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

6.3
NN47200-502, 07.01
August 2012

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

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

Copyright

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://www.avaya.com/support/Copyright/.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

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

Contents

Chapter 1: New in this Release 13
Features 13
802.1AB Integration 13
802.1AB new default parameters 14
MLT/DMLT/LAG Dynamic VLAN Changes 14
SLPP Guard 14
Voice VLAN Integration 14
Chapter 2: Purpose of this document 15
ACLI command modes 15
Chapter 3: VLAN fundamentals 17
VLANs 17
IEEE 802.1Q tagging 18
VLANs spanning multiple switches 24
VLAN summary 27
VLAN configuration rules 28
VCC 29
Multinetting 30
MLT DMLT LAG dynamic VLAN changes 30
DHCP 30
Voice VLAN Integration 31
Chapter 4: STP fundamentals 33
STP groups 33
STG configuration guidelines 34
Spanning Tree Fast Learning 35
STG port membership mode 36
802.1t path cost calculation 36
RSTP 37
MSTP 37
Interoperability with legacy STP 38
Differences in STP and RSTP port roles 38
Rapid convergent 39
Spanning Tree BPDU Filtering 41
Configuring Spanning Tree using the Console Interface 42
Spanning Tree configuration in STPG mode 42
Spanning Tree configuration in RSTP mode 50
Spanning Tree configuration in MSTP mode 56
Spanning Tree VLAN Membership in MSTP mode 63
Chapter 5: MLT fundamentals 65
MLT 65
Client-server configuration using MLT 65
Before configuring trunks 66
MLT configuration rules 67
Port management for existing MLTs 69
How a MLT reacts to losing distributed trunk members 69

Spanning Tree Considerations for MLTs 70
Port membership in MLT 73
SMLT 74
Overview 74
Advantages of SMLT 75
How does SMLT work? 76
SLT 98
SMLT with SLT 100
SMLT and SLT configuration steps 102
SLPP 113
SLPP Guard 113
LACP over SMLT 114
SMLT with Routing protocol support 115
SMLT consistency with the Ethernet Routing Switch 8800/8600 115
IEEE 802.3ad Link Aggregation 115
Link aggregation rules 116
LACP port mode 117
Chapter 6: VLACP Fundamentals 119
VLACP 119
VLACP overview 119
VLACP features 121
Chapter 7: ADAC fundamentals 123
ADAC operation 123
Auto-detection of Avaya IP Phones 124
Auto-detection by MAC address 124
Auto-detection by LLDP (IEEE 802.1ab) 126
Auto-configuration of Avaya IP Phones 127
Initial user settings 128
Operating modes 129
ADAC and stacking 134
ADAC and LACP enabled on an Uplink port 135
ADAC and EAP configuration 135
ADAC user restrictions 136
Chapter 8: LLDP fundamentals 137
LLDP overview 137
LLDP operational modes 138
Connectivity and management information 139
802.1AB MED network policies 142
802.1AB integration 142
Chapter 9: VLAN Configuration using ACLI 145
Creating and Managing VLANs using the ACLI 145
Displaying VLAN information 145
Displaying VLAN interface information 146
Displaying VLAN port membership 147
Setting the management VLAN 147
Resetting the management VLAN to default 147
Displaying Voice VLAN information 148

Creating a VLAN 148
Deleting a VLAN 149
Disabling a voice VLAN 150
Modifying VLAN MAC address flooding 150
Configuring VLAN name 151
Enabling automatic PVID 151
Configuring VLAN port settings 151
Configuring VLAN members 152
Configuring VLAN Configuration Control 153
Displaying VLAN Configuration Control settings 154
Modifying VLAN Configuration Control settings 154
Managing the MAC address forwarding database table 155
Displaying MAC address forwarding table 155
Configuring MAC address retention 156
Setting MAC address retention time to default 156
Clearing the MAC address table 156
Clearing the MAC address table on a VLAN 157
Clearing the MAC address table on a FastEthernet interface 157
Clearing the MAC address table on a trunk 157
Removing a single address from the MAC address table 157
IP Directed Broadcasting 158
Enabling IP directed broadcast 158
Chapter 10: STP Configuration using the ACLI 159
Setting the STP mode using the ACLI 159
Configuring STP BPDU Filtering using the ACLI 159
Creating and Managing STGs using the ACLI 160
Configuring path cost calculation mode 160
Configuring STG port membership mode 161
Displaying STP configuration information 161
Creating a Spanning Tree Group 162
Deleting a Spanning Tree Group 162
Enabling a Spanning Tree Group 162
Disabling a Spanning Tree Group 163
Configuring STP values 163
Restoring default Spanning Tree values 164
Adding a VLAN to a STG 165
Removing a VLAN from a STG 165
Configuring STP and MSTG participation 166
Resetting Spanning Tree values for ports to default 167
Managing RSTP using the ACLI 168
Configuring RSTP parameters 168
Configuring RSTP on a port 169
Displaying RSTP configuration 170
Displaying RSTP port configuration 170
Managing MSTP using the ACLI 171
Configuring MSTP parameters 171
Configuring MSTP on a port 172

Configuring MSTP region parameters 173
Configuring MSTP parameters 174
Disabling a MSTP bridge instance 175
Deleting a MSTP bridge instance 175
Displaying MSTP status 175
Displaying MSTP Cist port information 176
Displaying MSTP MSTI settings 177
Chapter 11: MLT Configuration using the ACLI 179
Displaying MLT configuration and utilization 179
Job aid: show mlt command output 179
Configuring a Multi-Link trunk 180
Disabling an MLT 181
Displaying MLT properties 181
Displaying IP address-based MLT load-balance link calculation 182
Variable definitions 182
Displaying MAC address-based MLT load-balance link calculation 182
Variable definitions 183
Configuring MLT port shutdown when MLT is disabled 183
Enabling shutdown on MLT ports when MLT is disabled 183
Disabling MLT port shutdown when MLT is disabled 183
Setting default value to the MLT port shutdown when MLT is disabled 184
Displaying the MLT port shutdown status when MLT is disabled 184
Configuring STP participation for MLTs 184
Configuring SMLT using the ACLI 185
Setting command mode to MLT Interface mode 185
Creating a SMLT 186
Creating a IST 186
Creating a SLT on a port 187
Disabling SMLT 188
Disabling IST 188
Disabling a SLT on a port 188
Resetting SMLT to default 189
Resetting a IST to default 189
Resetting a SMLT to default 190
Displaying IST parameters 190
Displaying IST statistics 190
Displaying SLT and SMLT configurations 190
Configuring SLPP using the ACLI 191
Configuring SLPP transmitting list 191
Enabling SLPP 191
Configuring SLPP PDU transmit interval 192
Configuring SLPP PDU ether type 192
Configuring SLPP port auto enable 193
Enabling SLPP PDU receive function per port 193
Configuring the SLPP PDU receipt threshold 193
Configuring SLPP Guard using ACLI 194
Selecting an SLPP Guard Ethernet type using ACLI 194

Configuring SLPP Guard using ACLI ... 195
Viewing the SLPP Guard status using ACLI ... 196
Link Aggregation Control Protocol over SMLT using the ACLI ... 197
Configuring an SMLT MAC address ... 198
Configuring the default SMLT MAC address ... 198
Binding an MLT group to an administrative key and to an SMLT ... 199
Freeing an MLT group ... 200
Troubleshooting IST problems ... 200
Chapter 12: LACP and VLACP Configuration using the ACLI ... 203
Configuring Link Aggregation using the ACLI ... 203
Displaying LACP system settings ... 203
Displaying LACP per port configuration ... 203
Displaying LACP port mode ... 204
Displaying LACP port statistics ... 204
Clearing LACP port statistics ... 205
Displaying LACP port debug information ... 205
Displaying LACP aggregators ... 205
Configuring LACP system priority ... 205
Enabling LACP port aggregation mode ... 206
Configuring the LACP administrative key ... 206
Configuring LACP operating mode ... 207
Configuring per port LACP priority ... 207
Configuring LACP periodic transmission timeout interval ... 208
Configuring LACP port mode ... 208
Configuring VLACP using the ACLI ... 209
Enabling VLACP globally ... 209
Configuring VLACP multicast MAC address ... 209
Configuring VLACP port parameters ... 210
Displaying VLACP status ... 212
Displaying VLACP port configuration ... 212
Chapter 13: ADAC Configuration using ACLI ... 215
Configuring ADAC for Avaya IP Phones using ACLI ... 215
Configuring global ADAC settings ... 215
Restoring default ADAC settings ... 216
Configuring ADAC per port settings ... 217
Resetting ADAC per port settings to default ... 217
Configuring autodetection method ... 218
Resetting autodetection method to default ... 219
Configuring autodetection for ports ... 219
Restoring ADAC port settings ... 220
Adding a range to ADAC MAC address table ... 220
Restoring ADAC MAC range table ... 220
Displaying global ADAC settings ... 221
Displaying ADAC port settings ... 221
Displaying ADAC MAC ranges ... 221
Displaying configured detection mechanism ... 222
ADAC UFA configuration example ... 222

ADAC configuration commands........ 223
Verifying new ADAC settings........ 223
ADAC and EAP configuration commands........ 225
Chapter 14: LLDP Configuration using ACLI........ 229
Configuring LLDP transmit properties........ 229
Configuring LLDP Timers using ACLI........ 230
Configuring LLDP port parameters........ 231
Configuring management TLVs for LLDP ports........ 231
Configuring dot1 TLVs for LLDP ports........ 232
Configuring dot3 TLVs for LLDP ports........ 233
Configuring TLVs for MED devices........ 234
Configuring parameters for LLDP location identification........ 234
Configuring LLDP civic address parameters........ 235
Configuring the LLDP emergency call service emergency location identification number........ 237
Setting LLDP transmission parameters to default values........ 237
Setting port parameters to default values........ 238
Setting Management TLVs to default values........ 239
Setting the IEEE 802.1 organizationally-specific TLVs to default values........ 240
Setting the IEEE 802.3 organizationally-specific TLVs to default values........ 241
Setting optional TLVs for MED devices to default values........ 242
Disabling LLDP features on the port........ 243
Configuring Management TLVs........ 243
Configuring the IEEE 802.1 TLVs........ 243
Configuring the IEEE 802.3 TLVs........ 244
Configuring optional TLVs for MED devices........ 244
Displaying configuration data for LLDP........ 244
Configuring LLDP MED policies for switch ports........ 246
Setting lldp med-network-policies to the default values........ 248
Disabling LLDP MED policies for switch ports........ 248
Viewing lldp med-network-policies........ 249
Configuring LLDP........ 250
802.1AB Integration configuration........ 258
Chapter 15: VLANs Configuration using Enterprise Device Manager........ 265
Displaying VLAN configuration........ 265
Creating a VLAN........ 266
Modifying a VLAN........ 267
Deleting VLANs........ 267
Clearing DHCP statistics counters on a VLAN........ 268
Configuring VLAN Snoop........ 268
Configuring VLAN Ports........ 269
VLAN NSNA Configuration........ 270
Viewing VLAN NSNA........ 271
Configuring NSNA per VLAN........ 271
Deleting an NSNA VLAN........ 272
Filtering an NSNA VLAN........ 273
Enabling AutoPVID........ 274
MAC address table maintenance........ 274

Flushing the MAC address table.......... 274
Selecting VLAN configuration control.......... 275
Chapter 16: Spanning Tree Configuration using Enterprise Device Manager.......... 277
Setting the STP mode.......... 277
Resetting the switch.......... 278
Configuring STP BPDU filtering for specific ports.......... 278
Spanning Tree STG configuration.......... 279
Configuring STG Global properties.......... 279
Creating an STG.......... 280
Adding a VLAN to an STG.......... 281
Moving a VLAN between STGs.......... 281
Deleting an STG.......... 282
Displaying STG Status.......... 282
Displaying STG ports.......... 283
Configuring STG port properties.......... 284
Rapid Spanning Tree Protocol.......... 285
Viewing RSTP general information.......... 286
Displaying RSTP ports information.......... 288
Displaying RSTP status.......... 289
Graphing RSTP port statistics.......... 290
Multiple Spanning Tree Protocol.......... 291
Displaying MSTP general information.......... 292
Displaying CIST port information.......... 294
Graphing CIST Port statistics.......... 296
Displaying MSTI Bridges.......... 298
Inserting MSTI Bridges.......... 299
Deleting MSTP MSTI Bridges.......... 299
Associating a VLAN with the CIST or an MSTI instance.......... 300
Modifying VLAN CIST or MSTI association.......... 300
Viewing MSTP MSTI Ports.......... 300
Graphing MSTP MSTI Port Statistics.......... 302
Chapter 17: MLT Configuration using Enterprise Device Manager.......... 303
MultiLink Trunks configuration.......... 303
Configuring Multi-Link Trunks.......... 303
Filtering the Multi-Link Trunks tab display.......... 305
Adding MLT Ports.......... 305
Disabling MLT ports on Shutdown.......... 305
Configuring SMLT.......... 306
Adding an MLT-based SMLT.......... 306
Viewing SLTs configured on your switch.......... 307
Configuring an SLT.......... 307
Deleting an SLT.......... 308
Configuring an IST MLT.......... 309
Removing an IST MLT.......... 310
Viewing IST statistics.......... 310
Chapter 18: LACP and VLACP Configuration using Enterprise Device Manager.......... 313
LACP Configuration.......... 313

Configuring the LACP port compatibility mode.... 313
Configuring Link Aggregation Groups.... 314
Configuring LACP ports.... 315
Mapping the LACP key mapping.... 317
VLACP Configuration.... 317
Viewing VLACP Global information.... 317
VLACP tab for ports.... 318
Chapter 19: SLPP Configuration using Enterprise Device Manager.... 321
Configuring SLPP transmitting list.... 321
Enabling SLPP.... 321
Configuring SLPP PDU transmit interval.... 322
Configuring SLPP PDU ether type.... 322
Configuring SLPP port auto enable.... 322
Enabling SLPP PDU received function per port.... 323
Configuring the SLPP PDU receipt threshold.... 323
Configuring SLPP Guard using Enterprise Device Manager.... 324
Selecting an SLPP Guard Ethernet type using EDM.... 324
Configuring SLPP Guard using EDM.... 324
Viewing the SLPP Guard configuration using EDM.... 325
Chapter 20: ADAC Configuration using Enterprise Device Manager.... 327
Configuring ADAC settings.... 327
Configuring ADAC MAC address ranges using EDM.... 328
Deleting MAC address ranges using Device Manager.... 329
Configuring ADAC settings on a port.... 329
Chapter 21: Bridge configuration using Enterprise Device Manager.... 333
Displaying basic system bridge information.... 333
Viewing transparent bridge information.... 334
Viewing forwarding bridge information.... 334
Chapter 22: LLDP configuration using Enterprise Device Manager.... 337
Configuring LLDP transmit properties.... 337
Viewing LLDP remote properties.... 339
Configuring LLDP ports.... 341
Displaying LLDP transmit statistics.... 342
Graphing LLDP transmit statistics.... 343
Displaying LLDP receive statistics.... 343
Graphing LLDP receive statistics.... 345
Viewing LLDP local system properties.... 345
Viewing LLDP local port properties.... 347
Viewing LLDP management properites.... 348
Viewing LLDP remote management properties.... 349
Viewing LLDP organizationally-specific properties.... 350
LLDP Port dot1 configuration using Enterprise Device Manager.... 352
Viewing LLDP VLAN ID properties.... 352
Viewing LLDP protocol properties.... 354
Viewing LLDP VLAN ID properties.... 355
Viewing LLDP Neighbor Protocol VLAN properties.... 355
Viewing LLDP VLAN Name properties.... 356

Viewing LLDP Neighbor Protocol properties.......... 357
LLDP Port dot3 configuration using Enterprise Device Manager.......... 358
Viewing LLDP auto-negotiation properties.......... 358
Viewing LLDP PoE porperties.......... 359
Viewing LLDP link aggregation properties.......... 360
Viewing LLDP maximum frame size properties.......... 361
Viewing LLDP neighbor auto-negotiation properties.......... 361
Viewing LLDP neighbor PoE properties.......... 362
Viewing LLDP neighbor link aggregation properties.......... 363
Viewing LLDP neighbor maximum frame size properties.......... 364
LLDP Port MED configuration using Enterprise Device Manager.......... 365
Viewing local policy properties.......... 365
Viewing local location properties.......... 366
Viewing coordinate-based location details.......... 367
Viewing civic address location details.......... 368
Viewing LLDP local PoE PSE properties.......... 370
Viewing LLDP neighbor capabilities properties.......... 370
Viewing LLDP neighbor policy properties.......... 371
Viewing LLDP neighbor location properties.......... 372
Viewing coordinate-based location details.......... 373
Viewing civic address location details.......... 374
Viewing LLDP neighbor PoE properties.......... 374
Viewing LLDP neighbor PoE PSE properties.......... 375
Viewing LLDP neighbor PoE PD properties.......... 376
Viewing LLDP neighbor inventory properties.......... 377
LLDP MED policy management using Enterprises Device Manager.......... 379
Viewing LLDP MED policies.......... 379
Creating LLDP MED policies.......... 380
Editing LLDP MED policies.......... 381
Deleting LLDP MED policies.......... 383
Configuring LLDP Timers using EDM.......... 383
Enabling or disabling Avaya TLV transmit flags.......... 385
Configuring the PoE conservation level request TLV.......... 386
Configuring the 802.1Q framing TLV.......... 387
Configuring the switch call server IP address TLV.......... 388
Configuring the switch file server IP address TLV.......... 388
Viewing Avaya IP phone power level TLV information.......... 389
Viewing remote call server IP address TLV information.......... 390
Viewing remote file server IP address TLV information.......... 391
Viewing PoE conservation level support TLV information.......... 392
Viewing remote 802.1Q Framing TLV information.......... 393
Viewing remote IP TLV information.......... 394
Appendix A: LACP over SMLT configuration example.......... 397
LACP over SMLT configuration example.......... 397
Switch A configuration.......... 397
Switch B configuration.......... 398
Switch C configuration.......... 399

Index.. 401

Chapter 1: New in this Release

The following sections detail what's new in *Avaya Ethernet Routing Switch 5000 Configuration — VLANs, Spanning Tree and Link Aggregation,* NN47200-502 Release 6.3.

