only when the global STP mode <code>avayaStpg</code> is selected.</p>
<code>SpanningTreePortMode</code>	<p>Specifies the STG port membership mode for all Spanning Tree Groups on the switch. Values are:</p> <ul style="list-style-type: none"> • <code>normal</code> • <code>auto</code>
<code>SpanningTreeAdminCompatibility</code>	<p>Specifies the administrative feature compatibility mode.</p> <p><code>port802dot1dLearning</code>—enables or disables STP 802.1D compliancy support for the switch</p>

Variable	Value
SpanningTreeOperCompatibility	Indicates the operational feature compatibility mode. For some features, this read-only display will not change until the system is reset.

Configuring STP BPDU filtering ignore self using EDM

Use this procedure to configure whether or not local bridge BPDUs are ignored during the STP BPDU filtering process.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. In the work area, click the **Globals** tab.
5. Select the **SpanningTreeBpduFilterIgnoreSelf** check box to enable STP BPDU filtering ignore self.

OR

Clear the **SpanningTreeBpduFilterIgnoreSelf** check box to disable STP BPDU filtering ignore self.

6. Click **Apply**.

STG configuration using EDM

Use the information in this section to create and manage STGs on your network.

STG configuration using EDM navigation

- [STG configuration prerequisites](#) on page 216
- [Viewing an STG using EDM](#) on page 216
- [Modifying an STG using EDM](#) on page 217
- [Creating an STG using EDM](#) on page 219
- [Deleting an STG using EDM](#) on page 220

STG configuration prerequisites

Select `avayaStpg` for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see [Configuring the STP mode using EDM](#) on page 211.

Viewing an STG using EDM

Use the following procedure to display STG configuration information.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. On the work area, click the **Configuration** tab.

Variable Definitions

Use the data in the following table to help you understand the STG display.

Variable	Value
Id	Indicates the identifier for the STG. Values range from 1 to 8. The default STG ID is 1.
BridgeAddress	Indicates the MAC address used by a bridge when the bridge must be referred to in a unique fashion. The bridge MAC address can be integrated with the priority value to form a unique bridge identifier that is used in the Spanning Tree Protocol.
NumPorts	Indicates the number of ports controlled by this bridging entity.
Protocol Specification	Indicates the version of the spanning tree protocol being run. Values include: <ul style="list-style-type: none"> • <code>decLb100</code>: Indicates the DEC LANbridge 100 Spanning Tree Protocol. • <code>ieee8021d</code>: IEEE 802.1d implementations will return this entry. When future versions of the IEEE

Variable	Value
	Spanning Tree Protocol are released that are incompatible with the current version, a new value will be defined.
Priority	Indicates the first two octets of the 8-octet bridge ID. Values range from 0 to 65535.
BridgeMaxAge	Indicates the maximum time you want to allow before the specified STG times out, in seconds; the range, measured in hundredths of a second, is 600 (6 seconds) to 4000 (40 seconds).
BridgeHelloTime	Indicates the maximum time between hellos, in seconds; the range, measured in hundredths of a second, is 100 (1 second) to 1000 (10 seconds).
BridgeForwardDelay	Indicates the maximum delay in forwarding, in seconds; the range, measured in hundredths of a second) is 400 (4 seconds) to 3000 (30 seconds).
EnableStp	Indicates whether STP is enabled (true) or disabled (false) for the STG.
TaggedBpduAddress	Indicates the destination MAC address assigned to tagged BPDUs.
TaggedBpduVlanId	Indicates the VLAN ID for tagged BPDUs. This value must be unique for each specific STG.

Modifying an STG using EDM

Use the following procedure to edit an existing STG configuration.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. On the work area, click the **Configuration** tab.
5. To select an STG to edit, click the STG ID.
6. In the STG row, double-click the cell in the **Priority** column.
7. Type a value in the dialog box.
8. In the STG row, double-click the cell in the **BridgeMaxAge** column.

9. Type a value in the dialog box.
10. In the STG row, double-click the cell in the **BridgeHelloTime** column.
11. Type a value in the dialog box.
12. In the STG row, double-click the cell in the **EnableStp** column.
13. Select a value from the list—**true** to enable STP for the STG, or **false** to disable STP for the STG.
14. In the STG row, double-click the cell in the **TaggedBpduAddress** column.
15. Type a value in the dialog box.
16. In the STG row, double-click the cell in the **TaggedBpduVlanId** column.
17. Type a value in the dialog box.
18. You can repeat steps **6** through **17** to create additional STGs.
19. Click **Apply**.

Variable Definitions

Use the data in the following table to edit an existing STG.

Variable	Value
Id	Indicates the identifier for the STG. Values range from 1 to 8. The default STG ID is 1. This is a read-only cell.
BridgeAddress	Indicates the MAC address used by a bridge when the bridge must be referred to in a unique fashion. The bridge MAC address can be integrated with the priority value to form a unique bridge identifier that is used in the Spanning Tree Protocol. This is a read-only cell.
NumPorts	Indicates the number of ports controlled by this bridging entity. This is a read-only cell.
Protocol Specification	Version of the spanning tree protocol being run. Values include: <ul style="list-style-type: none"> • decLb100: Indicates the DEC LANbridge 100 Spanning Tree Protocol. • ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version, a new value will be defined. This is a read-only cell.

Variable	Value
Priority	Specifies the first two octets of the 8-octet bridge ID. Values range from 0 to 65535.
BridgeMaxAge	Specifies the maximum time you want to allow before the specified STG times out, in seconds; the range, measured in hundredths of a second, is 600 (6 seconds) to 4000 (40 seconds).
BridgeHelloTime	Specifies the maximum time between hellos, in seconds; the range, measured in hundredths of a second, is 100 (1 second) to 1000 (10 seconds).
BridgeForwardDelay	Specifies the maximum delay in forwarding, in seconds; the range, measured in hundredths of a second) is 400 (4 seconds) to 3000 (30 seconds).
EnableStp	Enables (true) or disables (false) STP for the STG.
TaggedBpduAddress	Specifies the destination MAC address assigned to tagged BPDUs.
TaggedBpduVlanId	Specifies the VLAN ID for tagged BPDUs. This value must be unique for each specific STG.

Creating an STG using EDM

Use the following procedure to create an STG.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. On the work area, click the **Configuration** tab.
5. On the toolbar, click **Insert**.
6. Edit the default information in the dialog boxes to create an STG.
7. Click **Insert**.
8. You can repeat steps **5** through **7** to create additional STGs.
9. Click **Apply**.

Variable Definitions

Use the data in the following table to create an STG.

Variable	Value
Id	Identifies the STG. Value range is 1–8; 1 is the default STG.
Priority	Specifies the first two octets of the 8-octet bridge ID; the range is 0–65535.
BridgeMaxAge	Specifies the maximum time you want to allow before the specified STG times out, in seconds; the range, measured in hundredths of a second, is 600 (6 seconds) to 4000 (40 seconds).
BridgeHelloTime	Specifies the maximum time between hellos, in seconds; the range, measured in hundredths of a second, is 100 (1 second) to 1000 (10 seconds).
BridgeForwardDelay	Specifies the maximum delay in forwarding, in seconds; the range, measured in hundredths of a second) is 400 (4 seconds) to 3000 (30 seconds).
TaggedBpduVlanId	Specifies the VLAN ID for tagged BPDUs.

Deleting an STG using EDM

Use this procedure to delete an STG.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. On the work area, click the **Configuration** tab.
5. To select an STG to edit, click the STG ID.
6. Click **Delete**.

Moving a VLAN between STGs using EDM

You cannot use EDM to move VLANs between STGs on the Avaya Ethernet Routing Switch 4500 Series. Instead, delete the VLAN to be moved and add a replacement VLAN in the STG to which you want to move the VLAN.

Viewing STG Status using EDM

Use this procedure to display the status of an configured STGs.

Prerequisites

Select `avayaStpg` for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see [Configuring the STP mode using EDM](#) on page 211.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. On the work area, click the **Status** tab.

Variable Definitions

Use the data in the following table to help you understand the STG status display.

Variable	Value
Id	Indicates the STG ID.
BridgeAddress	Indicates the MAC address used by this bridge.
NumPorts	Indicates the number of ports controlled by this bridging entity.

Variable	Value
ProtocolSpecification	Indicates the version of spanning tree that is running.
TimeSinceTopology Change	Indicates the time, in hundredths of seconds, since the last topology change.
TopChanges	Indicates the number of topology changes since the switch was reset.
DesignatedRoot	Indicates the MAC address of the STP designated root.
RootCost	Indicates the cost of the path to the root.
RootPort	Indicates the port number of the port with the lowest-cost path from this bridge to the root bridge.
MaxAge	Indicates the maximum age, in hundredths of a second, of STP information learned from any port in the network before the information is discarded.
HelloTime	Indicates the amount of time, in hundredths of seconds, between Hello messages.
HoldTime	Indicates the interval, in hundredths of seconds, during which no more than two Hello messages can be transmitted.
ForwardDelay	Indicates the interval, in hundredths of seconds, during which the switch stays in Listening or Learning mode, before moving to Forwarding mode. This value is also used to age dynamic entries in the Forwarding Database.