Features

See the following sections for information about feature changes:

802.1AB Integration

802.1AB Integration enhances the functionality to support heritage Avaya IP Phones and UC/ IP Telephony solutions.

The newly supported features configured on the switch-side are:

- PoE Conservation Level Request TLV - Setting the PoE Conservation Level
- Call Server TLV - Define up to 8 Call server IP addresses
- File Server TLV - Define up to 4 File server IP addresses
- 802.1Q Framing TLV - Set the advertisement of Layer 2 priority tagging information with parameter options as per CLI command structure example

Added support for receiving, storing and displaying the TLVs sent by the Avaya IP Phones:

- PoE Conservation Levels TLV – power conservation levels supported by the Avaya IP Phone.
- Phone IP TLV – the IP address set for the Avaya IP Phone.
- Call Server TLV – the IP address used by the Avaya IP Phone to access the Call Server.
- File Server TLV – the IP address used by the Avaya IP Phone to access the File Server.
- 802.1Q Framing TLV – the tagging mode used by the Avaya IP Phone for 802.1Q framing.

802.1AB new default parameters

Beginning with Release 6.3, you can improve Voice and Video over IP function because some of the LLDP parameters are enabled by default. Now you can connect LLDP enabled IP handsets to the switch and start deployment without additional configuration. The following per-interface LLDP parameters are enabled by default:

- lldp config-notification
- lldp status txAndRx config-notification
- lldp tx-tlv local-mgmt-addr port-desc sys-desc sys-name
- lldp tx-tlv dot3 mdi-power-support
- lldp tx-tlv med extendedPSE inventory location med-capabilities network-policy
- lldp med-network-policies voice dscp 46 priority 6

MLT/DMLT/LAG Dynamic VLAN Changes

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

SLPP Guard

You can use Simple Loop Prevention Protocol (SLPP) Guard with Split Multi-Link Trunking (SMLT) to provide additional loop protection that occurs during switch clustering. SLPP Guard is necessary as to use SMLT, STP/MSTP/RSTP must be disabled on links to the switch performing switch clustering.

Voice VLAN Integration

Voice VLAN Integration provides centralized creation and management of up to 6 voice VLANS using VLAN-specific commands. With Voice VLAN Integration, each application (e.g. ADAC or EAP) will use these voice VLANs. For ADAC this means you must configure a VLAN as Voice type and be present on the switch before you can configure the ADAC to use that VLAN. As the ADAC VLAN is no longer dynamic, this brings additional benefits in that VLAN membership and configuration can be customized and retained across reboots and that if required, Layer 3 can also be enabled on the ADAC VLAN.

Chapter 2: Purpose of this document

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

ACLI command modes

ACLI provides the following command modes:

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

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

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

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

Command mode and sample prompt	Entrance commands	Exit commands

User EXEC
`5650TD>`
	No entrance command, default mode	`exit`
		or
		`logout`

Privileged EXEC
`5650TD#`
	`enable`	`exit`
		or
		`logout`

Global Configuration
`5650TD(config)#`
	`configure`	To return to Privileged EXEC mode, enter:
		`end`
		or
		`exit`

Command mode and sample prompt	Entrance commands	Exit commands
		To exit ACLI completely, enter: `logout`

Interface Configuration
`5650TD(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`

Router Configuration
`5650TD (config-router)#`
	From Global Configuration mode, to configure OSPF, enter:
	`router ospf`
	To configure RIP, enter:
	`router rip`
	To configure VRRP, enter:
	`router vrrp`
		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 5000 Series Fundamentals* , NN47200-104

Chapter 3: VLAN fundamentals

The following sections describe Virtual Local Area Network (VLAN) fundamentals.

VLANs

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

Important:

The target scaling number is up to 4096 concurrent VLAN IDs with the scaling capacity limited to 1024 simultaneous VLANs. The ERS 5000 Series supports a maximum of 1024 VLANs.

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

Setting up VLAN is a method to segment networks to increase network capacity and performance without changing the physical network topology (Figure 1: Port-based VLAN on page 18). 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.

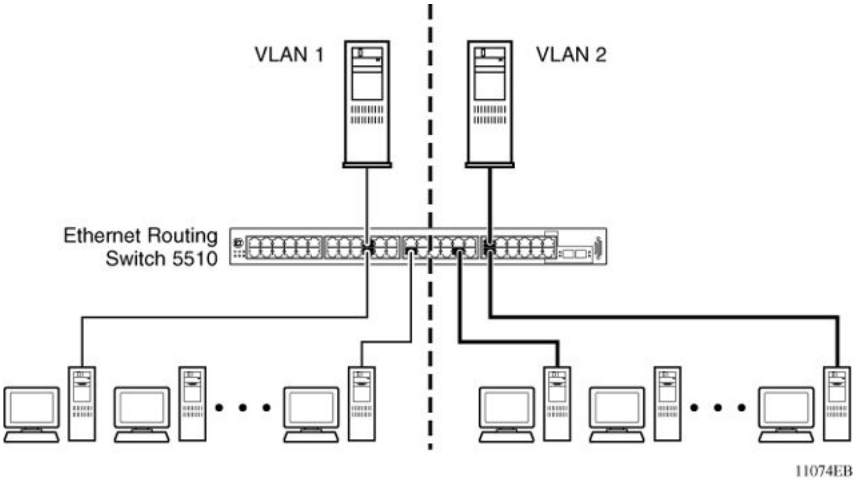


Figure 1: Port-based VLAN

You can assign ports to a VLANs using ACLI, or EDM. Different ports (and their devices) can be assigned to different broadcast domains. VLANs can be reassigned to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.

IEEE 802.1Q tagging

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

- VLAN identifier (VID) -- the 12-bit portion of the VLAN tag in the frame header that identifies an explicit VLAN. When other types of VLANs are enabled, this default value can be overridden by the values enabled in the management interfaces.
- Port VLAN identifier (PVID) -- a classification mechanism that associates a port with a specific VLAN. For example, a port with a PVID of 3 (PVID =3) assigns all untagged frames received on this port to VLAN 3.
- Tagged frame -- a frame that contains the 32-bit 802.1q field (VLAN tag). This field identifies the frame as belonging to a specific VLAN.
- Untagged frame -- a frame that does not carry any VLAN tagging information in the frame header.
- VLAN port members -- a group of ports that are all members of a particular VLAN. A port can be a member of one or more VLANs.
- Untagged member -- a port that has been configured as an untagged member of a specific VLAN. When an untagged frame exits the switch through an untagged member port, the frame header remains unchanged. When a tagged frame exits the switch through an untagged member port, the tag is stripped and the tagged frame is changed to an untagged frame.
- Tagged member -- a port that has been configured as a tagged member of a specific VLAN. When an untagged frame exits the switch through a tagged member port, the frame

header is modified to include the 32-bit tag associated with the ingress port PVID. When a tagged frame exits the switch through a tagged member port, the frame header remains unchanged (original VID remains).

- User priority -- a three-bit field in the header of a tagged frame. The field is interpreted as a binary number, therefore has a value of 0 - 7. This field allows the tagged frame to carry the user-priority across bridged LANs where the individual LAN segments may be unable to signal priority information.
- Port priority -- the priority level assigned to untagged frames received on a port. This value becomes the user priority for the frame. Tagged packets get their user priority from the value contained in the 32-bit 802.1Q frame header.
- Unregistered packet -- a tagged frame that contains a VID where the receiving port is not a member of that VLAN.
- Filtering database identifier (FID) -- the specific filtering/forwarding database within the Avaya Ethernet Routing Switch 5000 Series switch that is assigned to each VLAN. Each VLAN has its own filtering database, which is called independent VLAN learning (IVL). IVLs can have duplicate MAC addresses in different VLANs.

The default configuration settings for the Avaya Ethernet Routing Switch 5000 Series have all ports set as untagged members of VLAN 1 with all ports configured as PVID = 1. Every VLAN is assigned a unique VLAN identifier (VID) that distinguishes it from all other VLANs. In the default configuration example shown in Figure 2: Default VLAN settings on page 20, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID =1). Untagged packets enter and leave the switch unchanged.

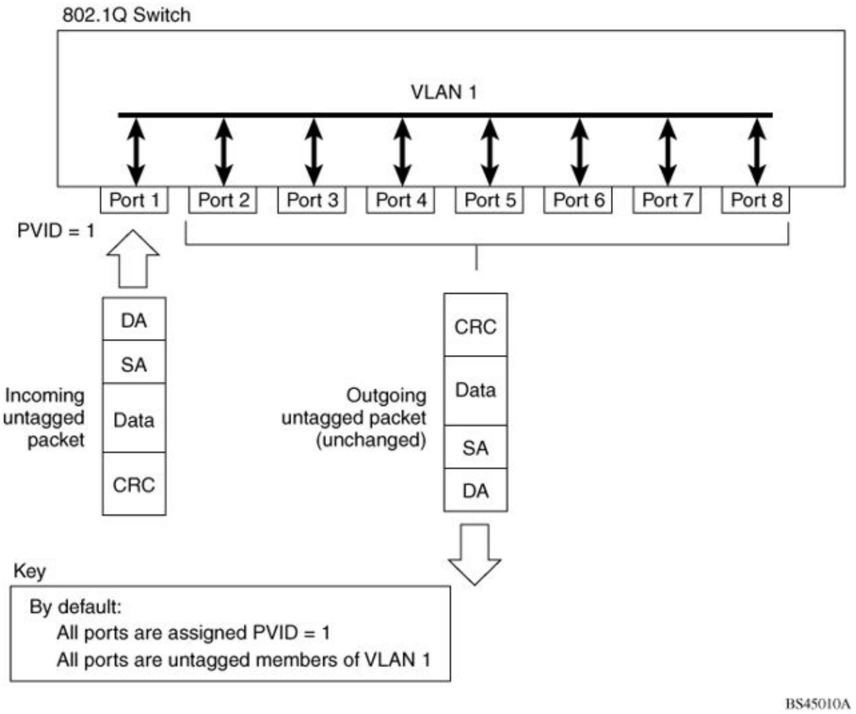


Figure 2: Default VLAN settings

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

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

In [Figure 3: Port-based VLAN assignment](#) on page 20, untagged incoming packets are assigned directly to VLAN 2 (PVID = 2). Port 5 is configured as a *tagged* member of VLAN 2, and port 7 is configured as an *untagged* member of VLAN 2.

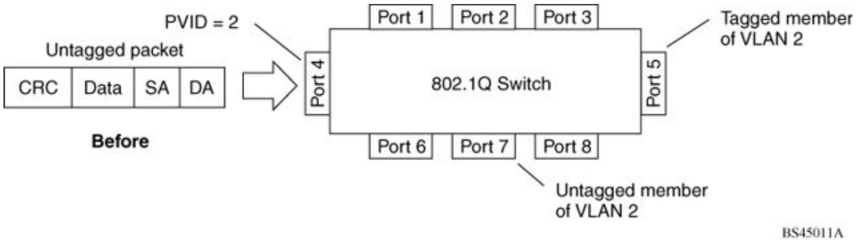


Figure 3: Port-based VLAN assignment

As shown in [Figure 4: 802.1Q tagging (after port-based VLAN assignment)](#) on page 21, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.

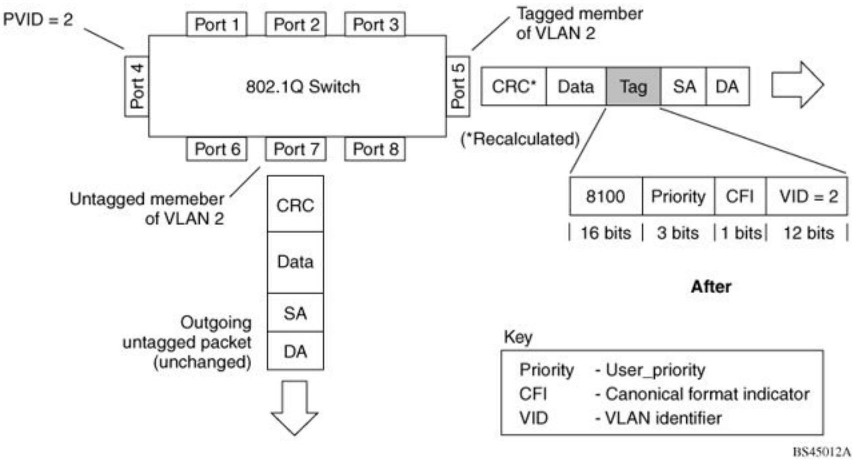


Figure 4: 802.1Q tagging (after port-based VLAN assignment)

In Figure 5: Protocol-based VLAN assignment on page 21, untagged incoming packets are assigned to VLAN 3 (protocol-based VLAN = 3, PVID = 2). Port 5 is configured as a tagged member of VLAN 3, and port 7 is configured as an untagged member of VLAN 3.

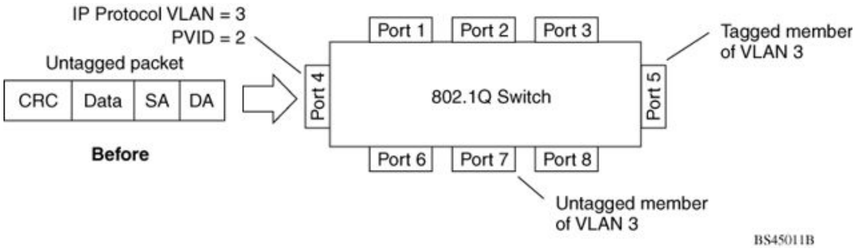


Figure 5: Protocol-based VLAN assignment

In Figure 6: 802.1Q tagging (after protocol-based VLAN assignment) on page 22, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of VLAN 3. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of VLAN 3.

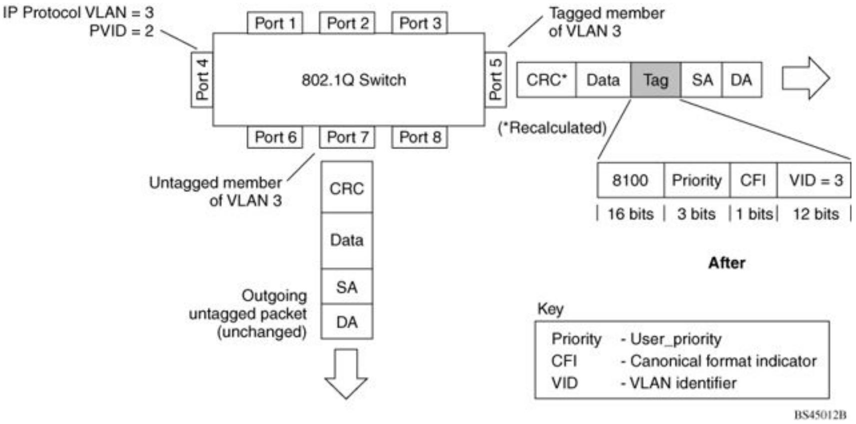


Figure 6: 802.1Q tagging (after protocol-based VLAN assignment)

In Figure 7: 802.1Q tag assignment on page 22, tagged incoming packets are assigned directly to VLAN 2 because of the tag assignment in the packet. Port 5 is configured as a tagged member of VLAN 2, and port 7 is configured as an untagged member of VLAN 2.

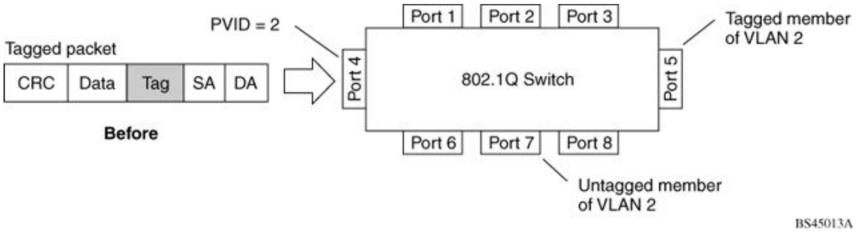


Figure 7: 802.1Q tag assignment

In Figure 8: 802.1Q tagging (after 32-bit 802.1Q tag assignment) on page 23, the tagged packet remains unchanged as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. However, the tagged packet is stripped (untagged) as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.

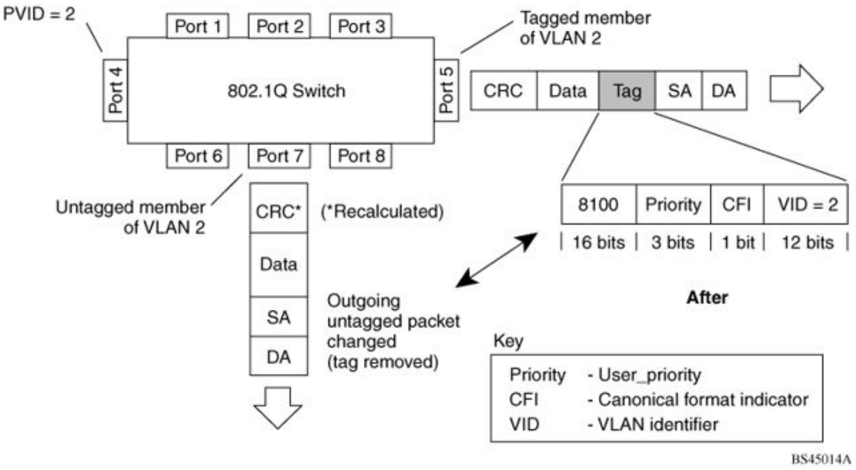


Figure 8: 802.1Q tagging (after 32-bit 802.1Q tag assignment)

In Figure 9: 802.1Q tag assignment on page 23, untagged incoming packets are assigned directly to VLAN 2. Port 5 is configured as a tagged member of VLAN 2, and port 7 is configured as an untagged member of VLAN 2.

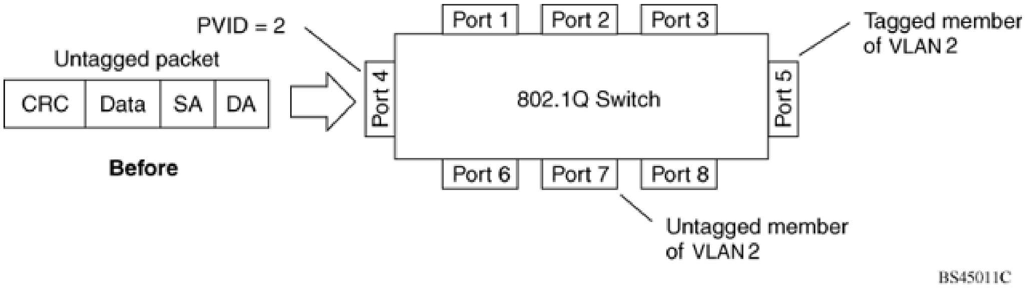


Figure 9: 802.1Q tag assignment

In Figure 10: 802.1Q tagging (after 32-bit 802.1Q tag assignment) on page 24, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.

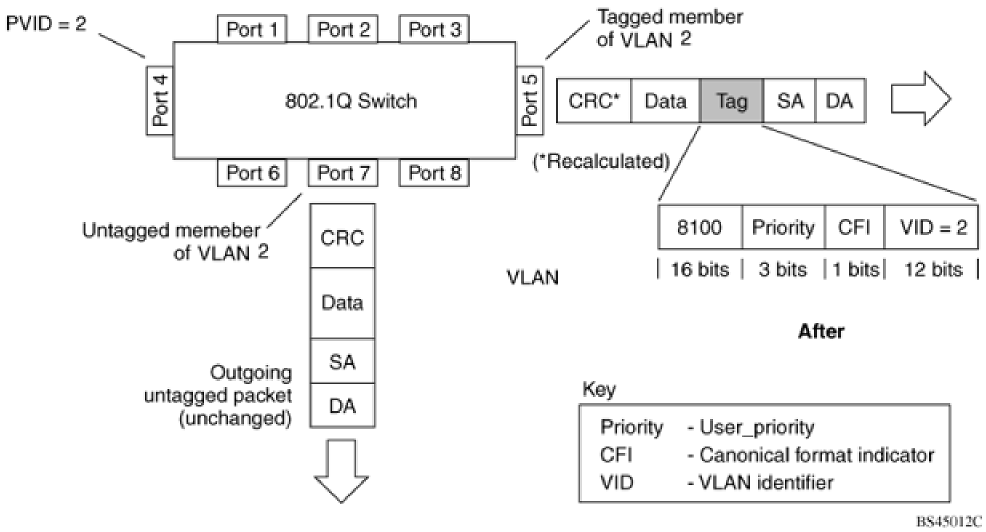


Figure 10: 802.1Q tagging (after 32-bit 802.1Q tag assignment)

VLANs spanning multiple switches

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

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

VLANs spanning multiple 802.1Q tagged switches

Figure 11: VLANs spanning multiple 802.1Q tagged switches on page 25 shows VLANs spanning two Avaya Ethernet Routing Switch 5000 Series switches. The 32-bit 802.1Q tagging is enabled on S1, port 14 and on S2, port 13 for VLAN 1 and VLAN 2. Both ports are tagged members of VLAN 1 and VLAN 2.

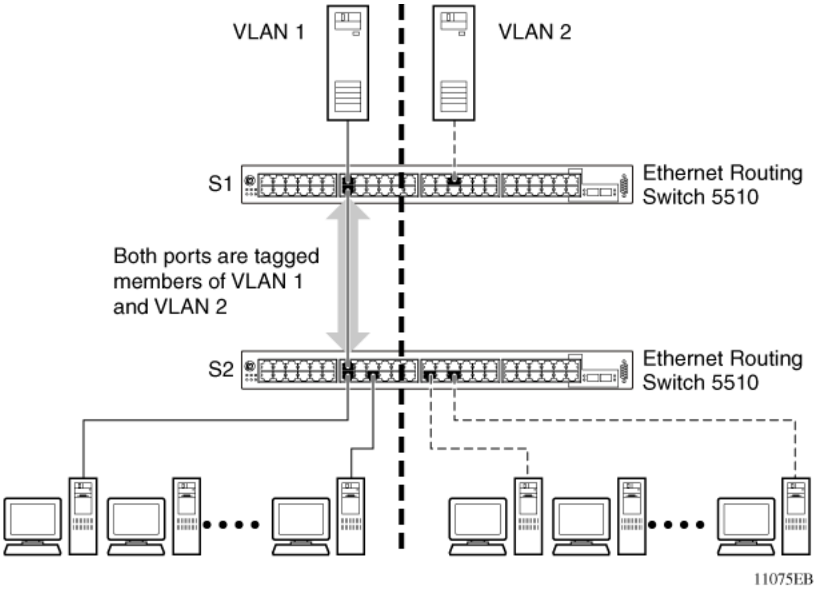

VLAN 1
VLAN 2
S1
Ethernet Routing Switch 5510
Both ports are tagged members of VLAN 1 and VLAN 2
S2
Ethernet Routing Switch 5510
11075EB

Figure 11: VLANs spanning multiple 802.1Q tagged switches

Because only one link exists between the two switches, the Spanning Tree Protocol (STP) treats this configuration as 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 26 shows VLANs spanning multiple untagged switches. In this configuration, Switch S2 does not support 32-bit 802.1Q tagging and you must use a single switch port on each switch for each VLAN.

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

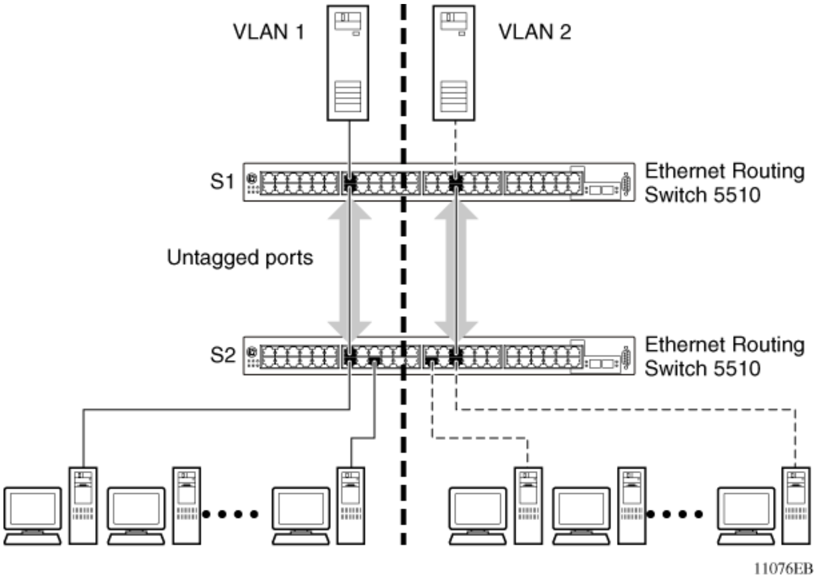


Figure 12: VLANs spanning multiple untagged switches

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

To connect multiple VLANs across switches with redundant links, you must disable the STP on all participating switch ports. Figure 13: Possible problems with VLANs and Spanning Tree Protocol on page 26 shows possible consequences of enabling the STP when using VLANs between untagged (non-802.1Q tagged) switches.

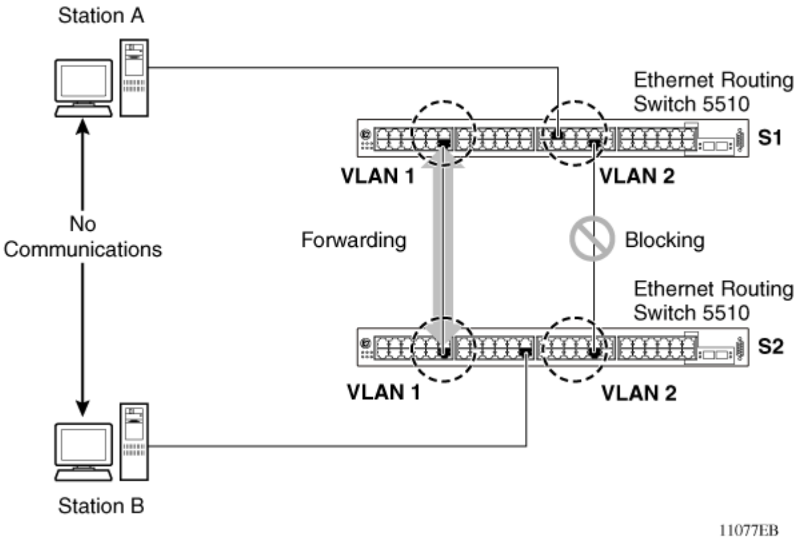


Figure 13: Possible problems with VLANs and Spanning Tree Protocol

As shown in Figure 13: Possible problems with VLANs and Spanning Tree Protocol on page 26, with STP enabled, only one connection between Switch S1 and Switch S2 is forwarding at any time. Communications failure occurs between VLAN 2 of S1 and VLAN 2 of S2, blocking communications between Stations A and B.

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

VLAN summary

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

As shown in Figure 14: VLAN configuration spanning multiple switches on page 28, Switch S1 (Avaya Ethernet Routing Switch 5510) is configured with multiple VLANs:

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

Because S4 does not support 32-bit 802.1Q tagging, a single switch port on each switch must be used for each VLAN (see Figure 12: VLANs spanning multiple untagged switches on page 26).

The connection to S2 requires only one link between the switches because S1 and S2 are both Avaya Ethernet Routing Switch 5000 Series switches that support 32-bit 802.1Q tagging (see VLANs spanning multiple 802.1Q tagged switches on page 24).

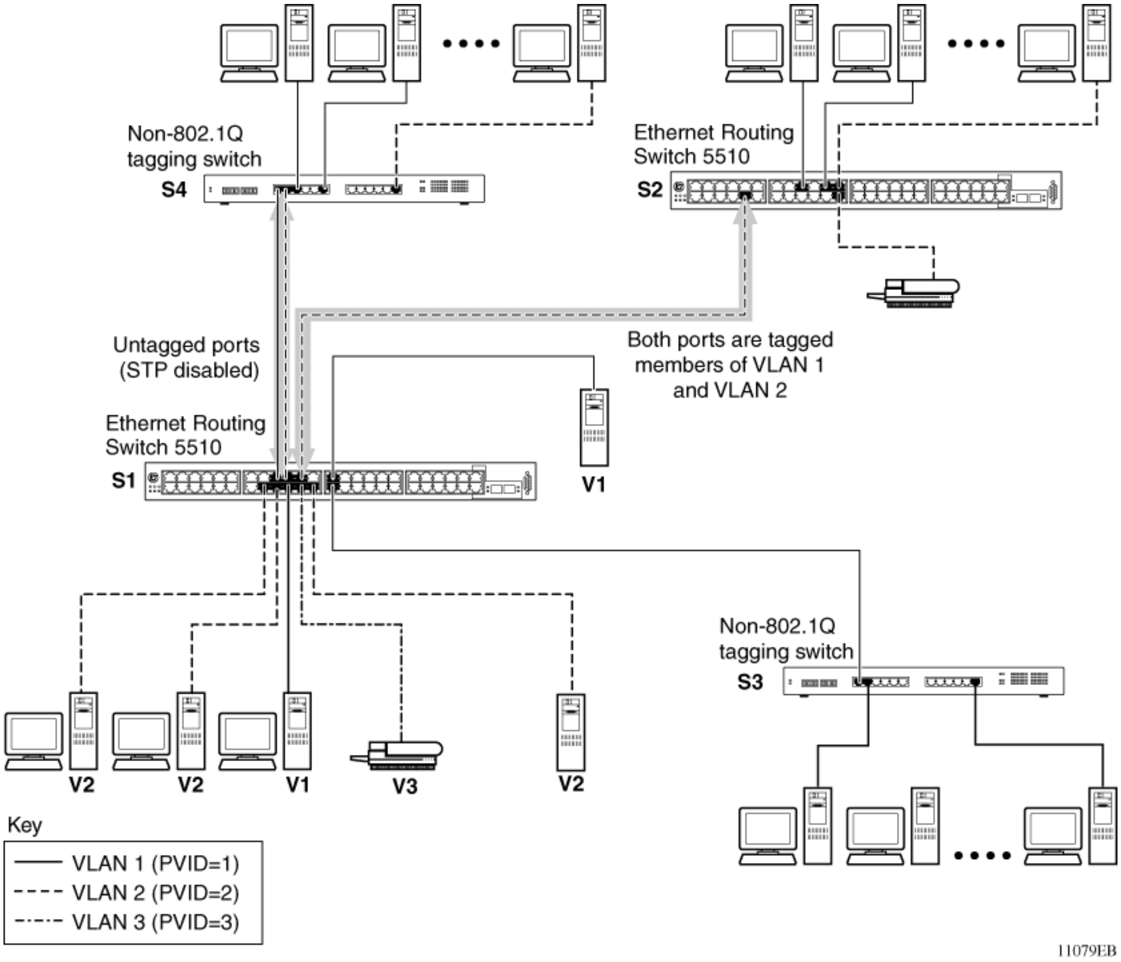


Figure 14: VLAN configuration spanning multiple switches

VLAN configuration rules

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

- If a port is a trunk group member, all trunk members are added or deleted from the VLAN.
- All ports involved in trunking must have the same VLAN configuration.
- VLANs are not dependent on Rate Limiting settings.
- If a port is an Internet Gateway Management Protocol (IGMP) member on any VLAN, and the port is removed from a VLAN, the port's IGMP membership is also removed.
- If you add a port to a different VLAN, and the port is already configured as a static router port, you configure the port as an IGMP member on that specific VLAN.

VCC

VLAN Configuration Control (VCC) allows a switch administrator to control how VLANs are modified. 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.

VCC offers four options for controlling VLAN modification:

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

   Note:

   Strict is the factory default setting.

2. **Automatic** -- This option automatically adds an untagged port to a new VLAN and automatically removes the port from any previous VLAN membership. The PVID of the port automatically changes to the VID of the VLAN it joins. Since the port is added to the new VLAN first, and then is removed from any previous membership, the Spanning Tree Group participation of the port can not be disabled if the VLANs involved are in the same Spanning Tree Group.
3. **AutoPVID** -- This option functions in the same manner as previous AutoPVID functionality. When an untagged port is added to a new VLAN, the port is added to the new VLAN and the PVID is assigned to the new VID without removing it from any previous VLAN memberships. Using this option an untagged port can have membership in multiple VLANs.
4. **Flexible** -- This option functions in a similar manner to disabling AutoPVID functionality. When this option is used, an untagged port can belong to an unlimited number of VLANs. Any new additions of an untagged port to a new VLAN does not change the PVID of that port.

VCCl is only applied to ports with the tagging modes of **Untag All** and **Tag PVID Only**. Ports with the tagging modes of **Tag All** and **Untag PVID Only** are not governed by VCC. Ports with the tagging modes of **Tag All** and **Untag PVID Only** can belong to multiple VLANs regardless of VCC settings and you must change the PVID manually.

Multinetting

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

MLT DMLT LAG dynamic VLAN changes

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

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

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

When you add a port to a new STG, consider using STG port membership in auto mode. In auto mode STP is automatically enabled on the port to prevent loops.

DHCP

Dynamic Host Configuration Protocol (DHCP) is defined by the RFC 2131. DHCP allows individual TCP/IP hosts on an IP network to obtain configuration information from a DHCP server (or servers). DHCP reduces the work of system administrators, especially in larger IP networks, by eliminating the need to manually set every IP address. The most significant pieces of information distributed through DHCP are:

- the IP address
- the network mask
- the IP address of the gateway

In many networks, DHCP must coexist with VLANs, and the DHCP client can make its broadcasts only in the trusted VLANs. The DHCP client runs at startup just like the BootP client. The DHCP client restricts its discovery broadcasts to the management VLAN.

The DHCP modes supported by the Avaya Ethernet Routing Switch 5000 Series are:

- DHCP or Last Address mode
- DHCP When Needed.
- DHCP Always
- DHCP Disabled. Disable DHCP by setting BootP Disabled.

The host cannot act as a DHCP relay while the DHCP client is running.

Voice VLAN Integration

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

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

When you manually create an LLPD MED network policy, LLDP checks that the specified VLAN ID corresponds to a voice VLAN created inside the VLAN application. If the VLAN is not a voice VLAN or the VLAN does not exist, the switch displays a warning message. The switch creates the policy even if the VLAN is not voice enabled or does not exist. The switch may display one of the following messages:

```
% Policy will be set on port x with vlan-id of a non-existent vlan y
```

```
% Policy will be set on port x member of the non-voice vlan y
```

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

Note:

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

You can configure up to 6 Voice VLANs.

Chapter 4: STP fundamentals

The following sections describe Spanning Tree Protocol (STP) fundamentals.

STP groups

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

The Avaya Ethernet Routing Switch 5000 Series supports multiple spanning tree groups (STG). The Avaya Ethernet Routing Switch 5000 Series supports a maximum of 8 STGs, either all in one stand-alone switch or across a stack. Multiple STGs provide multiple data paths, which can be used for load balancing and redundancy. You can enable load balancing between two switches using multiple STGs by configuring each path with a different VLAN and 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 Local Area Network (VLAN). The Avaya Ethernet Routing Switch 5000 Series supports multiple instances (8) of STGs running simultaneously.

The Avaya Ethernet Routing Switch 5000 Series supports a maximum of 1024 VLANs. With a maximum of 8 STGs, on average, each STG can have 128 VLANs.

In the default configuration of the Avaya Ethernet Routing Switch 5000 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 or delete ports from the default STG, you cannot delete the default STG (STG1) from the system. Also you cannot delete the default VLAN (VLAN1) from STG1.