STG port membership management using EDM

Use the information in this section to view and modify STG membership configurations for switch ports.

STG port membership management using EDM navigation

- [STG port membership management prerequisites](#) on page 223
- [Viewing STG port information using EDM](#) on page 223
- [Configuring STG for port using EDM](#) on page 224

STG port membership management prerequisites

Select `avayaStpg` for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see [Configuring the STP mode using EDM](#) on page 211.

Viewing STG port information using EDM

Use this procedure to display STG port membership status.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. On the work area, click the **Ports** tab.

Variable Definitions

Variable	Value
Port	Indicates the unit and port number.
StgId	Indicates the STG ID number.
Priority	Indicates the port priority
State	Indicates the STP state of the port—Disabled, Blocking, Listening, Learning, and Forwarding.
EnableStp	Indicates whether STP is enabled (true) or disabled (false) on the port.
FastStart	Indicates whether Fast Start STP is enabled (true) or disabled (false) on the port.
AdminPathCost	Indicates the PathCost value. The field displays 0 if no user-configured value exists.
PathCost	Indicates the contribution of this port to the cost path of the spanning tree root.

Variable	Value
DesignatedRoot	Indicates the MAC address of the STP designated root.
DesignatedCost	Indicates the path cost of the designated port of the segment connected to this port.
DesignatedBridge	Indicates the MAC address of the designated bridge this port considers the designated bridge for this segment.
DesignatedPort	Indicates the port ID of the designated bridge for this port segment.

Configuring STG for port using EDM

Use this procedure to configure STG membership for switch ports.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **STG**.
4. On the work area, click the **Ports** tab.
5. To select an STG port to edit, click the port row.
6. In the port row, double-click the cell in the **Priority** column.
7. Type a value in the dialog box.
8. In the port row, double-click the cell in the **EnableStp** column.
9. Select a value from the list—**true** to enable STP for the port, or **false** to disable STP for the port.
10. In the port row, double-click the cell in the **FastStart** column.
11. Select a value from the list—**true** to enable fast start for the port, or **false** to disable fast start for the port.
12. In the port row, double-click the cell in the **AdminPathCost** column.
13. Type a value in the dialog box.
14. In the port row, double-click the cell in the **PathCost** column.
15. Type a value in the dialog box.

16. You can repeat steps **5** through **15** to configure STG for additional ports.
17. Click **Apply**.

Variable Definitions

Use the data in the following table to edit STG port configurations.

Variable	Value
Port	Specifies the unit and port number.
StgId	Specifies the STG ID number.
Priority	Specifies the port priority
State	Specifies the STP state of the port—Disabled, Blocking, Listening, Learning, and Forwarding.
EnableStp	Enables or disables STP on the port: True is enabled, and False is disabled.
FastStart	Enables or disables Fast Start STP on the port: True is enabled, and False is disabled.
AdminPathCost	Sets the PathCost value. The field displays 0 if no user-configured value exists.
PathCost	Specifies the contribution of this port to the cost path of the spanning tree root.
DesignatedRoot	Specifies the MAC address of the STP designated root.
DesignatedCost	Specifies the path cost of the designated port of the segment connected to this port.
DesignatedBridge	Specifies the MAC address of the designated bridge this port considers the designated bridge for this segment.
DesignatedPort	Specifies the port ID of the designated bridge for this port segment.
ForwardTransitions	Specifies the number of times the port transitioned from STP Learning to Forwarding state.

Port STG membership configuration using EDM

Use the information in this section to view and modify switch port STG memberships.

Prerequisites

Ensure that STP is enabled before enabling FastStart.

Viewing STG port membership information using EDM

Use this procedure to display information about switch port STG memberships.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. In the work area, click the **STG** tab.

Variable Definitions

Use the data in the following table to help you understand the switch port STG display.

Variable	Value
Port	Indicates the unit and port number.
StgId	Indicates the STG ID number.
Priority	Indicates the port priority
State	Indicates the STP state of the port—Disabled, Blocking, Listening, Learning, and Forwarding.
EnableStp	Indicates whether STP is enabled (true) or disabled (false) on the port.
FastStart	Indicates whether fast start STP is enabled (true) or disabled (false) on the port.
AdminPathCost	Indicates the PathCost value. The field displays 0 if no user-configured value exists.
PathCost	Indicates the contribution of this port to the cost path of the spanning tree root.
DesignatedRoot	Indicates the MAC address of the STP designated root.

Variable	Value
DesignatedCost	Indicates the path cost of the designated port of the segment connected to this port.
DesignatedBridge	Indicates the MAC address of the designated bridge this port considers the designated bridge for this segment.
DesignatedPort	Indicates the port ID of the designated bridge for this port segment.
ForwardTransitions	Indicates the number of times the port transitioned from STP Learning to Forwarding state.

Configuring STG port membership using EDM

Use this procedure to configure switch ports as STG members.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. In the work area, click the **STG** tab.
5. To select an port to edit, click the port row.
6. In the port row, double-click the cell in the **Priority** column.
7. Type a value in the dialog box.
8. In the port row, double-click the cell in the **EnableStp** column.
9. Select a value from the list—**true** to enable STP for the port, or **false** to disable STP for the port.
10. In the port row, double-click the cell in the **FastStart** column.
11. Select a value from the list—**true** to enable fast start for the port, or **false** to disable fast start for the port.
12. In the port row, double-click the cell in the **AdminPathCost** column.
13. Type a value in the dialog box.
14. In the port row, double-click the cell in the **PathCost** column.
15. Type a value in the dialog box.

16. You can repeat steps **5** through **15** to configure additional ports as STG members.
17. Click **Apply**.

Variable Definitions

Use the data in the following table to configure switch ports as STG members.

Variable	Value
Port	Specifies the unit and port number.
StgId	Specifies the STG ID number.
Priority	Specifies the port priority
State	Specifies the STP state of the port—Disabled, Blocking, Listening, Learning, and Forwarding.
EnableStp	Enables or disables STP on the port: True is enabled, and False is disabled.
FastStart	Enables or disables Fast Start STP on the port: True is enabled, and False is disabled.
AdminPathCost	Sets the PathCost value. The field displays 0 if no user-configured value exists.
PathCost	Specifies the contribution of this port to the cost path of the spanning tree root.
DesignatedRoot	Specifies the MAC address of the STP designated root.
DesignatedCost	Specifies the path cost of the designated port of the segment connected to this port.
DesignatedBridge	Specifies the MAC address of the designated bridge this port considers the designated bridge for this segment.
DesignatedPort	Specifies the port ID of the designated bridge for this port segment.
ForwardTransitions	Specifies the number of times the port transitioned from STP Learning to Forwarding state.

Chapter 16: RSTP configuration using Enterprise Device Manager

This chapter describes how you can configure Rapid Spanning Tree protocol (RSTP) using Enterprise Device Manager (EDM).

RSTP (or IEEE 802.1w) reduces the recovery time after a network breakdown. It also maintains a backward compatibility with the IEEE 802.1D which was the Spanning Tree implementation prior to RSTP. In certain configurations, the recovery time of RSTP can be reduced to less than 1 second.

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

Prerequisites

Select RSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see [Configuring the STP mode using EDM](#) on page 211.

Navigation

- [Viewing global RSTP information using EDM](#) on page 229
- [Viewing RSTP port information using EDM](#) on page 232
- [Viewing RSTP statistics using EDM](#) on page 234
- [Graphing RSTP port statistics using EDM](#) on page 235

Viewing global RSTP information using EDM

Use this procedure to display global RSTP information .

Prerequisites

Select RSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see [Configuring the STP mode using EDM](#) on page 211.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **RSTP**.
4. On the work area, click the **Globals** tab to display the RSTP information.

Variable Definitions

Variable	Value
PathCostDefault	Sets the version of the Spanning Tree default Path Costs that the Bridge uses. A value of 16-bit uses the 16-bit default Path Costs from IEEE Std. 802.1D-1998. A value of 32-bit uses the 32-bit default Path Costs from IEEE Std. 802.1t.
TXHoldCount	Specifies the value used by the Port Transmit state machine to limit the maximum transmission rate. The value can range from 1–10.
Version	Specifies the version of the Spanning Tree Protocol the bridge is currently running: <ul style="list-style-type: none"> • stpCompatible—indicates that the bridge uses the Spanning Tree Protocol specified in IEEE 802.1D. • rstp—indicates that the bridge uses the Rapid Spanning Tree Protocol specified in IEEE 802.1w.
Priority	Specifies the value of the writable portion of the Bridge Identifier comprising the first two octets. The values that are set for Priority must be in steps of 4096.