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

Note:

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

You must create all other STGs, except the Default STG. To become active, you must enable each STG after creation. Each STG is assigned an ID number from 2 to 8 (the Default STG is assigned the ID number 1). Ports or VLANs are assigned to an active STG. However, a port that is not a member of a VLAN is not allowed to join an STG.

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

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

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

Note:

If you configure a unique multicast address for an STG, you must also configure each device in the STG with the same spanning tree multicast address.

Note:

If Virtual LACP is enabled, the number of unique multicast addresses you can configure for STGs is reduced to 3 (1 to 3).

STG configuration guidelines

This section provides important information about configuring STGs:

- You must create an STG by following 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, you must assign it to another STG.
- You can move a newly created VLAN to an existing STG by following these steps:
  - Create the VLAN
  - Add the VLAN to an existing STG
- VLAN1 cannot be moved or deleted from STG1.
- You can create and add VLAN X directly to STG Y with **`vlan create X type port Y`** from ACLI if STG Y exists.
- VLANs must be contained within a single STG; a VLAN cannot span multiple STGs. By confining VLANs within a single STG, you avoid problems with spanning tree blocking ports and causing a loss of connectivity within the VLAN. When a VLAN spans multiple switches, the VLAN must be within the same spanning tree group (have the same STG ID) across all the switches.

- A port that is not a member of any VLAN cannot be added to any STG. You can add the port 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
- A VLAN ID can be selected for tagged BPDUs for each STG. Valid VLAN IDs are 1 to 4094.
- Tagged BPDUs cannot use the same VID as an active VLAN.
- An untagged port cannot span multiple STGs.
- When 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 cannot delete an STG until you disable 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 Avaya Ethernet Routing Switch 5000 Series. If Spanning Tree Fast Learning is enabled on a port with no other bridges, the port is brought up quicker after a switch initialization or a spanning tree change. The port goes through the normal blocking and learning states before the forwarding state, but the hold times for these states is the bridge hello timer (2 seconds by default) instead of the bridge forward delay timer (15 seconds by default).

The port 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.

Note:

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

STG port membership mode

IEEE 802.1D STGs support two different STP port membership modes: normal and auto. In the normal mode, when 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 the auto 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.

To set the STG port membership mode using the ACLI, see Configuring STG port membership mode on page 161 and using EDM, see Configuring STG Global properties on page 279.

802.1t path cost calculation

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

To set the path cost calculation mode for the switch, see Configuring path cost calculation mode on page 160.

RSTP

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

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

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

MSTP

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

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

- Reduction of converging time from 30 seconds to less than 1 or 2 seconds when a topology change occurs in the network (ports going up or down).
- Elimination of unnecessary flushing of the MAC database and flooding of traffic to the network with a new Topology Change mechanism.
- Backward compatibility with other switches running legacy 802.1d STP or Avaya MSTP (STP group 1 only).
- Under MSTP mode, simultaneous support of eight instances of RSTP. Instance 0 or CIST is the default group, which includes default VLAN 1. Instances 1 to 7 are called MSTIs 1-7.
- Ability to run Avaya MSTP, RSTP, or MSTP.

Interoperability with legacy STP

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

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

Differences in STP and RSTP port roles

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

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

Table 1: Differences in port roles for STP and RSTP

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

Edge port

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

Path cost values

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

Table 2: Recommended path cost values

Link speed	Recommended value

Less than or equal to 100 Kbit/s
1 Mbit/s
10 Mbit/s
100 Mbit/s
	200 000 000
	20 000 000
	2 000 000
	200 000

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

1 Tbit/s 10 Tbit/s	20 2

Rapid convergent

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

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

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

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

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

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

Switch A is the Root.

Negotiation Process

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

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

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

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

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

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

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

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

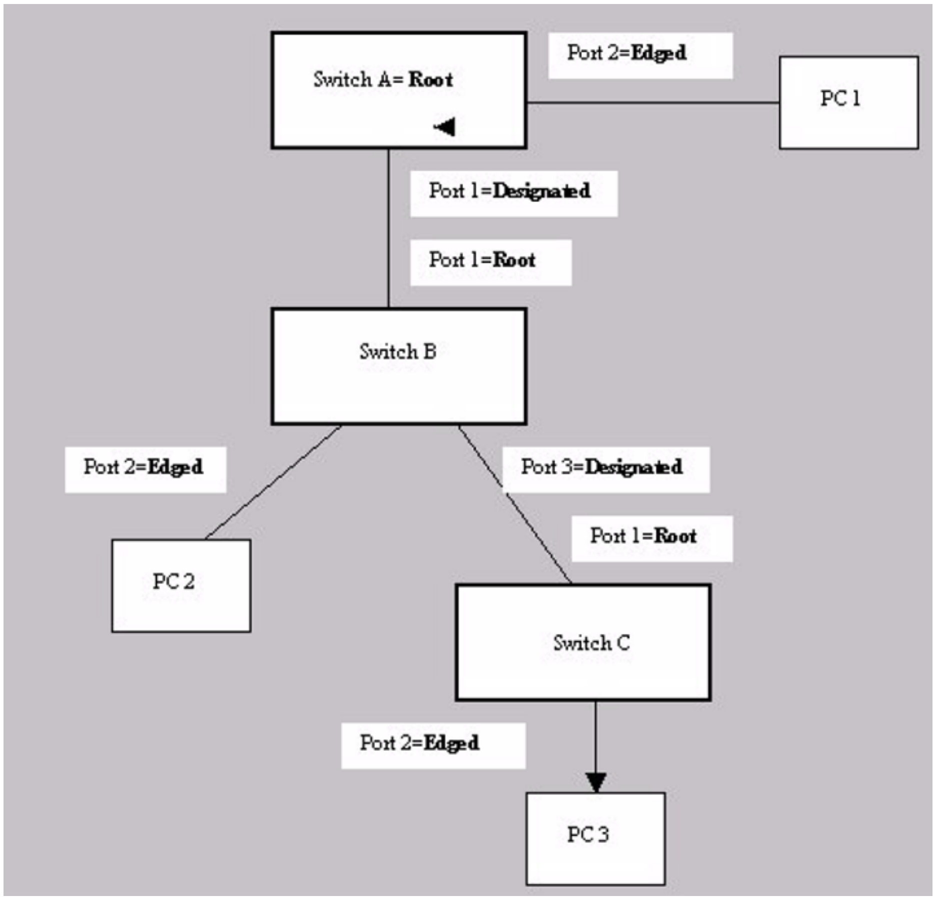


Figure 15: Negotiation process

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

Spanning Tree BPDU Filtering

The Ethernet Routing Switch 5000 Series supports the Bridge Protocol Data Unit (BPDU) Filtering feature for STPG, RSTP, and MSTP.

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

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

The BPDU Filtering feature allows you to achieve the following:

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

Note:

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

When a port with BPDU Filtering enabled receives an STP BPDU, the following actions occur:

- The port immediately enters 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 remains in the operational disabled state until the port timer expires.

If you disable the timer, or the switch resets before the timer expires, the port remains in the disabled state. Similarly, if BPDU-Filtering is disabled while the timer is running, the timer stops and that port remains in the disabled state. In this case, you must manually enable the port to restore the port to the normal mode.

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

For details on configuring BPDU Filtering, see: Configuring STP BPDU Filtering using the ACLI on page 159.

Configuring Spanning Tree using the Console Interface

The following sections provide instructions for configuring Spanning Tree in the three modes using the Console Interface main menu.

Spanning Tree configuration in STPG mode

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

To open the Spanning Tree Configuration Menu screen from the Main Menu:

→ Choose **Spanning Tree Configuration** (or press **p**).

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

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

Option	Description
Spanning Tree Group Configuration	Displays the Spanning Tree Group Configuration screen. (See Spanning Tree Group Configuration in STPG mode on page 42.)
Spanning Tree Port Configuration	Displays the Spanning Tree Port Configuration screen. (See Spanning Tree Port Configuration in STPG mode on page 45.)
Display Spanning Tree Switch Settings	Displays the Spanning Tree Switch Settings screen. (See Spanning Tree Switch Settings in STPG mode on page 47.)
Display Spanning Tree VLAN Membership	Displays the Spanning Tree VLAN Membership screen.

Spanning Tree Group Configuration in STPG mode

To open the Spanning Tree Group Configuration:

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

Table 4: Spanning Tree Group Configuration parameters in STPG mode

Parameter	Description	
STP Mode	Shows the current STP operational mode for switch/stack. The modes available are: • STPG (Avaya MSTP) • RSTP (IEEE 802.1w) • MSTP (IEEE 802.1s)	
Create STP Group	Creates a spanning tree group.	
	Default value	1
	Range	1 to 8
Delete STP Group	Deletes a spanning tree group.	
	Default value	Blank
	Range	Configured STP groups from 1 to 8
Bridge Priority (in Hex)	Configures the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values.	
	Default value	0x8000
	Range	0x0000 to 0xF000
Bridge Hello Time	Configures the Hello Interval (the amount of time between transmissions of BPDUs) for the STP Group. This parameter takes effect only when this bridge becomes the root bridge. **Note:** Although you can set the Hello Interval for a bridge using bridge management software, after the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network.	
	Default value	2 seconds
	Range	1 to 10 seconds

Parameter	Description	
Bridge Max. Age Time	Configures the maximum age (in seconds) that a Hello message can attain before being discarded. This parameter takes effect only when the bridge becomes the root bridge. **Note:** If this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network.	
	Default value	20 seconds
	Range	6 to 40 seconds
Bridge Forward Delay Time	Configures the Forward Delay parameter value for this bridge. This parameter takes effect only when this bridge becomes the root bridge. The Forward Delay parameter value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. **Note:** All bridges participating in the spanning tree network use the root bridge Forward Delay parameter value.	
	Default value	15 seconds
	Range	4 to 30 seconds
Add VLAN Membership	Adds a VLAN to the specified spanning tree group.	
	Default value	1
	Range	1 to 4094.
Delete VLAN Membership	Deletes a VLAN from the specified spanning tree group.	
	Default value	Blank
	Range	Configured VLANs from 1 to 4094
Tagged BPDU on tagged port	Specifies whether to send tagged or untagged BPDUs from a tagged port.	
	Default value	STP Group 1: No; Other STP Groups: Yes
	Range	No or Yes
VID used for tagged BPDU	Specifies the VLAN ID (VID) for tagged BPDU for the specified spanning tree group.	
	Default value	4001 to 4008 for STGs 1 through 8, respectively

Parameter	Description	
	Range	1 to 4094
STP Multicast Address	Specifies the STP Multicast Address.	
	Default value	01-80-C2-00-00-00
STP Group State	Sets the STP Group to active or inactive. **Note**: You cannot set the default STG (STG 1) to Inactive.	
	Default value	Active for STG 1; Inactive for STGs 2 to 8
	Range	Active or Inactive

Spanning Tree Port Configuration in STPG mode

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

Note:

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

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

Table 5: Spanning Tree Port Configuration parameters in STPG mode

Field	Description	
STP Group	Specifies the number of the spanning tree group (STG) to view. To view another STG, type that STG ID number and press Enter, or press the spacebar on your keyboard to toggle the STP Group numbers.	
	Default value	1
	Range	Configured STP Groups from 1 to 8
STP Mode	Indicates the STP mode in which the switch or stack is operating.	
Unit	This field only appears if the switch is participating in a stack configuration. The field specifies the number of the unit to view. To view another unit, type its unit number and press Enter, or press the spacebar on your keyboard to toggle the unit numbers.	
Port	Indicates the switch port numbers that correspond to the field values in that row (for example, the field values in row 2 apply to switch port 2).	

Field	Description	
	Note: The values in the Switch row affect all switch ports and, when the switch is part of a stack, the values in the Stack row affect all ports in the entire stack.	
Trunk	The read-only data displayed in this column indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen.	
Participation	Configures any (or all) of ports on the switch for Spanning tree participation. When an individual port is a trunk member, changing this setting for one trunk member changes the setting for all members of that trunk. Consider how this can change your network topology before you change this setting. The Fast Learning parameter is the same as Normal Learning, except that the state transition timer is shortened to 2 seconds.	
	Default value	Normal Learning
	Range	Normal Learning, Fast Learning, Disabled
Priority	This read-only field is a bridge spanning tree parameter that prioritizes the lowest port path cost to the root. When one or more ports have the same path cost, STP selects the path with the highest priority (lowest numerical value).	
	Default value	128
	Range	0 to 255
Path Cost	This read-only field is a bridge spanning tree parameter that determines the lowest path cost to the root.	
	Default value	in 802.1d mode: • Path cost = 1000 / LAN speed in Mbyte/s • 1 for 1 Gigabit port in 802.1t mode: • Path cost = 2*10^10 / LAN speed in Kbyte/s • 20 000 for 1 Gigabit port (default on ERS5000) . The higher the LAN speed, the lower the path cost.

Field	Description	
	Range	in 802.1d mode: 1 to 65535 in 802.1t mode: 1 to 200 000 000
State	This read-only field indicates the current port state within the spanning tree network. Each port can transition to various states, as determined by the Participation field setting. For example, when the Participation field is set to Disabled, the port does not participate in the spanning tree and transitions to the Forwarding state (the default). When the Participation field is set to Enabled, the port transitions from the Disabled state through the Blocking, Listening, and Learning states before entering the Forwarding state.	
	Default value	Topology dependent
	Range	Disabled, Blocking, Listening, Learning, Forwarding

Spanning Tree Switch Settings in STPG mode

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

To open the Spanning Tree Switch Settings:

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

Table 6: Spanning Tree Switch Settings parameters in STPG mode

Parameter	Description	
STP Group	Specifies the number of the spanning tree group (STG) to view. To view another STG, type that STG ID number and press Enter, or press the spacebar on your keyboard to toggle the STP Group numbers.	
	Default value	1
	Range	Configured STP Groups from 1 to 8
STP Mode	Shows the current STP operational mode for switch/stack: • Avaya MSTP (STPG) • IEEE 802.1w (RSTP) • IEEE 802.1s (MSTP)	
Bridge Priority	Indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most	

Parameter	Description	
	significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values compared first, followed by the hardware addresses.	
	Default value	0x8000
	Range	HEX: 0x0000 - 0xF000
Designated Root	Indicates the bridge ID of the root bridge, as determined by spanning tree.	
Root Port	Indicates the switch port number that offers the lowest path cost to the root bridge.	
Root Path Cost	Indicates the path cost from this switch port to the root bridge.	
	Default value	0
	Range	Unit 1-8 Port 1-50 (in stack mode) Port 1-50 (in standalone mode)
Hello Time	Defines the amount of time between transmissions of BPDUs.	
	Range	1 to 10 seconds
Maximum Age Time	Indicates the Maximum Age Time parameter value that the root bridge is currently using. This value specifies the maximum age that a Hello message can attain before being discarded. **Note:** The root bridge Maximum Age Time parameter value becomes the actual Maximum Age Time parameter value for all bridges participating in the spanning tree network.	
	Default value	20 seconds
	Range	6 to 40 seconds
Forward Delay	Indicates the Forward Delay parameter value that the root bridge is currently using. This value specifies the amount of time that the bridge ports remain in each of the Listening and Learning states before entering the Forwarding state.	

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

Spanning Tree VLAN Membership in STPG mode

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

To open the Spanning Tree VLAN Membership:

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

Table 7: Spanning Tree VLAN Membership parameters

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

Spanning Tree configuration in RSTP mode

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

To open the Spanning Tree Configuration Menu:

Choose **Spanning Tree Configuration** (or press p) from the Main Menu.

Table 8: Spanning Tree Configuration main menu options

Menu option	Description
Spanning Tree Group Configuration	Displays the Spanning Tree Group Configuration screen. (See Spanning Tree Group Configuration in RSTP mode on page 50.)
Spanning Tree Port Configuration	Displays the Spanning Tree Port Configuration screen. (See Spanning Tree Port Configuration in RSTP mode on page 52.)
Display Spanning Tree Switch Settings	Displays the Spanning Tree Switch Settings screen. (See Spanning Tree Switch Settings in RSTP mode on page 53.)

Spanning Tree Group Configuration in RSTP mode

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

To open the Spanning Tree Group Configuration:

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

Table 9: Spanning Tree Group Configuration parameters in RSTP mode

Parameter	Description	
STP Mode	Shows the current STP operational mode for switch/stack: • Avaya MSTP (STPG) • IEEE 802.1w (RSTP) • IEEE 802.1s (MSTP)	
Bridge Priority (in Hex)	For the STP Group, configures the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values.	
	Default value	0x8000
	Range	0x0000 to 0xF000
Bridge Hello Time	For the STP Group, configures the Hello Interval (the amount of time between transmissions of BPDUs). This parameter takes effect only when this bridge becomes the root bridge. Although you can set the Hello Interval for a bridge using bridge management software, after the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network.	
	Default value	2 seconds
	Range	1 to 10 seconds
Bridge Max. Age Time	For the STP Group, configures the maximum age (in seconds) that a Hello message can attain before being discarded. This parameter takes effect only when the bridge becomes the root bridge. If this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network.	
	Default value	20 seconds
	Range	6 to 40 seconds

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

Spanning Tree Port Configuration in RSTP mode

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

Note:

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

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

Table 10: Spanning Tree Port Configuration parameters in RSTP mode

Field	Description
Unit	This field appears only if the switch is participating in a stack configuration. The field specifies the number of the unit to view. To view another unit, type its unit number and press Enter, or press the spacebar on your keyboard to toggle the unit numbers.

Field	Description	
Port	Indicates the switch port numbers that correspond to the field values in that row (for example, the field values in row 2 apply to switch port 2). The values in the Switch row affect all switch ports, and when the switch is part of a stack, the values in the Stack row affect all ports in the entire stack.	
Trunk	The read-only data displayed in this column indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen.	
Learning	Indicates the port states of Spanning Tree.	
	Range	Enabled, Disabled
Edge	Indicates if a port is an Edge port. When a port is connected to a non-switch device such as a PC or a workstation, configure it as an Edge port. An active Edge port goes directly to Forwarding state without any delay.	
Priority	This read-only field is a bridge spanning tree parameter that prioritizes the lowest port path cost to the root. When one or more ports have the same path cost, STP selects the path with the highest priority (lowest numerical value).	
	Default value	128
	Range	0 to 255
Path Cost	This read-only field is a bridge spanning tree parameter that determines the lowest path cost to the root.	
	Default value	20000 for 1 Gigabit port Path cost = 2*10^10/LAN speed (in Kbits/s) The higher the LAN speed, the lower the path cost.
	Range	1 to 200 000 000
Role	A role represents a functionality characteristic or capability of a resource to which policies are applied. The role of a port can be Root, Designated, Alternate, or Backup.	
State	Indicates the current state of the Port as defined by the Rapid Spanning Tree Protocol. The state of a Port can be Forwarding in one instance and Discarding (Blocking) in another.	

Spanning Tree Switch Settings in RSTP mode

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

To open the Spanning Tree Switch Settings:

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

Table 11: Spanning Tree Switch Settings parameters in RSTP mode

Field	Description	
STP Mode	Indicates the mode of the STP operation for the switch. The possible values for the STP mode are: • STPG (Avaya MSTP) • RSTP (IEEE 802.1w) • MSTP (IEEE 802.1s)	
Bridge Priority	Indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values compared first, followed by the hardware addresses.	
	Default value	0x8000
	Range	HEX: 0x0000 - 0xF000
Designated Root	This field specifies the unique Bridge Identifier of the bridge. It is recorded as the CIST Root in the configuration BPDUs that are transmitted.	
Root Port	Indicates the switch port number that offers the lowest path cost to the root bridge. The local switch is the root bridge when this value is 0 (path cost).	
	Default value	0
	Range	Unit: 1-8, Port 1-50 (in stack mode) Port: 1-98 (in standalone mode)
Root Path Cost	Indicates the path cost from this switch port to the root bridge.	
	Default value	0
	Range	Not applicable
Hello Time	Defines the amount of time between transmissions of BPDUs.	
	Range	1 to 10 seconds

Field	Description	
Maximum Age Time	Indicates the Maximum Age Time parameter value that the root bridge is currently using. This value specifies the maximum age that a Hello message can attain before being discarded. The root bridge Maximum Age Time parameter value becomes the actual Maximum Age Time parameter value for all bridges participating in the spanning tree network.	
	Default value	20 seconds
	Range	6 to 40 seconds
Forward Delay	Indicates the Forward Delay parameter value that the root bridge is currently using. This value specifies the amount of time that the bridge ports remain in each of the Discarding and Learning states before entering the Forwarding state. The root bridge Forward Delay parameter value becomes the actual Forward Delay parameter value for all bridges participating in the spanning tree network.	
	Default value	15 seconds
	Range	4 to 30 seconds
Bridge Hello Time	For the STP Group, configures the Hello Interval. This parameter takes effect only when this bridge becomes the root bridge. Although you can set the Hello Interval for a bridge using the bridge management software, after the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network.	
	Default value	2 seconds
	Range	1 to 10 seconds
Bridge Maximum Age Time	Specifies the maximum age (in seconds) that a Hello message can attain before being discarded. This parameter, specified by management for this bridge, takes effect only when the bridge becomes the root bridge. If this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network.	
	Default value	20 seconds
	Range	6 to 40 seconds

Field	Description	
Bridge Forward Delay	Indicates the Forward Delay parameter value specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. The Forward Delay parameter value specifies the amount of time that the bridge ports remain in each of the Discarding and Learning states before entering the Forwarding state. All bridges participating in the spanning tree network use the root bridge Forward Delay parameter value.	
	Default value	15 seconds
	Range	4 to 30 seconds
Tx Hold Count	This is the value used by the Port Transmit state machine to limit the maximum transmission rate. The value can range from 1 to 10	
Default Path Cost Type	Indicates the way that path cost is represented and used.	

Spanning Tree configuration in MSTP mode

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

To open the Spanning Tree Configuration Menu:

Choose **Spanning Tree Configuration** (or press p) from the Main Menu.

Table 12: Spanning Tree Configuration Menu options in MSTP mode

Option	Description
Spanning Tree Group Configuration	Displays the Spanning Tree Group Configuration screen.
Spanning Tree Port Configuration	Displays the Spanning Tree Port Configuration screen.
Display Spanning Tree Switch Settings	Displays the Spanning Tree Switch Settings screen.
Display Spanning Tree VLAN Membership	Displays the Spanning Tree VLAN Membership screen.

Spanning Tree Group Configuration in MSTP mode

With the Spanning Tree Group Configuration, you can create and configure Spanning Tree Groups (STGs).

To open the Spanning Tree Group Configuration:

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

Table 13: Spanning Tree Group Configuration parameters in MSTP mode

Parameter	Description	
STP mode	Indicates the STP mode in which the switch is operating. The available modes are: • STPG (Avaya MSTP) • RSTP (IEEE 802.1w) • MSTP (IEEE 802.1s)	
Create STP Group	Creates a spanning Tree group. You can also use this parameter to select the STP Group information to display.	
	Default value	CIST
	Range	1 to 7 (MSTIs)
Delete STP Group	Deletes a spanning tree group. You cannot delete the CIST STP Group, and you can delete only nonactive STP Groups (that is, MSTIs).	
	Default Value	Blank
	Range	1 to 8; only created STP Groups are available
Bridge Priority	For the STP Group, configures the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values.	
	Default value	0x8000
	Range	0x0000 -0xF000
Bridge Max. Age Time	For the STP Group, configures the maximum age (in seconds) that a Hello message can attain before being discarded. This parameter takes effect only when the bridge becomes the root bridge. If this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network.	
	Default value	20 seconds
	Range	6 to 40 seconds

Parameter	Description	
Bridge Forward Delay Time	For the STP Group, configures the Forward Delay parameter value for this bridge. This parameter takes effect only when this bridge becomes the root bridge. The Forward Delay parameter value specifies the amount of time that the bridge ports remain in each of the Discarding and Learning states before entering the Forwarding state. All bridges participating in the spanning tree network use the root bridge Forward Delay parameter value.	
	Default value	15 seconds
	Range	4 to 30 seconds
Bridge Tx Hold Count	Indicates the number of BPDUs that are sent in each Hello Time interval. The value used by the Port Transmit state machine to limit the maximum transmission rate.	
	Default value	3
	Range	1 to 10
Max. Hop Count	The Maximum Hop Count value in 1/100 seconds. The specified value must be a multiple of 100.	
	Default value	2000
	Range	600 to 4000, measured in 1/100 second
Default Path Cost Type	The version of the Spanning Tree default Path Costs that are used by this Bridge. A value of 16 Bits specifies the 16-bit default path costs from IEEE Standard 802.1D-1998. A value of 32 Bits specifies the 32-bit default path costs from IEEE Standard 802.1t.	
	Default value	32 Bits
	Range	16 Bits, 32 Bits
Add VLAN Membership	Adds a VLAN to the specified spanning tree group. **Note:** This field is updated with active VLANs currently defined in the system. A newly created and active VLAN is assigned to STP Group 1 by default.	
	Default value	1
	Range	1 to 4094
Delete VLAN Membership	Deletes a VLAN from the specified STP group. **Note:** You cannot remove VLAN 1 from STP Group 1.	
	Default value	Blank

Parameter	Description	
	Range	1 to 4094; but only configured ones are available
STP Group State	Specifies whether the MSTI is active or inactive. **Note:** You cannot set the default STG (CIST) to inactive. To enable an STP Group, at least one active VLAN must be assigned to that STP Group (MSTI).	
	Default value	Active for CIST; Inactive for MSTIs 1 to 7.
	Range	Active or Inactive

Spanning Tree Port Configuration in MSTP mode

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

Note:

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

To open the Spanning Tree Port Configuration:

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

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

Field	Description
STP Group	Specifies the MSTP instance for which to display the port properties. Press the spacebar to toggle between the CIST and the configured MSTI instances.
Port	Indicates the switch port numbers that correspond to the field values in that row (for example, the field values in row 2 apply to switch port 2). The values in the Switch row affect all switch ports, and when the switch is part of a stack, the values in the Stack row affect all ports in the entire stack.
Trunk	The read-only data displayed in this column indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen.
Learning	Configures any (or all) of the switch ports for Spanning tree participation.

Field	Description	
	When an individual port is a trunk member (see Trunk field), changing this setting for one of the trunk members changes the setting for all members of that trunk. Consider how this will change your network topology before you change this setting.	
	Default value	Enabled
Edge	A value of Yes indicates that this port is to be assumed as an edge-port and a value of No indicates that this port is to be assumed as a non-edge port.	
	Default value	No
	Range	No, Yes
Priority	This read-only field is a bridge spanning tree parameter that prioritizes the lowest port path cost to the root. When one or more ports have the same path cost, STP selects the path with the highest priority (lowest numerical value).	
	Default value	128
	Range	0 to 255
Path Cost	This read-only field is a bridge spanning tree parameter that determines the lowest path cost to the root.	
	Default value	Default value is 20000 for 1 Gigabit port Path Cost = 2*10^10/LAN speed (in Kbit/s) The higher the LAN speed, the lower the path cost.
	Range	1 to 200 000 000
Role	The current role of the port as defined by Multiple Spanning Tree Protocol.	
	Default	Disabled
	Range	Disabled, Root, Designated, Alternate, Backup
State	This read-only field indicates the current port state within the spanning tree network. Each port can transition to various states, as determined by the Participation field setting. For example, when the Participation field is set to Disabled, the port does not participate in the spanning tree and transitions to the Forwarding state (the default). When the Participation field is set to Enabled, the port transitions from the Disabled state through the Blocking, Listening, and Learning states before entering the Forwarding state.	
	Default value	Topology dependent
	Range	Discarding, Learning, Forwarding

Spanning Tree Switch Settings in MSTP mode

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

To open the Spanning Tree Switch Settings:

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

Table 15: Spanning Tree Switch Settings parameters in MSTP mode

Parameter	Description	
STP Group	Specifies the MSTP instance for which to display the properties. Press the spacebar to toggle between the CIST and the configured MSTI instances.	
Bridge Priority	Indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values compared first, followed by the hardware addresses.	
	Default value	8000
	Range	0x0000 - 0xF000
CIST Root	Common and Internal Spanning Tree (CIST) Root field shows the CIST External or Internal Root elected between devices. CIST Internal Root is used only on devices from the same region. CIST External (Common Spanning Tree) Root is elected between devices from different regions or between devices with different STP modes. This parameter displays these values depending on network configuration.	
Regional Root	Shows the CIST Regional Root bridge elected between devices from the same region (in other words, the root for the Region).	
Root Port	Indicates the switch port number that offers the lowest path cost to the root bridge. The local switch is the root bridge when this value is 0 (path cost).	
	Range	Unit: 1-8, Port 1-50 (in stack mode) Port: 1-50 (in standalone mode)
Root Path Cost	Indicates the path cost from this switch port to the root bridge.	

Parameter	Description	
	Default value	0
	Range	Not applicable
Regional Root Path Cost	Indicates the Path Cost to CIST Regional Root seen from this device.	
Maximum Age Time	Indicates the Maximum Age Time parameter value that the root bridge is currently using. This value specifies the maximum age that a Hello message can attain before being discarded. The root bridge Maximum Age Time parameter value becomes the actual Maximum Age Time parameter value for all bridges participating in the spanning tree network.	
	Default value	20 seconds
	Range	6 to 40 seconds
Forward Delay	Indicates the Forward Delay parameter value that the root bridge is currently using. This value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. The root bridge Forward Delay parameter value becomes the actual Forward Delay parameter value for all bridges participating in the spanning tree network.	
	Default value	15 seconds
	Range	4 to 30 seconds
Bridge Hold Time	This value determines the time interval during which no more than two configuration BPDUs can be transmitted by this node.	
	Default value	1 second
Bridge Maximum Age Time	Specifies the maximum age (in seconds) that a Hello message can attain before being discarded. This parameter, specified by management for this bridge, takes effect only when the bridge becomes the root bridge. If this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network.	
	Default value	20 seconds
	Range	6 to 40 seconds
Bridge Forward Delay	Indicates the Forward Delay parameter value specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge.	

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

Spanning Tree VLAN Membership in MSTP mode

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

To open the Spanning Tree VLAN Membership:

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

Table 16: Spanning Tree VLAN Membership parameters

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

Chapter 5: MLT fundamentals

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

MLT

With Multi-Link trunks (MLTs), you can group up to eight switch ports together to form a link to another switch or server, thus increasing aggregate throughput of the interconnection between the devices (up to 8 Gigabits in full-duplex mode). Up to 32 MLTs can be configured. The trunk members can reside on a single unit or on multiple units within the same stack configuration as a distributed trunk. MLT 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 Avaya Command Line Interface (ACLI) or Enterprise Device Manager (EDM) to create switch-to-switch and switch-to-server MLT links.

Client-server configuration using MLT

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

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

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

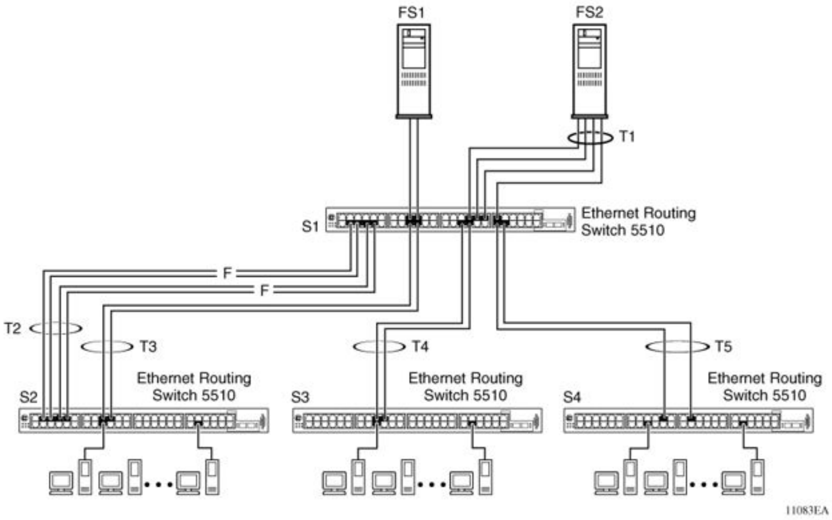

FS1
FS2
T1
S1
Ethernet Routing Switch 5510
F
F
T2
T3
T4
T5
S2
S3
S4
Ethernet Routing Switch 5510
Ethernet Routing Switch 5510
Ethernet Routing Switch 5510
11083EA

Figure 16: Client/server configuration example

Before configuring trunks

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

Before configuring a MLT, consider these settings, along with specific configuration rules, as follows:

1. Read the configuration rules provided in the next section, MLT configuration rules on page 67.
2. Determine which switch ports (up to eight) are to become trunk members (the specific ports making up the trunk). A minimum of two ports are required for each trunk.

   Note:

   Disabled ports can belong to MLTs. For traffic to flow to your configured MLT ports, be sure they are enabled.
3. Ensure that the trunk member ports have the same VLAN configuration.
4. To avoid configuration errors, all network cabling must be complete and stable before configuring any trunks.

   Note:

   If trunk ports are STP enabled, ensure that all potential trunk members are connected to their corresponding members and the same STP group learning mode is configured on both ends of the trunk; otherwise, STP cannot converge correctly, and traffic loss can result.

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

   Note:

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

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

MLT configuration rules

The Multi-Link Trunking feature operates according to specific configuration rules. When you create trunks, consider the following rules that determine how the MLT reacts in any network topology:

- Disabled ports can belong to MLTs. For traffic to flow to your configured MLT ports, they must be enabled (configure to enabled using ACLI or EDM port configuration).
- If the spanning tree participation of any trunk member is changed to Enabled or Disabled, the spanning tree participation of all members of that trunk changes similarly.
- If the VLAN settings of any trunk member is changed, the VLAN settings of all members of that trunk change similarly.
- A trunk member cannot be configured as a monitor port.
- Entire trunks cannot be monitored by a monitor port; however, trunk members can be monitored.
- All trunk members must have identical Internet Gateway Management Protocol (IGMP) configurations.
- If you change the IGMP snooping configuration for any trunk member, the IGMP snooping settings for all trunk members change.
- Avaya recommends that you do not enable MAC Address Security on trunk ports.
- MLT ports can be set to participate in different STGs. They must have the same spanning tree learning in every group but not necessarily have the same learning between different groups to consistently update their state in the port driver.
- Like normal ports, MLT ports can be set to participate with different spanning tree learning for different spanning tree groups. Trunk ports that are in multiple spanning tree groups must be tagged, and all MLT members must belong to the same spanning tree groups.
- You can disable the lowest numbered port in the trunk. Avaya does not recommend disabling the lowest numbered port if Spanning Tree is enabled on the trunk.

MLT load-balancing

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

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

{(A XOR B) MOD x}

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

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

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

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

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

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

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

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

Note:

Avaya recommends that you configure the same MLT load-balance mode at both ends of the trunk. Configuring different modes may result in traffic loss.

Port management for existing MLTs

When MLT is disabled, the ports assigned to the MLT are not disabled if trunk loop prevention is disabled. If trunk loop prevention is enabled then all ports except the first port from the MLT are disabled.