Variable	Value
BridgeMaxAge	Specifies the value in 1/100 seconds that all bridges use for MaxAge when this bridge acts as the root. The value must be a multiple of 100. The range is 600–4000.
BridgeHelloTime	Specifies the value in 1/100 seconds that all bridges use for HelloTime when this bridge acts as the root. The value must be a multiple of 100. The range is 100–1000.
BridgeForward Delay	Specifies the value in 1/100 seconds that all bridges use for ForwardDelay when this bridge is acting as the root. The 802.1D-1990 specifies that the range for this parameter is related to the value of BridgeMaxAge. The value must be a multiple of 100. The range is 400–3000.
DesignatedRoot	Specifies the unique identifier of the Bridge recorded as the Root in the Configuration BPDUs that are transmitted by the Designated Bridge for the segment to which the port is attached. Reference IEEE 802.1D-1990: Section 4.5.5.4.
RootCost	Specifies the cost of the path to the root as seen from this bridge.
RootPort	Specifies the port number of the port that offers the lowest cost path from this bridge to the root bridge.
MaxAge	Specifies the maximum age of Spanning Tree Protocol information learned from the network on any port before being discarded. The maximum age is specified in units of hundredths of a second. This is the actual value that the bridge uses.
HelloTime	Specifies the amount of time required for transmission of the configuration BPDUs by the node on any port when it is the root of the spanning tree or trying to become the root. This is specified in units of hundredths of a second. This is the actual value that the bridge uses.
ForwardDelay	Specifies this time value, measured in units of hundredths of a second, controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state.
RstpUpCount	Specifies the number of times the RSTP Module is enabled. A trap is generated on the occurrence of this event.
RstpDownCount	Specifies the number of times the RSTP Module is disabled. A trap is generated on the occurrence of this event
NewRootIdCount	Specifies the number of times this Bridge has detected a Root Identifier change. A trap is generated on the occurrence of this event.

Variable	Value
TimeSinceTopologyChange	Specifies the time (in hundredths of a second) since the TcWhile Timer for any port in this Bridge was non-zero for the Common Spanning Tree context.
TopChanges	Specifies the total number of topology changes detected by this bridge since the management entity was last reset or initialized.

Viewing RSTP port information using EDM

Use the following procedure to display RSTP port information.

Prerequisites

Select RSTP for the Spanning Tree administration mode.


For information about configuring the Spanning Tree administration mode, see [Configuring the STP mode using EDM](#) on page 211.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **RSTP**.
4. On the work area, click the **RSTP Ports** tab.

Variable Definitions

Variable	Value
Port	Specifies the port number.
State	Specifies the port state in this RSTP instance. The port state is cataloged as discarding, learning, and forwarding.
Priority	Specifies the value of the priority field which is in the first (in network byte order) octet of the (2 octet long) Port ID.

Variable	Value
PathCost	Specifies the contribution of this port to the cost of paths towards the spanning tree root.
ProtocolMigration	<p>Specifies the Protocol migration state of this port. Set this field to true to force the port to transmit RSTP BPDUs.</p> <p> Note: If this field is set to true, and the port receives an 802.1D type BPDUs, the port again begins transmitting 802.1D BPDUs.</p>
AdminEdgePort	Specifies the administrative value of the Edge Port parameter. A value of true indicates that this port is assumed to be an edge-port and a value of false indicates that this port is assumed to be a nonedge-port.
OperEdgePort	Specifies the operational value of the Edge Port parameter. The object is initialized to false on reception of a BPDUs.
AdminPointToPoint	<p>Specifies the administrative point-to-point status of the LAN segment attached to this port.</p> <ul style="list-style-type: none"> • forceTrue—indicates that this port is always treated as being connected to a point-to-point link. • forceFalse—indicates that this port is treated as having a shared media connection. • auto—indicates that this port is considered to have a point-to-point link if it is an Aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means.
OperPointToPoint	Specifies the operational point-to-point status of the LAN segment attached to this port. This field indicates whether a port is considered to have a point-to-point connection. The value is determined by management or by autodetection.
Participating	Specifies this field specifies whether a port is participating in the 802.1w protocol.
DesignatedRoot	Specifies the bridge identifier of the old root of the Spanning Tree as determined by the Spanning Tree Protocol as executed by this node.
DesignatedCost	Specifies the path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received BPDUs.
DesignatedBridge	Specifies the Bridge Identifier of the bridge which this port considers to be the Designated Bridge for this port segment.

Variable	Value
DesignatedPort	Specifies the Port Identifier for the port segment which is on the Designated Bridge.
ForwardTransitions	Specifies the number of times this port has transitioned from the Learning state to the Forwarding state.

Viewing RSTP statistics using EDM

Use the following procedure to display the RSTP statistics.

Prerequisites

Select RSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see [Configuring the STP mode using EDM](#) on page 211.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **RSTP**.
4. On the work area, click the **RSTP Status** tab.

Variable Definitions

Variable	Value
Port	Specifies the port number.
Role	Represents a functionality characteristic or capability of a resource to which policies are applied.
OperVersion	Indicates whether the Port is operationally in the RSTP mode or the STP-compatible mode; that is, whether the Port is transmitting RSTP BPDUs or Config/TCN BPDUs.

Variable	Value
EffectivePortState	Specifies the operational state of the port. This object is set to true only when the port is operationally up in the interface manager and when the force Port State and specified port state for this port is enabled. Otherwise, this object is set to false.

Graphing RSTP port statistics using EDM

Use the following procedure to display and graph RSTP port statistics.

Prerequisites

Select RSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see [Configuring the STP mode using EDM](#) on page 211.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **RSTP**.
4. On the work area, click the **RSTP Status** tab.
5. In the table, select a port for which you want to display the statistic graph.
6. On the toolbar, click **Graph** to get the statistics of the selected port.

Variable Definitions

Variable	Value
RxRstBpduCount	Specifies the number of RST BPDUs received on the port.
RxConfigBpduCount	Specifies the number of Config BPDUs received on the port.

Variable	Value
RxTcnBpduCount	Specifies the number of TCN BPDUs received on the port.
TxRstBpduCount	Specifies the number of RST BPDUs transmitted by this port.
TxConfigBpduCount	Specifies the number of Config BPDUs transmitted by this port.
TxTcnBpduCount	Specifies the number of TCN BPDUs transmitted by this port.
InvalidRstBpduRxCount	Specifies the number of invalid RSTP BPDUs received on this port.
InvalidConfigBpduRxCount	Specifies the number of invalid Configuration BPDUs received on this port.
InvalidTcnBpduRxCount	Specifies the number of invalid TCN BPDUs received on this port.
ProtocolMigrationCount	Specifies the number of times this Port is migrated from one STP protocol version to another. The relevant protocols are STP-COMPATIBLE and RSTP.

Chapter 17: MSTP configuration using Enterprise Device Manager

This chapter describes how you can configure Multiple Spanning Tree Protocol (MSTP) using Enterprise Device Manager (EDM).

With MSTP (or IEEE 802.1s), you can configure multiple instances of RSTP on the same switch. Each MSTP instance can include one or more VLANs. The operation of the MSTP is similar to the current Avaya proprietary STG.

In the MSTP mode, the 4500 Series switches support a maximum of one Common and Internal Spanning Tree (CIST) and seven Multiple Spanning Tree Instances (MSTI).

Within the CIST, the Internal Spanning Tree component is used only by devices from the same region (for which a regional root is elected). The Common (External) Spanning Tree component of the CIST is used by devices from different regions or between devices with different STP modes.

Prerequisites

Select MSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see [Configuring the STP mode using EDM](#) on page 211.

Navigation

- [Viewing global MSTP using EDM](#) on page 238
- [Viewing CIST port information using EDM](#) on page 241
- [Graphing CIST port statistics using EDM](#) on page 243
- [Viewing MSTI bridge information using EDM](#) on page 245
- [Viewing MSTI port information using EDM](#) on page 247
- [Graphing MSTI port statistics using EDM](#) on page 249

Viewing global MSTP using EDM

Use this procedure to display global MSTP information.

Prerequisites

Select MSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see [Configuring the STP mode using EDM](#) on page 211.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **Globals** tab.

Variable Definitions

Variable	Value
PathCostDefaultType	Specifies the version of the Spanning Tree default Path Costs that are used by this Bridge. A 16-bit value uses the 16-bit default path costs from IEEE Standard 802.1D-1998. A 32-bit value uses the 32-bit default path costs from IEEE Standard. 802.1t.
TxHoldCount	Specifies the value used by the Port Transmit state machine to limit the maximum transmission rate. The range in 1–10
MaxHopCount	Specifies the Maximum Hop Count value in 1/100 seconds. The value must be a multiple of 100. The range is 100–4000.
NoOfInstancesSupported	Specifies the maximum number of spanning tree instances supported.

Variable	Value
MSTPUpCount	Specifies the number of times the MSTP Module is enabled. A trap is generated on the occurrence of this event.
MSTPDownCount	Specifies the number of times the MSTP Module is disabled. A trap is generated on the occurrence of this event.
ForceProtocolVersion	<p>Signifies the version of the spanning tree protocol that the bridge is currently running.</p> <ul style="list-style-type: none"> • stpCompatible—indicates that the bridge is using the Spanning Tree Protocol as specified in IEEE 802.1D. • rstp—indicates that the bridge is using the Rapid Spanning Tree Protocol as specified in IEEE 802.1w. • MSTP—indicates that the bridge is running the Multiple Spanning Tree Protocol as specified in IEEE 802.1s.
BrgAddress	Specifies the bridge address is generated when events like protocol up or protocol down occurs.
Root	Specifies the bridge identifier of the root of the common spanning tree as determined by the Spanning Tree Protocol as executed by this node. This value is used as the CIST Root Identifier parameter in all Configuration BPDUs originated by this node.
RegionalRoot	Specifies the bridge identifier of the root of the Multiple Spanning Tree region as determined by the Spanning Tree Protocol as executed by this node. This value is used as the CIST Regional Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
RootCost	Specifies the cost of the path to the CIST Root as seen from this bridge.
RegionalRootCost	Specifies the cost of the path to the CIST Regional Root as seen from this bridge.
RootPort	Specifies the port number of the port which offers the lowest path cost from the bridge to the CIST Root Bridge
BridgePriority	Specifies the value of the writable portion of the Bridge Identifier comprising the first two octets. The values that are set for Bridge Priority must be in steps of 4096.

Variable	Value
BridgeMaxAge	Specifies the value in hundredths of a second that all bridges use for MaxAge when this bridge acts as the root. The value must be a multiple of 100. The range is 600–4000.
BridgeForwardDelay	Specifies the value in hundredths of a second that all bridges use for ForwardDelay when this bridge acts as the root. IEEE 802.1D specifies that the range for this parameter is related to the value of BridgeMaxAge. The value must be a multiple of 100. The range is 400–3000.
HoldTime	Determines the time interval during which no more than two Configuration BPDUs can be transmitted by this node. This value is measured in units of hundredths of a second.
MaxAge	Specifies the maximum age, in hundredths of a second, of the Spanning Tree Protocol information learned from the network on any port before being discarded. This value is the actual value that this bridge is currently using.
ForwardDelay	Controls how fast a port changes its STP state when moving towards the Forwarding state. This value determines how long the port stays in a particular state before moving to the next state. This value is measured in units of hundredths of a second.
TimeSinceTopology Change	Specifies the time, in hundredths of a second, since the TcWhile Timer for any port in this Bridge was non-zero for the Common Spanning Tree context.
TopChanges	Specifies the number of times that at least one non-zero TcWhile Timer occurred on this Bridge for the Common Spanning Tree context.
NewRootBridgeCount	Specifies the number of times this Bridge detects a Root Bridge change for the Common Spanning Tree context. A Trap is generated when this event occurs.
RegionName	Specifies the region name of the configuration. By default, the Region Name is equal to the Bridge Mac Address.
RegionVersion	Specifies the version of the MST Region.
ConfigIdSel	Specifies the Configuration Identifier Format Selector used by the Bridge. This has a fixed value of 0 which indicates RegionName, RegionVersion, as specified in the standard.

Variable	Value
ConfigDigest	Signifies the Configuration Digest value for this Region. This is an MD5 digest value and hence must always be 16 octets long.
RegionConfigChange Count	Specifies the number of times a Region Configuration Identifier Change is detected. A trap is generated when this event occurs.

Viewing CIST port information using EDM

Use this procedure to display CIST port information.

Prerequisites

Select MSTP for the Spanning Tree administration mode.


For information about configuring the Spanning Tree administration mode, see [Configuring the STP mode using EDM](#) on page 211.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **CIST Ports** tab.

Variable Definitions

Variable	Value
Port	Specifies the port number of the port containing Spanning Tree information.
PathCost	Specifies the contribution of this port to the cost of paths towards the CIST Root.
Priority	Specifies the four most significant bits of the Port Identifier of the Spanning Tree instance. It can be

Variable	Value
	modified by setting the CISTPortPriority value. The values that are set for Port Priority must be in steps of 16.
DesignatedRoot	Specifies the unique Bridge Identifier of the bridge. Recorded as the CIST Root in the configuration BPDUs which are transmitted.
DesignatedCost	Specifies the path cost of the Designated Port of the segment connected to this port.
DesignatedBridge	Specifies the unique Bridge Identifier of the bridge which the port considers to be the Designated Bridge for the port segment.
DesignatedPort	Specifies the Port identifier of the port on the Designated Bridge which is designated for the port segment.
RegionalRoot	Displays the unique Bridge Identifier of the bridge. Recorded as the CIST Regional Root Identifier in the configuration BPDUs which are transmitted.
RegionalPathCost	Specifies the contribution of this port to the cost of paths towards the CIST Regional Root.
ProtocolMigration	<p>Specifies the Protocol migration state of this port. When operating in MSTP mode, set this field to true to force the port to transmit MSTP BPDUs without instance information.</p> <p> Important:</p> <p>If this field is set to true and the port receives an 802.1D BPDU, the port begins transmitting 802.1D BPDUs. If the port receives an 802.1w BPDU, it begins transmitting 802.1w BPDUs.</p>
AdminEdgeStatus	Specifies the administrative value of the Edge Port parameter. A value of true indicates that this port can be assumed to be an edge-port, and a value of false indicates that this port can be assumed to be a nonedge-port.
OperEdgeStatus	Specifies the operational value of the Edge Port parameter. This value is initialized to the value of AdminEdgeStatus and set to false when the port receives a BPDU.
AdminP2P	Specifies the administrative point-to-point status of the LAN segment attached to this port. A value of 0 indicates that this port is always treated as being connected to a point-to-point link. A value of 1 indicates that this port is treated as having a shared media connection. A value of 2 indicates that this port

Variable	Value
	is considered to have a point-to-point link if it is an Aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation, or by management means.
OperP2P	Indicates the operational point-to-point status of the LAN segment attached to the port. It also indicates whether a port is considered to have a point-to-point connection. The value is determined by management or by autodetection, as described in the AdminP2P object.
HelloTime	Specifies the amount of time between the transmission of Configuration BPDUs transmitted by this node on the port. Measured in units of hundredths of a second.
OperVersion	Indicates whether the Port is operationally in the MSTP, RSTP, or STP-compatible mode; that is, whether the port is transmitting MST BPDUs, RST BPDUs, or Config/TCN BPDUs.
EffectivePortState	Specifies the operational state of the port for CIST. This is set to true only when the port is operationally up in the Interface level and Protocol level for CIST. This is set to false for all other times.
State	Specifies the current state of the port as defined by the Common Spanning Tree Protocol.
ForcePortState	Specifies the current state of the port which can be changed to either Disabled or Enabled for the base Spanning Tree instance.
SelectedPortRole	Specifies the selected port role for the Spanning Tree instance.
CurrentPortRole	Specifies the current port role for the Spanning Tree instance.

Graphing CIST port statistics using EDM

Use this procedure to display and graph CIST port statistics.

Prerequisites

Select MSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see [Configuring the STP mode using EDM](#) on page 211.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **CIST Ports** tab.
5. Select a port for which you want to view the statistic graph.
6. On the toolbar, click **Graph** to get the statistics for the CIST Port.

Variable Definitions

Variable	Value
ForwardTransitions	Specifies the number of times this port transitioned to the Forwarding State.
RxMstBpduCount	Specifies the number of MST BPDUs received on this port.
RxRstBpduCount	Specifies the number of RST BPDUs received on this port.
RxConfigBpduCount	Specifies the number of Configuration BPDUs received on this port.
RxTcnBpduCount	Specifies the number of TCN BPDUs received on this port.
TxMstBpduCount	Specifies the number of MST BPDUs transmitted from this port.
TxRstBpduCount	Specifies the number of RST BPDUs transmitted from this port.
TxConfigBpduCount	Specifies the number of Configuration BPDUs transmitted from this port.

Variable	Value
TxTcnBpduCount	Specifies the number of TCN BPDUs transmitted from this port.
InvalidMstBpduRxCount	Specifies the number of Invalid MST BPDUs received on this port.
InvalidRstBpduRxCount	Specifies the number of Invalid RST BPDUs received on this port.
InvalidConfigBpdu RxCount	Specifies the number of Invalid Configuration BPDUs received on this port.
InvalidTcnBpduRxCount	Specifies the number of Invalid TCN BPDUs received on this port.
ProtocolMigrationCount	Specifies the number of times this port migrated from one STP protocol version to another. The relevant migration protocols are STP-COMPATIBLE and RSTP/MSTP. A trap is generated when the port migrates.

Viewing MSTI bridge information using EDM

Use this procedure to display MSTI bridge information..

Prerequisites

Select MSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see [Configuring the STP mode using EDM](#) on page 211.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **MSTI Bridges** tab.