How a MLT reacts to losing distributed trunk members

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

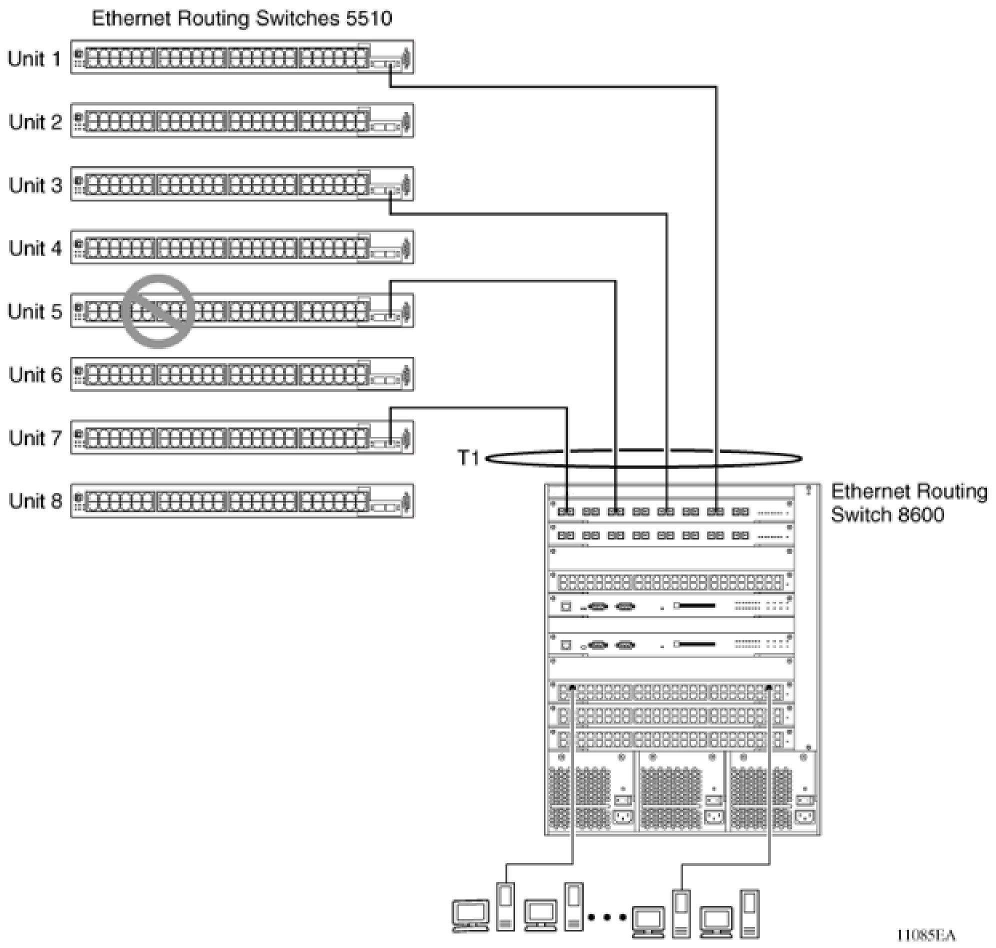


Figure 17: Loss of distributed trunk member

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

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

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

Spanning Tree Considerations for MLTs

The spanning tree Path Cost parameter is recalculated based on the aggregate bandwidth of the trunk. For example, Figure 18: Path Cost Arbitration on page 71 shows a two-port trunk

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

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

Note:

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

When configuring trunks, be careful to not add one gigabit link physically in front of another trunk; the trunk is blocked because they both have a Path Cost of 1. You can also change the STP priority of the port to avoid blocking of the trunk, though another gigabit port is physically connected in front of the trunk.

Alternatively, spanning-tree 802.1t calculation mode can be used. This mode assures a better cost for trunk in the situation described.

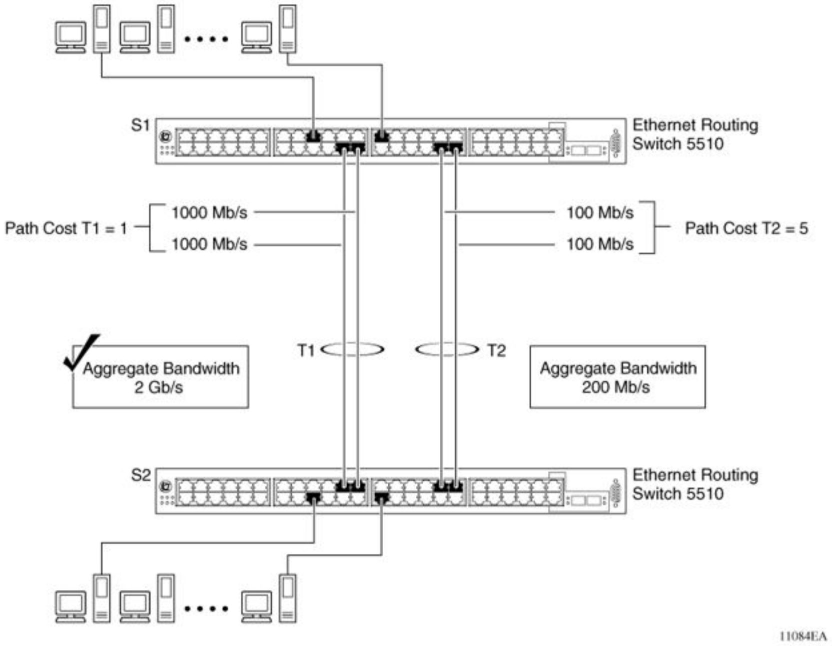
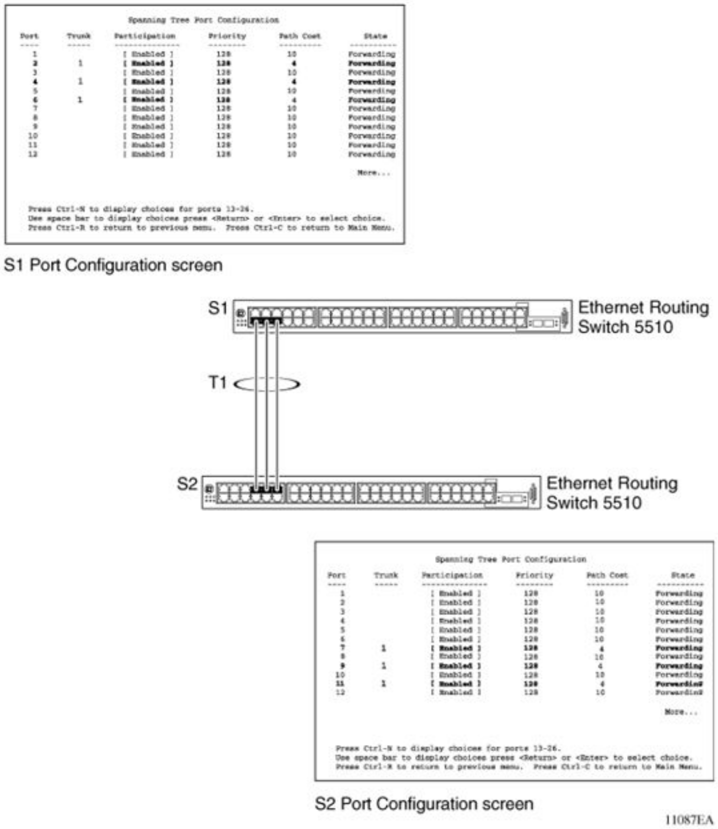

S1
Ethernet Routing Switch 5510
Path Cost T1 = 1
1000 Mb/s
1000 Mb/s
100 Mb/s
100 Mb/s
Path Cost T2 = 5
T1
T2
Aggregate Bandwidth 2 Gb/s
Aggregate Bandwidth 200 Mb/s
S2
Ethernet Routing Switch 5510
11084EA

Figure 18: Path Cost Arbitration

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



```
                      Spanning Tree Port Configuration

Port      Trunk     Participation      Priority      Path Cost       State
----      -----     --------------     --------      ---------     ----------
  1                  [ Enabled ]         128            10         Forwarding
  2         1        [ Enabled ]         128             4         Forwarding
  3                  [ Enabled ]         128            10         Forwarding
  4         1        [ Enabled ]         128             4         Forwarding
  5                  [ Enabled ]         128            10         Forwarding
  6         1        [ Enabled ]         128             4         Forwarding
  7                  [ Enabled ]         128            10         Forwarding
  8                  [ Enabled ]         128            10         Forwarding
  9                  [ Enabled ]         128            10         Forwarding
 10                  [ Enabled ]         128            10         Forwarding
 11                  [ Enabled ]         128            10         Forwarding
 12                  [ Enabled ]         128            10         Forwarding

                                                                    More...


  Press Ctrl-N to display choices for ports 13-26.
  Use space bar to display choices press <Return> or <Enter> to select choice.
  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

S1 Port Configuration screen

```
                      Spanning Tree Port Configuration

Port      Trunk     Participation      Priority      Path Cost       State
----      -----     --------------     --------      ---------     ----------
  1                  [ Enabled ]         128            10         Forwarding
  2                  [ Enabled ]         128            10         Forwarding
  3                  [ Enabled ]         128            10         Forwarding
  4                  [ Enabled ]         128            10         Forwarding
  5                  [ Enabled ]         128            10         Forwarding
  6                  [ Enabled ]         128            10         Forwarding
  7         1        [ Enabled ]         128             4         Forwarding
  8                  [ Enabled ]         128            10         Forwarding
  9         1        [ Enabled ]         128             4         Forwarding
 10                  [ Enabled ]         128            10         Forwarding
 11         1        [ Enabled ]         128             4         Forwarding
 12                  [ Enabled ]         128            10         Forwarding

                                                                    More...


  Press Ctrl-N to display choices for ports 13-26.
  Use space bar to display choices press <Return> or <Enter> to select choice.
  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

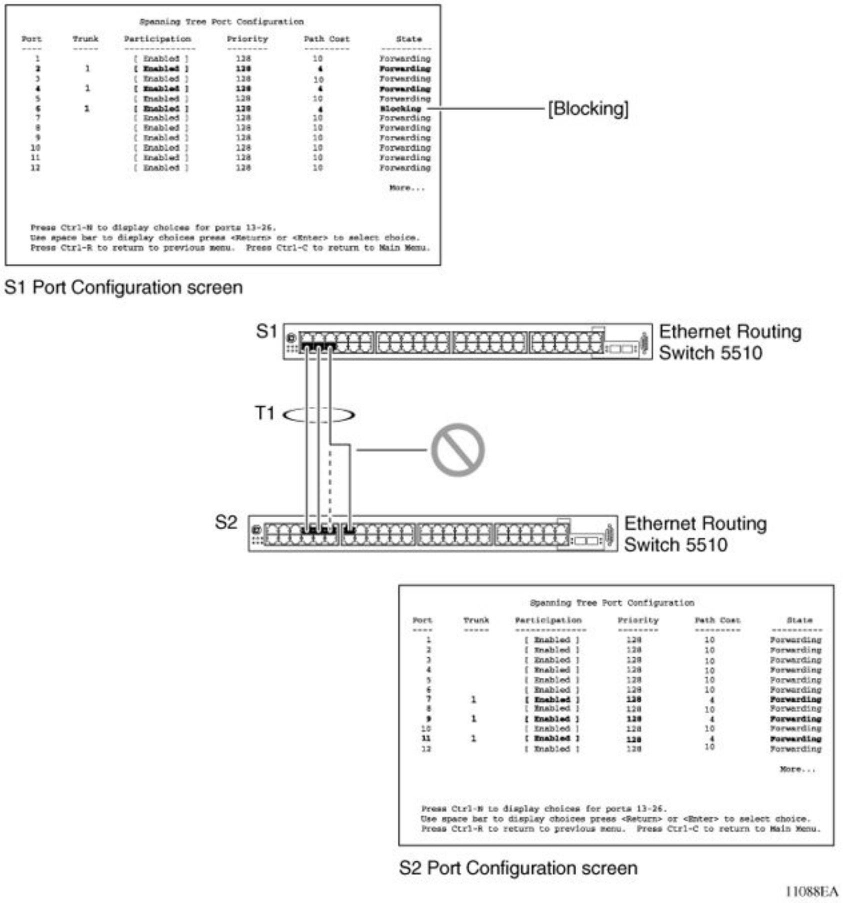
S2 Port Configuration screen

Figure 19: Correctly Configured Trunk

Note:

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

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



```
                     Spanning Tree Port Configuration

Port     Trunk     Participation     Priority     Path Cost         State
----     -----     -------------     --------     ---------     ----------
  1                 [ Enabled ]        128           10         Forwarding
  2        1        [ Enabled ]        128            4         Forwarding
  3                 [ Enabled ]        128           10         Forwarding
  4        1        [ Enabled ]        128            4         Forwarding
  5                 [ Enabled ]        128           10         Forwarding
  6        1        [ Enabled ]        128            4         Blocking
  7                 [ Enabled ]        128           10         Forwarding
  8                 [ Enabled ]        128           10         Forwarding
  9                 [ Enabled ]        128           10         Forwarding
 10                 [ Enabled ]        128           10         Forwarding
 11                 [ Enabled ]        128           10         Forwarding
 12                 [ Enabled ]        128           10         Forwarding

                                                                  More...

  Press Ctrl-N to display choices for ports 13-26.
  Use space bar to display choices press <Return> or <Enter> to select choice.
  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

S1 Port Configuration screen

```
                     Spanning Tree Port Configuration

Port     Trunk     Participation     Priority     Path Cost         State
----     -----     -------------     --------     ---------     ----------
  1                 [ Enabled ]        128           10         Forwarding
  2                 [ Enabled ]        128           10         Forwarding
  3                 [ Enabled ]        128           10         Forwarding
  4                 [ Enabled ]        128           10         Forwarding
  5                 [ Enabled ]        128           10         Forwarding
  6                 [ Enabled ]        128           10         Forwarding
  7        1        [ Enabled ]        128            4         Forwarding
  8                 [ Enabled ]        128           10         Forwarding
  9        1        [ Enabled ]        128            4         Forwarding
 10                 [ Enabled ]        128           10         Forwarding
 11        1        [ Enabled ]        128            4         Forwarding
 12                 [ Enabled ]        128           10         Forwarding

                                                                  More...

  Press Ctrl-N to display choices for ports 13-26.
  Use space bar to display choices press <Return> or <Enter> to select choice.
  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

S2 Port Configuration screen

Figure 20: Detecting a Misconfigured Port

Note:

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

Port membership in MLT

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

To change port membership in Multi-Link Trunking:

1. Disable the trunk.
2. Make the change.
3. Re-enable the trunk.

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

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

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

SMLT

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

Overview

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

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

SMLT avoids loops by allowing two aggregation switches to appear as a single device to edge switches, which are dual-homed to the aggregation switches. The aggregation switches are interconnected using an Inter-Switch Trunk (IST), which allows them to exchange addressing and state information (permitting rapid fault detection and forwarding path modification). Although SMLT is primarily designed for Layer 2, it also provides benefits for Layer 3 networks as well.

Important:

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

You can configure a maximum of 32 SMLT trunks on one device.

SMLT is supported on standalone or stacked units in triangle, square, or full mesh configuration (see Figure 21: SMLT in triangle configuration on page 76 and Figure 23: SMLT in square configuration on page 81) and on stacks in triangle configuration.

You cannot configure SMLT data when SMLT is running. To modify an SLT or SMLT, you must disable SMLT on that port or trunk. Starting with Release 6.3 IGMP over SMLT is supported.

Note:

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

Note:

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

Note:

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

Advantages of SMLT

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

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

SMLT compared to Spanning Tree Protocol

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

- Spanning Tree must be used to detect loops
- No load sharing exists over redundant links
- Slow network convergence exists in case of failure

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

How does SMLT work?

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

Triangle SMLT configuration

Triangle SMLT configuration requires one pair of aggregation switches as shown in Figure 21: SMLT in triangle configuration on page 76. Triangle SMLT can be set up with standalone switches or in a stack configuration.

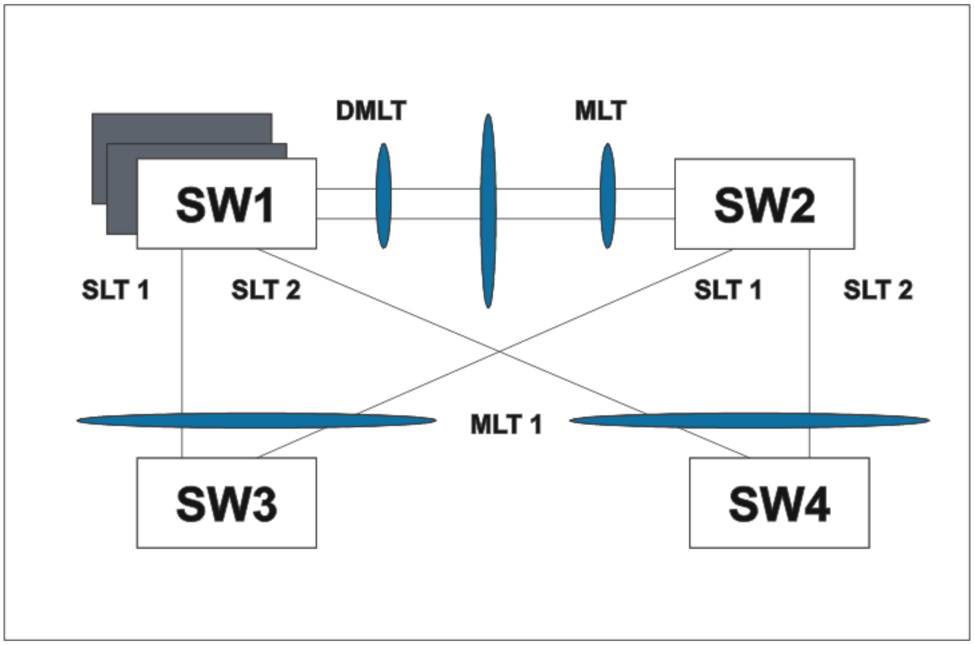


Figure 21: SMLT in triangle configuration

Detailed configuration example for SMLT triangle configuration

The following illustration and command set provides an example of SMLT triangle configuration.