Variable Definitions

Variable	Value
Instance	Specifies the Spanning Tree Instance to which the information belongs.
RegionalRoot	Specifies the MSTI Regional Root Identifier value for the Instance. This value is used as the MSTI Regional Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
Priority	Specifies the writable portion of the MSTI Bridge Identifier comprising the first two octets. The values that are set for Bridge Priority must be in steps of 4096.
RootCost	Specifies the cost of the path to the MSTI Regional Root as seen by this bridge.
RootPort	Specifies the number of the port which offers the lowest path cost from this bridge to the MSTI Region Root Bridge.
Enabled	Used to control whether the bridge instance is enabled or disabled.
TimeSinceTopology Change	Specifies the time (measured in hundredths of a second) since the TcWhile Timer for any port in this Bridge was non-zero for this Spanning Tree instance.
TopChanges	Specifies the number of times that at least one non-zero TcWhile Timer occurred on this Bridge for this Spanning Tree instance.
NewRootCount	Specifies the number of times this Bridge has detected a Root Bridge change for this Spanning Tree instance. A Trap is generated on the occurrence of this event.
InstanceUpCount	Specifies the number of times a new Spanning Tree instance was created. A Trap is generated on the occurrence of this event.
InstanceDownCount	Specifies the number of times a Spanning Tree instance was deleted. A Trap is generated on the occurrence of this event.

Inserting MSTI Bridges using EDM

Use the following procedure to insert an MSTI bridge.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **MSTI Bridges** tab.
5. On the toolbar, click **Insert**.

The Insert MSTI Bridges dialog box appears with the next available instance shown.

6. Click **Insert**.

Deleting MSTI Bridges using EDM

Use the following procedure to delete an MSTI bridge.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **MSTI Bridges** tab.
5. In the table, select the MSTI bridge instance that you want to delete.
6. On the toolbar, click **Delete**.

The selected instance is deleted from the MSTI Bridges tab.

Viewing MSTI port information using EDM

Use this procedure to display MSTI port information.

Prerequisites

Select MSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see [Configuring the STP mode using EDM](#) on page 211.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **MSTI Port** tab.

Variable Definitions

Variable	Value
Port	Specifies the port number.
Instance	Specifies the number of times a Spanning Tree instance was deleted. A Trap is generated when this event occurs.
State	Specifies the current state of the port as defined by the Multiple Spanning Tree Protocol. The state of a port can be Forwarding or Discarding (Blocking).
ForcePortState	Specifies the current state of the port which can be changed to either Disabled or Enabled for the specific Spanning Tree instance.
PathCost	Specifies the contribution of this port to the cost of paths towards the MSTI Root which includes this port.
Priority	Specifies the four most significant bits of the Port Identifier for a given Spanning Tree instance. This value can be modified independently for each Spanning Tree instance supported by the Bridge. The values set for Port Priority must be in steps of 16.

Variable	Value
DesignatedRoot	Specifies the unique Bridge Identifier of the bridge recorded as the MSTI Regional Root in the configuration BPDUs that are transmitted.
DesignatedBridge	Specifies the unique Bridge Identifier of the bridge which this port considers to be the Designated Bridge for the port segment.
DesignatedPort	Specifies the Port identifier of the port on the Designated Bridge for this port segment.
DesignatedCost	Specifies the path cost of the Designated Port of the segment connected to this port.
CurrentPortRole	Specifies the Current Port Role of the port for this spanning tree instance.
EffectivePortState	Specifies the effective operational state of the port for the specific instance. This is set to true only when the port is operationally up in the interface level and Protocol level for the specific instance. This is set to false at all other times.

Graphing MSTI port statistics using EDM

Use this procedure to display and graph MSTI port statistics.

Prerequisites

Select MSTP for the Spanning Tree administration mode.

For information about configuring the Spanning Tree administration mode, see [Configuring the STP mode using EDM](#) on page 211.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree tree, double-click **MSTP**.
4. On the work area, click the **MSTI Port** tab.

5. In the table, select the port for which you want to view the statistics.
6. On the toolbar, click **Graph** to get the statistics for the MSTI Port.

Variable Definitions

Variable	Value
ForwardTransitions	Specifies the number of times this port transitioned to the Forwarding State for the specific instance.
ReceivedBPDUs	Specifies the number of BPDUs received by this port for this spanning tree instance.
TransmittedBPDUs	Specifies the number of Invalid BPDUs received on this Port for this Spanning Tree instance.
InvalidBPDUsRcvd	Specifies the number of BPDUs transmitted on this port for this Spanning Tree instance.

Chapter 18: Configuring ADAC using Enterprise Device Manager

This chapter provides information you can use to configure Autodetection and Autoconfiguration (ADAC) using Enterprise Device Manager (EDM).

Navigation

- [Configuring ADAC globally using EDM](#) on page 251
- [ADAC MAC address range configuration using EDM](#) on page 253
- [ADAC port configuration using EDM](#) on page 254

Configuring ADAC globally using EDM

Use the following procedure to configure ADAC for the switch.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **ADAC**.
3. Click the **ADAC** tab.
4. Select the **AdminEnable** check box to enable ADAC.
OR
Clear the **AdminEnable** check box to disable ADAC.
5. In the **OperatingMode** section, select a radio button.
6. Select the **NotificationControlEnable** check box to enable trap notifications.
OR
Clear the **NotificationControlEnable** check box to disable trap notifications.

7. Double-click the **Voice VLAN** dialog box to edit the value as required.
8. Click the **CallServerPortList** elipsis.
9. From the call server port list, select call server ports.
10. Click **Ok**.
11. Click the **UplinkPortList** elipsis.
12. From the uplink port list, select uplink ports.
13. Click **Ok**.
14. In the **MacAddrRangeControl** section, select a radio button.
15. Click **Apply**.


 **Important:**

You cannot apply the global ADAC configuration if VoiceVLAN, CallServerPort, or UplinkPort boxes are set to 0 or empty when AdminEnable is selected and the operating mode is tagged frames or advanced untagged frames.

 **Important:**

You cannot configure the same port values for Call Server and Uplink.

Variable Definitions

Variable	Value
AdminEnable	Enables or disables ADAC.
OperEnable	Indicates ADAC operational state: true is enabled and false is disabled.  Important: If AdminEnable is True and OperEnable is False, this indicates an error condition such as missing Uplink and Call Server ports.
OperatingMode	Selects the ADAC operation mode: <ul style="list-style-type: none"> • 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.

Variable	Value
VoiceVLAN	Sets the Voice VLAN ID.
CallServerPort	Selects the Call Server port. A maximum of 8 Call Server ports are supported.
UplinkPort	Selects the Uplink port. A maximum of 8 Uplink ports are supported.
MacAddrRangeControl	Selects a MAC address range table control option. <ul style="list-style-type: none"> • none—default • clearTable—clears all MAC address range table entries. • defaultTable—replaces all MAC address range table entries to default values.

ADAC MAC address range configuration using EDM

Use the information in this section to manage the ADAC MAC address range table.

ADAC MAC address range configuration using EDM navigation

- [Creating a ADAC MAC address range using EDM](#) on page 253
- [Deleting MAC address ranges using EDM](#) on page 254

Creating a ADAC MAC address range using EDM

Use the following procedure to add an Avaya IP Phone MAC address range to the ADAC MAC address range table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **ADAC**.
3. Click the **ADAC MAC Ranges** tab.
4. Click **Insert**.

5. In the **MacAddrRangeLowEndIndex** box, type the MAC address for the low end of the IP Phone MAC address range.
6. In the **MacAddrRangeHighEndIndex** box, type the MAC address for the high end of the IP Phone MAC address range.
7. Click **Insert**.
8. Click **Apply**.

Deleting MAC address ranges using EDM

Use the following procedure to remove Avaya IP Phone MAC address ranges from the ADAC MAC address range table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **ADAC**.
3. Click the **ADAC MAC Ranges** tab.
4. Click the MAC address range to delete.
5. Click **Delete**.

ADAC port configuration using EDM

Use the information in this section to configure ADAC for switch ports and to display port-based ADAC information.

ADAC port configuration using EDM navigation

- [Viewing the ADAC configuration for ports using EDM](#) on page 254
- [Configuring ADAC for specific ports using EDM](#) on page 256

Viewing the ADAC configuration for ports using EDM

Use the following procedure to display the ADAC configuration for ports on the switch.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis** then double-click **Ports**.

OR

In the Edit tree, double-click **ADAC** .


3. In the Ports work area, click the **ADAC** tab.



OR

In the ADAC work area, click the **ADAC Ports** tab.

Variable Definitions

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

Variable	Value
Index	Indicates the switch position in a stack and the port number. The default value for a standalone switch is 1.
Index	Indicates the switch position in the stack and the port number. For a standalone switch, the switch position is 1.
AdminEnable	Indicates whether ADAC is enabled (true) or disabled (false) for the port.
OperEnable	Indicates whether the port ADAC operational state is true (enabled) or false (disabled). This is a read-only cell.  Important: If OperEnable is false and AdminEnable is true, ADAC is disabled. This can occur if you reach the maximum number of devices supported on a port.
ConfigStatus	Indicates the ADAC status for the port. <ul style="list-style-type: none"> • configApplied—the ADAC configuration is applied to the port. • configNotApplied—the ADAC configuration is not applied to the port. This is a read-only cell.

Variable	Value
TaggedFramesPVID	Indicates the unique Port VLAN identifier (PVID). Values range from 0–4094. A value of 0 indicates that Auto-Configuration cannot change the PVID for the port.
TaggedFramesTagging	Indicates the tagging value that Auto-Configuration applies to a port that has ADAC enabled and has tagged frames selected as the operating mode. <ul style="list-style-type: none"> • tagAll—tagging is enabled on all frames • tagPvidOnly—tagging is enabled on frames with a PVID that matches the PVID of this port • untagPvidOnly—tagging is disabled on frames with a PVID that matches the PVID of this port • noChange—accepts frames without change
AdacPortType	Indicates how ADAC classifies the port: <ul style="list-style-type: none"> • telephony—autodetection is enabled for the port • callServer—the port is configured as a Call Server • uplink—the port is configured as an Uplink • other—the port is not classified as telephony, callServer, or uplink
MacDetectionEnable	Indicates whether Autodetection of Avaya IP Phones, based on MAC address is enabled (true) or disabled (false) on the interface. <p> Important: You cannot configure MacDetectionEnable to false if no other supported detection mechanism is enabled on the port.</p>
LldpDetectionEnable	Indicates whether Autodetection of Avaya IP Phones, based on 802.1ab is enabled (true) or disabled (false) on the interface. <p> Important: You cannot configure LldpDetectionEnable to false if no other supported detection mechanism is enabled on the port.</p>

Configuring ADAC for specific ports using EDM

Use the following procedure to configure ADAC for one or more ports in a standalone switch or switch stack.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis** then double-click **Ports**.

OR

In the Edit tree, double-click **ADAC** .

3. In the Ports work area, click the **ADAC** tab.

OR


In the ADAC work area, click the **ADAC Ports** tab.



4. To select a port to edit, click the port **Index**.
5. In the port row, double-click the cell in the **AdminEnable** column.
6. Select a value from the list—**true** to enable ADAC for the port, or **false** to disable ADAC for the port.
7. In the port row, double-click the cell in the **TaggedFramesPvid** column.
8. Type a value in the dialog box.
9. In the port row, double-click the cell in the **TaggedFramesTagging** column.
10. Select a value from the list.
11. In the port row, double-click the cell in the **MacDetectionEnable** column.
12. Select a value from the list—**true** to enable MAC address detection for the port, or **false** to disable MAC address detection for the port.
13. In the port row, double-click the cell in the **LldpDetectionEnable** column.
14. Select a value from the list—**true** to enable LLDP detection for the port, or **false** to disable LLDP detection for the port.
15. You can repeat steps **4** through **14** to configure ADAC for additional ports.
16. Click **Apply**.

Variable Definitions

Use the data in this table to configure port-based ADAC.

Variable	Value
Index	Indicates the switch position in a stack and the port number. The default value for a standalone switch is 1.

Variable	Value
AdminEnable	Enables (true) or disables (false) ADAC for the port.
OperEnable	<p>Indicates whether the port ADAC operational state is true (enabled) or false (disabled). This is a read-only cell.</p> <p> Important: If OperEnable is false and AdminEnable is true, ADAC is disabled. This can occur if you reach the maximum number of devices supported on a port.</p>
ConfigStatus	<p>Indicates the ADAC status for the port.</p> <ul style="list-style-type: none"> • configApplied—the ADAC configuration is applied to the port. • configNotApplied—the ADAC configuration is not applied to the port. <p>This is a read-only cell.</p>
TaggedFramesPVID	Specifies a unique Port VLAN identifier (PVID). Values range from 0–4094. A value of 0 indicates that Auto-Configuration cannot change the PVID for the port.
TaggedFramesTagging	<p>Specifies the tagging value that Auto-Configuration applies to a port that has ADAC enabled and has tagged frames selected as the operating mode.</p> <ul style="list-style-type: none"> • tagAll—tagging is enabled on all frames • tagPvidOnly—tagging is enabled on frames with a PVID that matches the PVID of this port • untagPvidOnly—tagging is disabled on frames with a PVID that matches the PVID of this port • noChange—accepts frames without change
AdacPortType	<p>Indicates how ADAC classifies the port:</p> <ul style="list-style-type: none"> • telephony—autodetection is enabled for the port • callServer—the port is configured as a Call Server • uplink—the port is configured as an Uplink • other—the port is not classified as telephony, callServer, or uplink
MacDetectionEnable	Specifies whether Autodetection of Avaya IP Phones, based on MAC address is enabled (true) or disabled (false) on the interface.

Variable	Value
	 Important: You cannot configure MacDetectionEnable to false if no other supported detection mechanism is enabled on the port.
LldpDetectionEnable	Specifies whether Autodetection of Avaya IP Phones, based on 802.1ab is enabled (true) or disabled (false) on the interface.  Important: You cannot configure LldpDetectionEnable to false if no other supported detection mechanism is enabled on the port.

Chapter 19: Configuring LACP and VLACP using Enterprise Device Manager

This chapter provides information you can use to configure Link Aggregation Control Protocol (LACP) and Virtual LACP (VLACP) using Enterprise Device Manager (EDM).

Navigation

- [Viewing LAG information using EDM](#) on page 261
- [Link Aggregation Group configuration using EDM](#) on page 263
- [LACP configuration for ports using EDM](#) on page 267
- [Graphing port LACP statistics using EDM](#) on page 272
- [Global VLACP configuration using EDM](#) on page 273
- [VLACP configuration for ports using EDM](#) on page 274

Viewing LAG information using EDM

Use the following procedure to display Link Aggregation Group (LAG) configuration information.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **LACP** tab.

Variable Definitions

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

Variable	Value
Index	Indicates the unique identifier allocated to an Aggregator by the local system.
MacAddress	Indicates the MAC address assigned to an Aggregator.
AggregateOrIndividual	Indicates if an Aggregator represents an Aggregate (TRUE) or an individual link (FALSE).
ActorLagID	Indicates the combined information of ActorSystemPriority, ActorSystemID, and ActorOperKey in ActorSystemPriority-ActorSystemID-ActorOperKey format.
ActorSystemPriority	Indicates the priority value associated with the Actor's System ID.
ActorSystemID	Indicates the MAC address of the System that contains this Aggregator.
ActorOperKey	Indicates the current operational value of the Aggregator key.
ActorAdminKey	Indicates the current administrative value of the Aggregator key.
PartnerLagID	Indicates the combined of PartnerSystemPriority, PartnerSystemID, and PartnerOperKey in PartnerSystemPriority-PartnerSystemID-PartnerOper Key format.
PartnerSystemPriority	Indicates the priority value associated with the Partner System ID.
PartnerSystemID	Indicates the MAC address of the current protocol partner of this Aggregator. A value of zero indicates that no known Partner exists. If the aggregation is manually configured, this System ID value is assigned by the local System.
PartnerOperKey	Indicates the operational key value of the current Aggregator protocol partner.
CollectorMaxDelay	Indicates the maximum delay, in tens of microseconds, that can be imposed by the Frame Collector between receiving a frame from an Aggregator parser, and either delivering the frame to its MAC client or discarding the frame.

Link Aggregation Group configuration using EDM

Use the procedures in this section to display or modify LAG member configuration.

Link Aggregation Group configuration using EDM navigation

- [Viewing LACP for LAG members using EDM](#) on page 263
- [Configuring LACP for specific LAG members using EDM](#) on page 264

Viewing LACP for LAG members using EDM

Use the following procedure to display the existing LACP configuration for LAG members.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **LACP Ports** tab.

Variable Definitions

Use the data in this table to help you understand the LACP configuration for LAG members display.

Variable	Value
Index	Indicates the unique identifier allocated to an Aggregator by the local system.
AdminEnabled	Indicates the current administrative setting for the port. A value of true enables the port to participate in LACP. A value of false disables the port from participating in LACP.
OperEnabled	Indicates the current operational state for the port. A value of true means the port is participating in LACP. A value of false means the port is not participating in LACP.