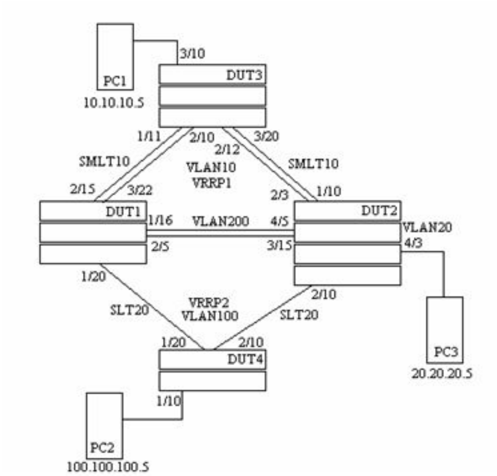


Figure 22: SMLT triangle configuration

Table 17: SMLT triangle configuration

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

Configure DUT1

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

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

```
ip add 100.100.100.3 255.255.255.0
exit
```

```
mlt 10 ena mem 2/15,3/22
```

```
mlt 30 ena mem 1/16,2/5
```

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

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

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

```
in vlan 100
ip vrrp address 2 100.100.100.1
ip vrrp 2 enable backup-master enable
ip ospf enable
exit
```

```
in vlan 10
ip vrrp address 1 10.10.10.1
ip vrrp 1 enable backup-master enabl
ip ospf enable
exit
```

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

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

Configure DUT2.

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

```
ip routing
in vlan 200
```

```
ip add 200.200.200.2 255.255.255.0
exit
in vlan 10
ip add 10.10.10.3 255.255.255.0
exit
in vlan 100
ip add 100.100.100.2 255.255.255.0
exit
```

```
in vlan 20
ip add 20.20.20.1 255.255.255.0
exit
```

```
mlt 10 ena mem 2/3,1/10
```

```
mlt 30 ena mem 4/5,3/15
```

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

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

```
in fast 2/10
smlt 20
exit
```

```
in vlan 100
\ip vrrp address 2 100.100.100.1
ip vrrp 2 enable backup-master enable
ip ospf enable
exit
```

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

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

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

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

Configure DUT3.

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

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

Configure DUT4.

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

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

Note:

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

Square SMLT configuration

Square SMLT configuration requires two pairs of aggregation switches connected back to back (see Figure 23: SMLT in square configuration on page 81). Square configuration supports standalone switches.

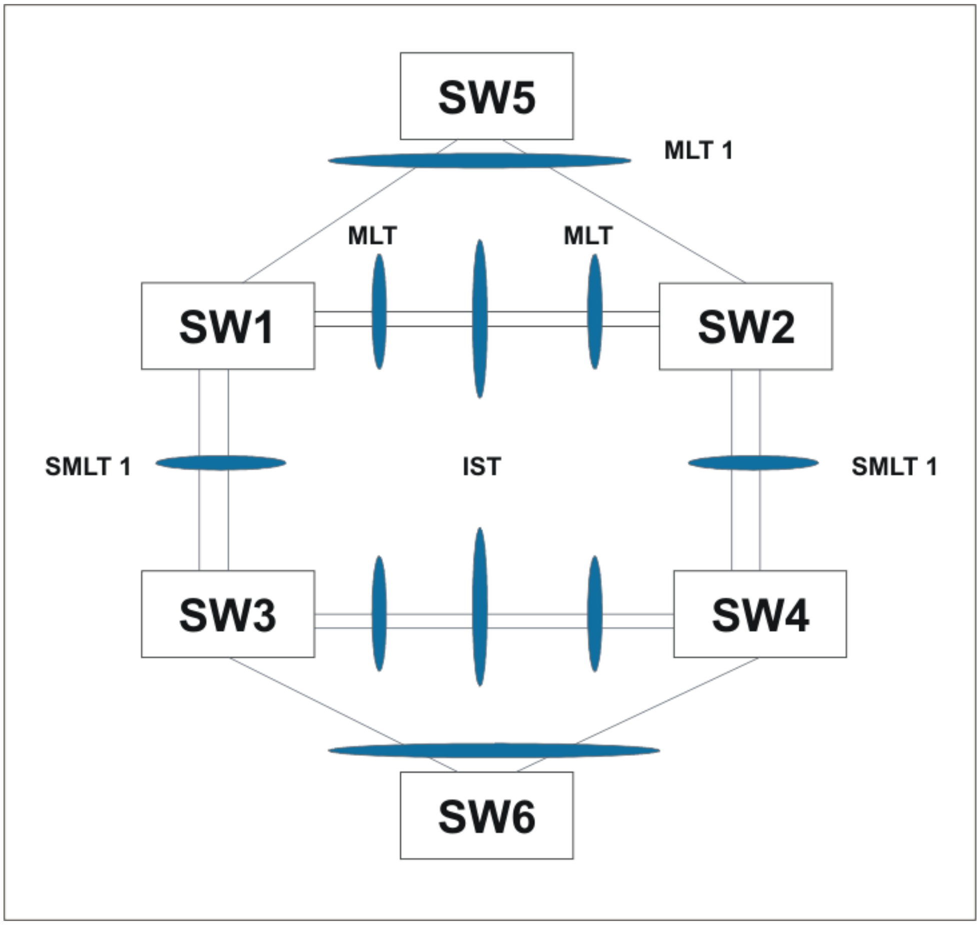


Figure 23: SMLT in square configuration

Detailed configuration example for SMLT in square configuration

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

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

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

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

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

IST ports on all switches must be tagged ports. SMLT ports can be tagged or untagged.

Each of the IST switches is running 2 VRRP instances.

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

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

If MLTs or ports are part of multiple Vlans, ensure that their PVID is configured appropriately.

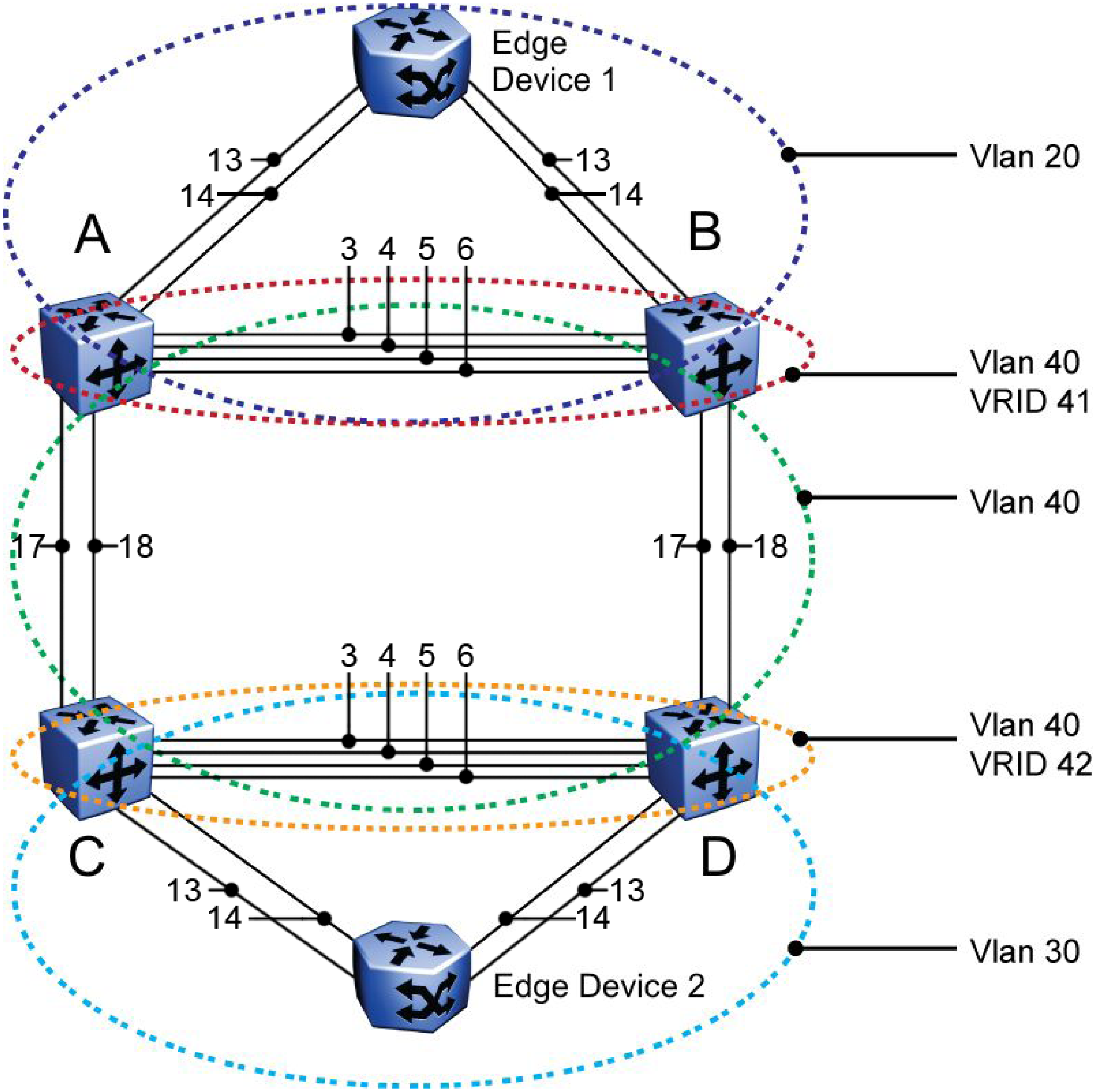


Figure 24: Square VRRP SMLT setup. Vlans and VRRP (IST vlans not indicated)

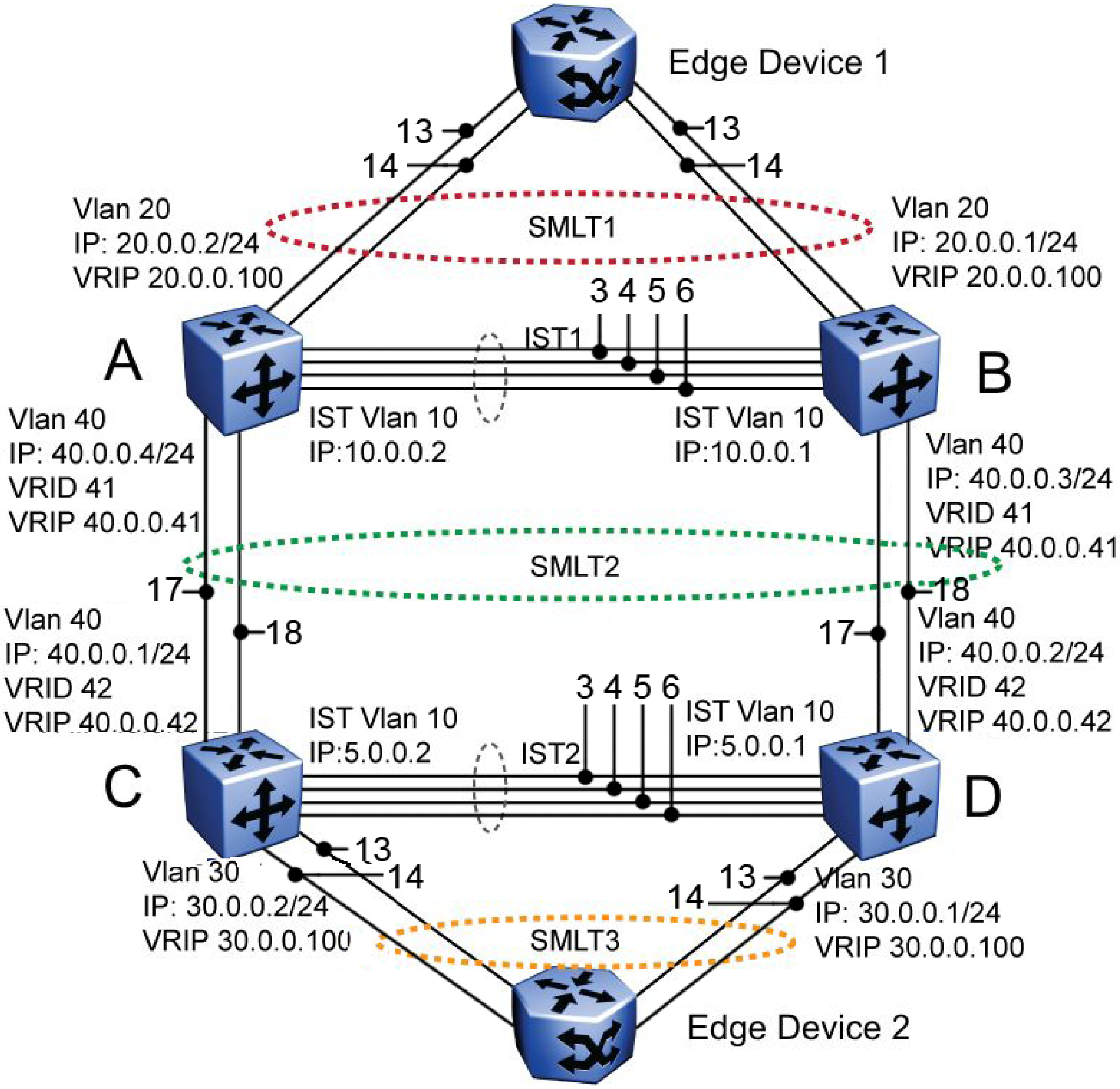


Figure 25: Square VRRP SMLT setup. SMLTs and ISTs

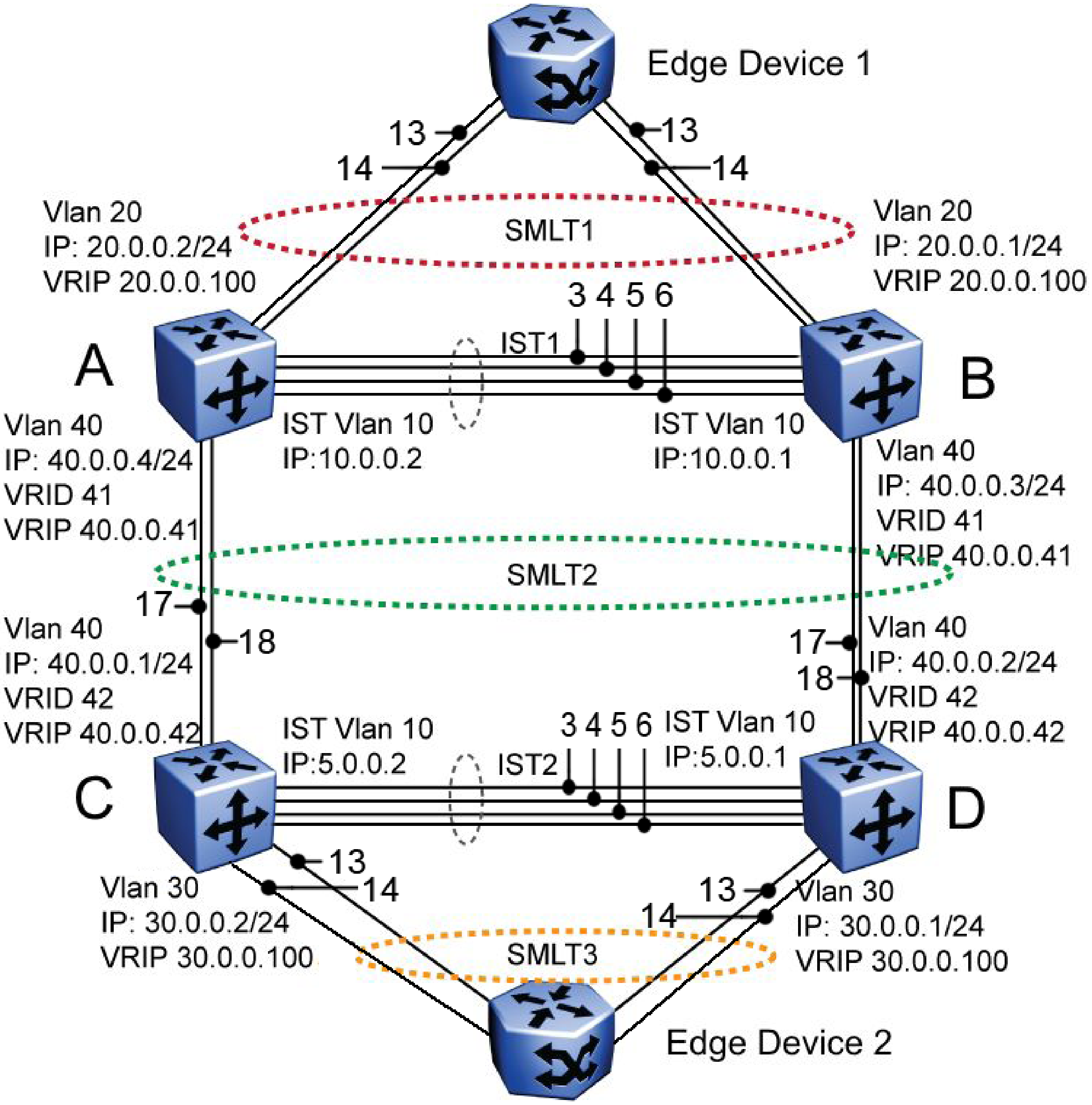


Figure 26: Square VRRP SMLT setup. Interface and VRRP IP addresses

The following paragraphs provide the configuration commands.