Variable	Value
ActorAdminState	Indicates the Actor administrative state for the port. Values include: <ul style="list-style-type: none"> • lacpActive • aggregation • shortTimeout
ActorOperState	Indicates the current operational values of Actor state transmitted by the Actor in LACPDUs.
AggregateOrIndividual	Indicates whether the port represents an Aggregate or an Individual link.
ActorPortPriority	Indicates the priority value assigned to this Aggregation port. Values range from 0–65535.
ActorAdminKey	Indicates the current administrative value of the Key for the Aggregation Port. Values range from 1–4095.
ActorOperKey	Indicates the current operational value of the Key for the Aggregation Port.
SelectedAggID	Indicates the identifier value of the Aggregator that this Aggregation Port has currently selected. Zero indicates that the Aggregation Port has not selected an Aggregator, either because it is in the process of detaching from an Aggregator or because no suitable Aggregator exists for it to select.
AttachedAggID	Indicates the identifier value of the Aggregator that this Aggregation Port is currently attached to. Zero indicates that the Aggregation Port is not currently attached to an Aggregator. This value is read-only.
ActorPort	Indicates the port number locally assigned to the Aggregation Port. The port number is communicated in LACPDUs as the Actor_Port. This value is read-only
MltId	Indicates the MLT that the port is assigned to. If the port is not assigned to an MLT, the MltId value is 0.
PartnerOperPort	Indicates the operational port number assigned by the port protocol partner.
OperStatus	Indicates the operational status of the interface. Values are up (operational) or down (not operational).

Configuring LACP for specific LAG members using EDM

Use the following procedure to configure LACP for one or more LAG member ports.

Prerequisites

- Ensure members you want to configure are not ADAC Call Server or Uplink ports.
- Disable ADAC for members you want to configure

 **Important:**

To configure the port LACP mode to active, you must set the **AdminEnabled** value to **true** and the **ActorAdminState** value to **lacpActive**.

 **Important:**


To configure the port LACP mode to passive, you must set the **AdminEnabled** value to **false** and clear the **lacpActive**, **aggregation**, and **shortTimeout** check boxes in **ActorAdminState**.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **LACP Ports** tab.
4. To select a port to configure, click the port **Index**.
5. In the port row, double-click the cell in the **AdminEnabled** column.
6. Select a value from the list—**true** to enable LACP for the port, or **false** to disable LACP for the port.
7. In the port row, double-click the cell in the **ActorAdminState** column.
8. Select an individual or combination of check boxes.
9. Click **Ok**.
10. In the port row, double-click the cell in the **ActorPortPriority** column.
11. In the dialog box, edit the value as required.
12. In the port row, double-click the cell in the **ActorAdminKey** column.
13. In the dialog box, edit the value as required.
14. You can repeat steps **4** through **13** to configure LACP for additional ports.
15. Click **Apply**.

Variable Definitions

Use the data in this table to configure LACP for LAG members.

Variable	Value
Index	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
AdminEnabled	<p>Specifies the current administrative setting for the port. A value of true enables the port to participate in LACP. A value of false disables the port from participating in LACP.</p> <p> Important: You cannot enable ports to participate in LACP if they are members of an enabled MLT.</p>
OperEnabled	Indicates the current operational state for the port. A value of true means the port is participating in LACP. A value of false means the port is not participating in LACP. This is a read-only cell.
ActorAdminState	<p>Specifies the Actor administrative state. Values include:</p> <ul style="list-style-type: none"> • lacpActive • aggregation • shortTimeout
ActorOperState	Indicates the current Actor operational state. This is a read-only cell.
AggregateOrIndividual	Indicates whether the Aggregator represents an Aggregate or an Individual link. This is a read-only cell.
ActorPortPriority	Specifies the priority value assigned to this Aggregation port. Values range from 0–65535.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation Port. Values range from 1–4095.
ActorOperKey	Indicates the current operational value of the Key for the Aggregation Port. This is a read-only cell.
SelectedAggID	Indicates the identifier value of the Aggregator that this Aggregation Port has currently selected. Zero indicates that the Aggregation Port has not selected an Aggregator, either because it is in the process of detaching from an Aggregator or because no suitable Aggregator exists for it to select. This is a read-only cell.
AttachedAggID	Indicates the identifier value of the Aggregator that this Aggregation Port is currently attached to. Zero indicates

Variable	Value
	that the Aggregation Port is not currently attached to an Aggregator. This is a read-only cell.
ActorPort	Indicates the port number locally assigned to the Aggregation Port. The port number is communicated in LACPDU as the Actor_Port. This is a read-only cell.
MltId	Indicates the MLT that the port is assigned to. If the port is not assigned to an MLT, the MltId value is 0. This is a read-only cell.
PartnerOperPort	The operational port number assigned by the port's protocol partner. This is a read-only cell.
OperStatus	Indicates the operational status of the interface. Values are up (operational) or down (not operational). This is a read-only cell.

LACP configuration for ports using EDM

You can use the information in this section to display or modify the LACP configuration for switch ports.

LACP configuration for ports using EDM navigation

- [Viewing the LACP configuration for ports using EDM](#) on page 267
- [Configuring LACP for ports using EDM](#) on page 269

Viewing the LACP configuration for ports using EDM


Use the following procedure to display the existing LACP configuration for switch ports.



Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. Click the **LACP** tab.

Variable definitions

Use the data in this table to help you understand the LACP configuration display for switch ports.

Variable	Value
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. Values range from 0–65535.
AdminEnabled	<p>Specifies the current administrative setting for the port. A value of true enables the port to participate in LACP. A value of false disables the port from participating in LACP.</p> <p> Important: You cannot enable ports to participate in LACP if they are members of an enabled MLT.</p>
OperEnabled	Indicates the current operational state for the port. A value of true means the port is participating in LACP. A value of false means the port is not participating in LACP. This is a read-only cell.
ActorAdminState	<p>Specifies the Actor administrative state. Values include:</p> <ul style="list-style-type: none"> • lacpActive • aggregation • shortTimeout
ActorOperState	Indicates the current Actor operational state. This is a read-only cell.
AggregateOrIndividual	Indicates whether the Aggregator represents an Aggregate or an Individual link. This is a read-only cell.
ActorPortPriority	Specifies the priority value assigned to this Aggregation port. Values range from 0–65535.
ActorSystemID	Indicates the MAC address of the System that contains this Aggregator.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation Port. Values range from 1–4095.
ActorOperKey	Indicates the current operational value of the Key for the Aggregation Port. This is a read-only cell.
SelectedAggID	Indicates the identifier value of the Aggregator that this Aggregation Port has currently selected. Zero indicates

Variable	Value
	that the Aggregation Port has not selected an Aggregator, either because it is in the process of detaching from an Aggregator or because no suitable Aggregator exists for it to select. This is a read-only cell.
AttachedAggID	Indicates the identifier value of the Aggregator that this Aggregation Port is currently attached to. Zero indicates that the Aggregation Port is not currently attached to an Aggregator. This is a read-only cell.
ActorPort	Indicates the port number locally assigned to the Aggregation Port. The port number is communicated in LACPDUs as the Actor_Port. This is a read-only cell.
PartnerOperPort	Indicates the operational port number assigned by the port's protocol partner. This is a read-only cell.
<p> Important: To configure the port LACP mode to active, you must set the AdminEnabled value to true and the ActorAdminState value to lacpActive.</p> <p> 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.</p>	

Configuring LACP for ports using EDM

Use the following procedure to modify the LACP configuration for switch ports.

Prerequisites

- Ensure ports you want to configure are not ADAC Call Server or Uplink ports.
- Disable ADAC for ports you want to configure


Procedure steps


1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. Click the **LACP** tab.

5. To select a port to configure, click the port **Index**.
6. In the port row, double-click the cell in the **ActorSystemPriority** column.
7. In the dialog box, edit the value as required.
8. In the port row, double-click the cell in the **AdminEnabled** column.
9. Select a value from the list—**true** to enable LACP for the port, or **false** to disable LACP for the port.
10. In the port row, double-click the cell in the **ActorAdminState** column.
11. Select an individual or combination of check boxes
12. Click **Ok**.
13. In the port row, double-click the cell in the **ActorPortPriority** column.
14. In the dialog box, edit the value as required.
15. In the port row, double-click the cell in the **ActorAdminKey** column.
16. In the dialog box, edit the value as required.
17. You can repeat steps **5** through **17** to configure LACP for additional ports as required.
18. Click **Apply**.

Variable definitions

Use the data in this table to help you to understand the LACP configuration.

Variable	Value
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. Values range from 0–65535.
AdminEnabled	<p>Specifies the current administrative setting for the port. A value of true enables the port to participate in LACP. A value of false disables the port from participating in LACP.</p> <p> Important: You cannot enable ports to participate in LACP if they are members of an enabled MLT.</p>
OperEnabled	Indicates the current operational state for the port. A value of true means the port is participating in LACP. A value of false means the port is not participating in LACP. This is a read-only cell.
ActorAdminState	Specifies the Actor administrative state. Values include:

Variable	Value
	<ul style="list-style-type: none"> • lacpActive • aggregation • shortTimeout
ActorOperState	Indicates the current Actor operational state. This is a read-only cell.
AggregateOrIndividual	Indicates whether the Aggregator represents an Aggregate or an Individual link. This is a read-only cell.
ActorPortPriority	Specifies the priority value assigned to this Aggregation port. Values range from 0–65535.
ActorSystemID	Indicates the MAC address of the System that contains this Aggregator. This is a read-only cell.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation Port. Values range from 1–4095.
ActorOperKey	Indicates the current operational value of the Key for the Aggregation Port. This is a read-only cell.
SelectedAggID	Indicates the identifier value of the Aggregator that this Aggregation Port has currently selected. Zero indicates that the Aggregation Port has not selected an Aggregator, either because it is in the process of detaching from an Aggregator or because no suitable Aggregator exists for it to select. This is a read-only cell.
AttachedAggID	Indicates the identifier value of the Aggregator that this Aggregation Port is currently attached to. Zero indicates that the Aggregation Port is not currently attached to an Aggregator. This is a read-only cell.
ActorPort	Indicates the port number locally assigned to the Aggregation Port. The port number is communicated in LACPDU as the Actor_Port. This is a read-only cell.
PartnerOperPort	Indicates the operational port number assigned by the protocol partner of port. This is a read-only cell.
<p> Important: To configure the port LACP mode to active, you must set the AdminEnabled value to true and the ActorAdminState value to lacpActive.</p> <p> 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.</p>	

Graphing port LACP statistics using EDM

Use the following procedure to display and graph LACP statistics for switch ports.

Procedure steps

1. From the Device Physical View, click a port.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **LACP** tab.
5. On the toolbar, select a **Poll Interval** from the list.
6. To select statistics to graph, click a statistic type row under a column heading.
7. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

Use the data in the following table to help you understand the LACP port statistics display.

Variable	Value
LACPDUsRx	Denotes the number of valid LACPDUs received on this Aggregation Port. This value is read-only.
MarkerPDUsRx	Signifies the number of valid Marker PDUs received on this Aggregation Port. This value is read-only.
MarkerResponse PDUsRx	The number of valid Marker Response PDUs received on this Aggregation Port. This value is read-only.
UnknownRx	Indicates the number of frames received that can <ul style="list-style-type: none"> • Carry the Slow Protocols Ethernet Type value (43B.4), but contain an unknown PDU. • Are addressed to the Slow Protocols group MAC Address (43B.3), but do not carry the Slow Protocols Ethernet Type. This value is read-only.
IllegalRx	Denotes the number of frames received that carry the Slow Protocols Ethernet Type value (43B.4), but contain a badly

Variable	Value
	formed PDU or an illegal value of Protocol Subtype (43B.4). This value is read-only.
LACPDUstx	Signifies the number of LACPDUstx that are transmitted on this Aggregation Port. This value is read-only.
MarkerPDUstx	Displays the number of Marker PDUs transmitted on this Aggregation Port. This value is read-only.
MarkerResponse PDUstx	Indicates the number of Marker Response PDUs that are transmitted on this Aggregation Port. This value is read-only.

Global VLACP configuration using EDM

Use the information in this section to enable or disable VLACP globally.

Global VLACP configuration using EDM navigation

- [Enabling global VLACP using EDM](#) on page 273
- [Disabling global VLACP using EDM](#) on page 274

Enabling global VLACP using EDM

Use the following procedure to enable VLACP for the switch.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **VLACP Global** tab.
4. Select the **Enable** check box.
5. Type a value in the MulticastMACAddress dialog box.
6. Click **Apply**.

Variable Definitions

Use the data in this table to enable VLACP globally.

Variable	Value
MulticastMACAddress	Specifies a multicast MAC address used exclusively for VLACPDU. The default is 01:80:c2:00:11:00.

Disabling global VLACP using EDM

Use the following procedure to disable VLACP for the switch.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **VLACP Global** tab.
4. Clear the **Enable** check box.
5. Click **Apply**.

VLACP configuration for ports using EDM

Use the procedures in this section to view and configure VLACP at the port level.

VLACP configuration for ports using EDM navigation

- [Viewing the VLACP configuration for ports using EDM](#) on page 274
- [Configuring VLACP for specific ports using EDM](#) on page 276

Viewing the VLACP configuration for ports using EDM


Use the following procedure to display the VLACP configuration for all ports on a switch or stack.


Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. Click the **VLACP** tab.

Variable Definitions

Use the data in this table to help you understand the displayed port-level VLACP configuration.

Variable	Value
rcPortIndex	Indicates the switch and port number.
AdminEnable	Indicates whether VLACP is enabled (true) or disabled (false) on ports. The default value is disabled.
OperEnable	Indicates whether VLACP is operationally enabled (true) or disabled (false).  Important: VLACP is only operational when OperEnable is true and PortState is up.
FastPeriodicTimer	Indicates the number of milliseconds between periodic transmissions using short timeouts. Valid values range from 400-20000 with a default of 500.
SlowPeriodicTimer	Indicates the number of milliseconds between periodic transmissions using long timeouts. Values range from 10000-30000 with a default of 30000.
Timeout	Indicates whether the timeout control value is a short or long timeout.
TimeoutScale	Indicates the scale value used to calculate timeout from periodic time. Values range from 1–10. The default is 3. With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. If the timeout-scale is set to 1, the port timeout value does not take into account the normal travel 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.

Variable	Value
	Avaya recommends that you set the timeout scale to a value larger than 1.
EtherType	Indicates VLACP protocol identification. The value can be entered as a numerical value ranging from 33025–33279 or a hexadecimal equivalent (8101–81ff). The default is 8103. Use the prefix 0x to type a hexadecimal value in the dialog box. Only hexadecimal values display in the EtherType column of the VLACP work area.
EtherMacAddress	<p>Indicates the MAC address of the switch or stack to which this port is sending VLACPDUs. This value cannot be configured as a multicast MAC. The default value is 00:00:00:00:00:00.</p> <p>VLACP uses only the multicast MAC address configured when VLACP is enabled globally. This is the Layer 2 destination address used for the VLACPDUs. The port-specific EtherMacAddress specifies the MAC address of the switch or stack to which this port is sending VLACPDUs. If you do not type a value for the EtherMacAddress, the first VLACP-enabled switch that receives the PDUs from a sending port becomes the intended recipient and processes the PDUs.</p> <p>If you want an intermediate switch to drop VLACP packets, configure EtherMacAddress with the desired destination MAC address. With EtherMacAddress configured, the intermediate switches do not misinterpret the VLACP packets.</p>
PortState	<p>Indicates whether the VLACP port state is up or down.</p> <p> Important: VLACP is only operational when OperEnable is true and PortState is up.</p>

Configuring VLACP for specific ports using EDM

Use the following procedure to configure VLACP for a single port or multiple ports.


Procedure steps


1. From the navigation tree, double-click **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 **rcPortIndex** row.
6. In the port row, double-click the cell in the **AdminEnable** column.
7. Select 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. Select a value from the list.
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. You can repeat steps **4** through **19** to configure VLACP for additional ports as required.
21. Click **Apply**.

Variable Definitions

Use the data in this table to edit the VLACP configuration for individual ports.

Variable	Value
rcPortIndex	Specifies the switch and port number.
AdminEnable	Indicates whether VLACP is enabled (true) or disabled (false) on ports. The default value is disabled.
OperEnable	Indicates whether VLACP is operationally enabled or disabled. This is a read-only cell.  Important: VLACP is only operational when OperEnable is true and PortState is up.
FastPeriodicTimer	Specifies the number of milliseconds between periodic transmissions using short timeouts. Valid values range from 400-20000 with a default of 500.

Variable	Value
SlowPeriodicTimer	Specifies the number of milliseconds between periodic transmissions using long timeouts. Valid values range from 10000-30000 with a default of 30000.
Timeout	Specifies whether the timeout control value is a short or long timeout.
TimeoutScale	Specifies the scale value used to calculate timeout from periodic time. Values range from 1–10. The default is 3. With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. If the timeout-scale is set to 1, the port timeout value does not take into account the normal travel time of the VLACPDU. The port expects to receive a VLACPDU at the same moment the partner port sends it. Therefore, the delayed VLACPDU results in the link being blocked, and then enabled again when the packet arrives. Avaya recommends that you set the timeout scale to a value larger than 1.
EtherType	Specifies VLACP protocol identification. The value can be entered as a numerical value ranging from 33025–33279 or a hexadecimal equivalent (8101–81ff). The default is 8103. Use the prefix 0x to type a hexadecimal value in the dialog box. Only hexadecimal values display in the EtherType column of the VLACP work area.
EtherMacAddress	<p>Specifies the MAC address of the switch or stack to which a port is sending VLACPDUs. The default value is 00:00:00:00:00:00. It cannot be configured as a multicast MAC.</p> <p>VLACP uses only the multicast MAC address configured when VLACP is enabled globally. This is the Layer 2 destination address used for the VLACPDUs. If you do not type a value for the EtherMacAddress, the first VLACP-enabled switch that receives the PDUs from a sending port becomes the intended recipient and processes the PDUs. If you want an intermediate switch to drop VLACP packets, configure EtherMacAddress with the desired destination MAC address. With EtherMacAddress configured, the intermediate switches do not misinterpret the VLACP packets.</p>
PortState	<p>Indicates whether the VLACP port state is up or down. This is a read-only cell.</p> <p> Important: VLACP is only operational when OperEnable is true and PortState is up.</p>