Edge Device 1

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

Edge Device 2

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

IST switch A

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

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

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

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

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

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

IST switch B

```
enable
configure terminal
```

```
vlan configcontrol autopvid
ip routing
router vrrp enable
vlan create 10 type port
vlan members add 10 3,4,5,6
interface vlan 10
ip address 10.0.0.1 255.255.255.0
exit
```

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

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

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

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

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

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

IST switch C

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

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

```
ip address 5.0.0.1 255.255.255.0
exit
```

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

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

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

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

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

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

IST switch D

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

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

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

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

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

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

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

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

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

SMLT in full mesh configuration

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

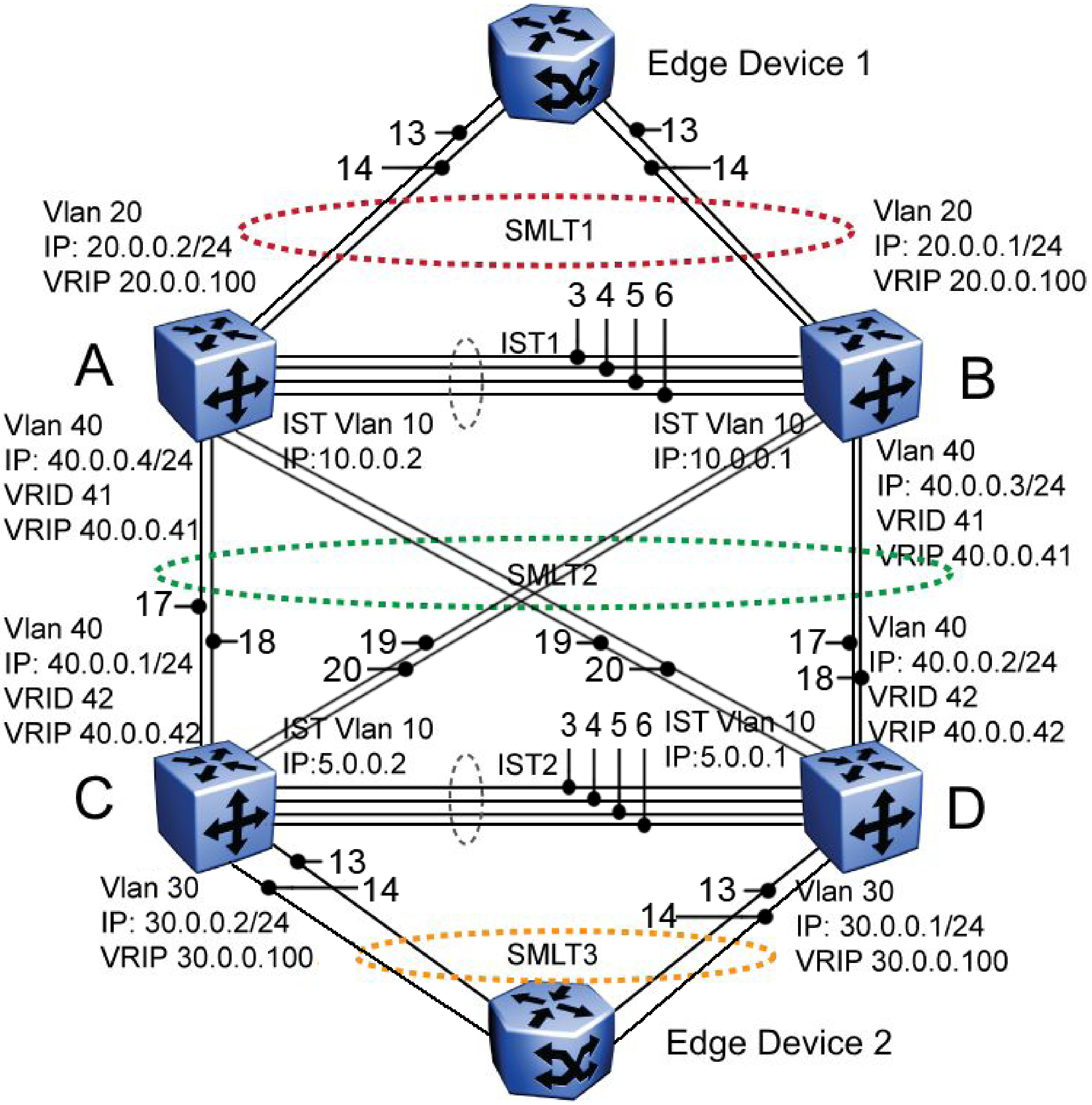


Figure 27: Full mesh SMLT configuration

Edge Device 1

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

Edge Device 2

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

IST switch A

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

```
ip routing
router vrrp enable
```

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

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

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

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

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

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

IST switch B

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

```
ip routing
router vrrp enable
```

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

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

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

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

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

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

IST switch C

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

```
ip routing
router vrrp enable
```

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

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

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

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

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

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

IST switch D

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

```
ip routing
router vrrp enable
```

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

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

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

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

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

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

SMLT in stack configuration

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

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

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

Each non base unit receives the SMLT configuration data from the base unit and saves to its own NVRAM.

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

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

If one or more of these checks is not successful, the SMLT application stops running, but SMLT remains administratively enabled.

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

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

- If the base unit becomes inactive, the temporary base takes over.
- If a non base unit becomes inactive, the base unit notifies the rest of the stack with a list of all SMLT and SLT ports lost.
- If all of the IST ports were on the inactive unit, SMLT stops running.

SMLT aggregation switches

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

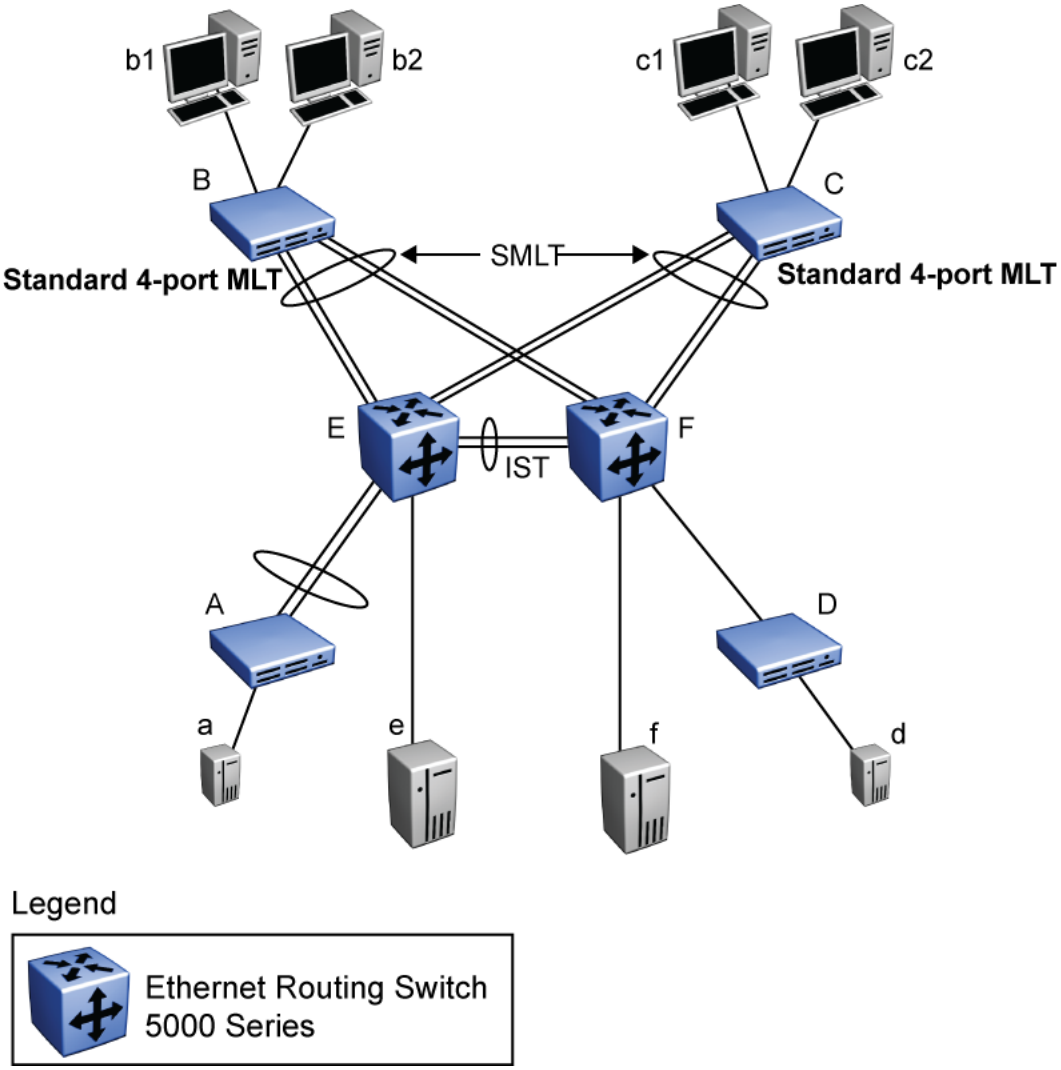


Figure 28: ERS 5000 Series switches as SMLT aggregation switches

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

IST

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

Important:

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

Aggregation switches use the IST to:

- Confirm that they are alive and exchange MAC address forwarding tables.
- Send traffic between single switches attached to the aggregation switches.
- Serve as a backup if one SMLT link fails.

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

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

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

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

ERS 5000 Series IST links cannot be partnered with ERS 8000 Series devices.

Important:

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

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

Other SMLT aggregation switch connections

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

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

The examples that follow explain the process in more detail.

Example 1- Traffic flow from a to b1 or b2

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

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

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

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

Example 3- Traffic flow from a to d

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

Example 4- Traffic flow from f to c1/c2

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

SLT

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

Important:

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

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

- MLT-based SMLT + MLT-based SMLT
- MLT-based SMLT + SLT
- SLT + SLT

Rules for configuring SLTs:

- The dual-homed device connected to the aggregation switches must be capable of supporting MLT.
- Each SLT is assigned an SMLT ID from 1 to 512. (The actual number of SLTs is limited only by the number of available ports on the device, minus two that must be reserved for the IST connection. For example, with a 48-port unit, you can configure a maximum of 46 SLTs.)
- SLT ports can be designated as Access or Trunk (that is, IEEE 802.1Q tagged or not tagged) and changing the type does not affect their behavior.
- You cannot change an SLT into an MLT-based SMLT by adding more ports. You must first delete the SLT, and then reconfigure the port as SMLT/MLT.
- You cannot change an MLT-based SMLT into a SLT by deleting all ports but one. You must first remove the SMLT, delete the MLT, and then reconfigure the port as an SLT.
- A port cannot be configured as an MLT-based SMLT and as an SLT at the same time.

Figure 29: SLT example on page 100 shows a configuration in which both aggregation switches have single port SLTs with the same IDs. This configuration allows as many SLTs, as available ports exist on the switch.

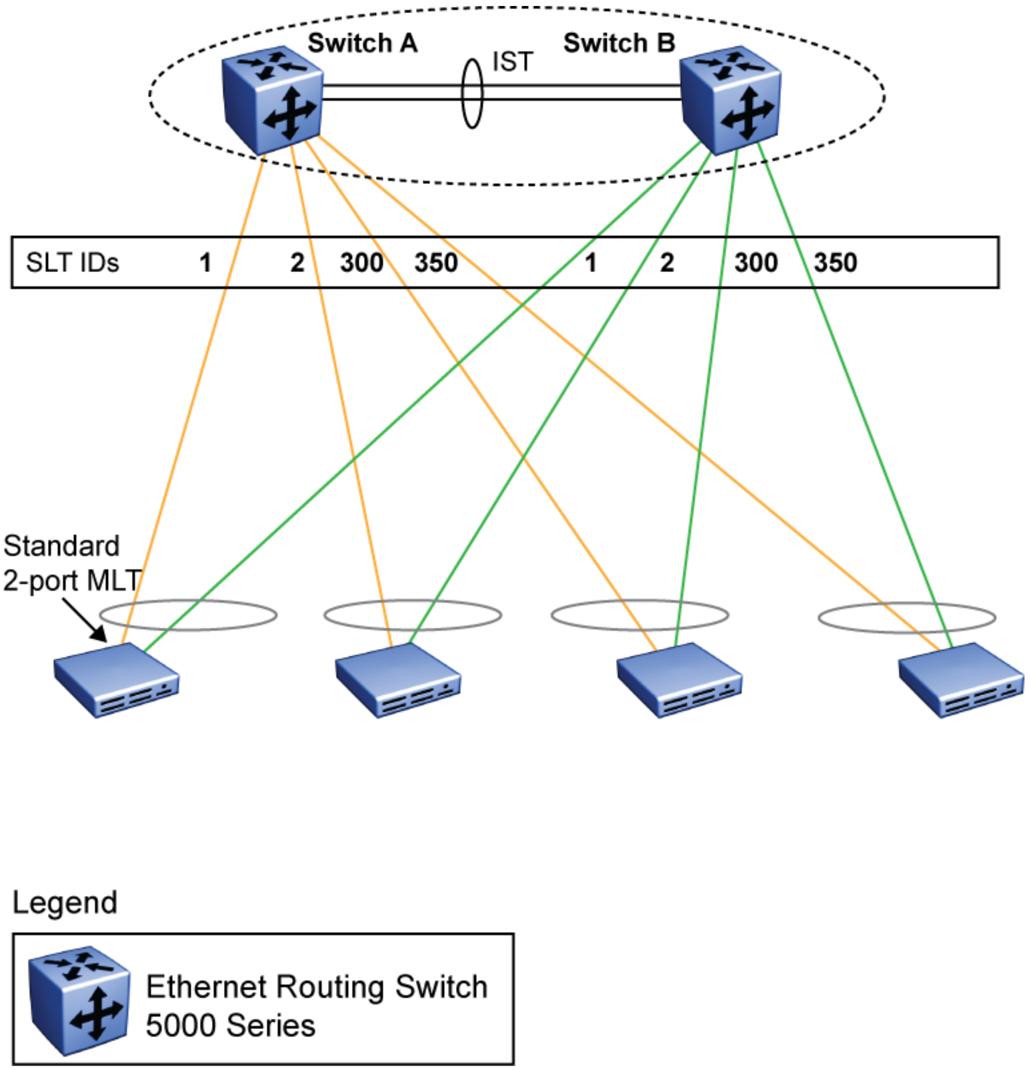


Figure 29: SLT example

SMLT with SLT

You can configure a split trunk with an SLT on one side and an MLT-based SMLT on the other. Both must have the same SMLT ID. In addition to general use, Figure 30: Changing a split trunk from MLT-based SMLT to SLT on page 101 shows how this configuration can be used for upgrading an MLT-based SMLT to an SLT without taking down the split trunk.

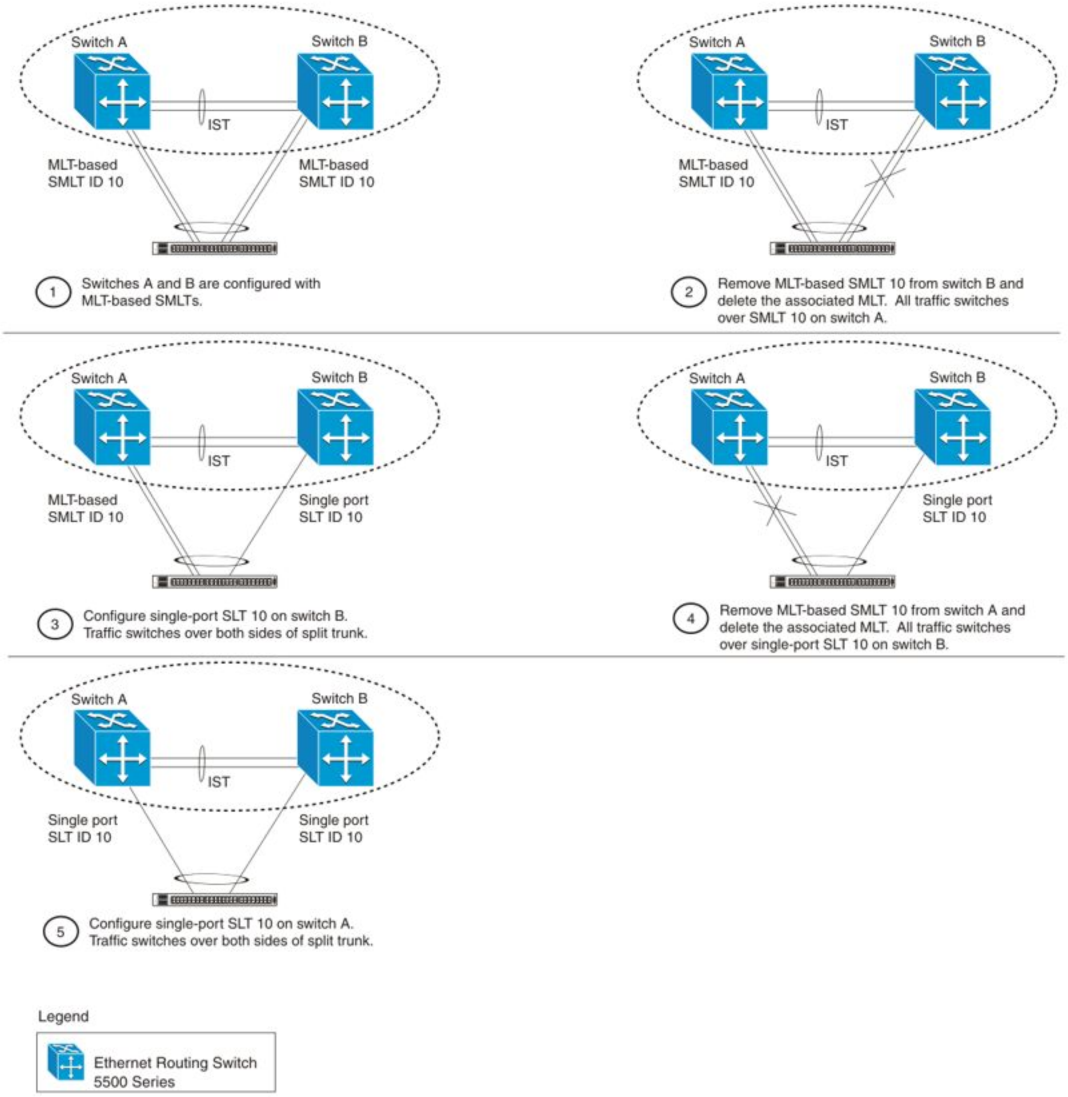

Switch A
Switch B
IST
MLT-based SMLT ID 10
MLT-based SMLT ID 10
1 Switches A and B are configured with MLT-based SMLTs.
Switch A
Switch B
IST
MLT-based SMLT ID 10
2 Remove MLT-based SMLT 10 from switch B and delete the associated MLT. All traffic switches over SMLT 10 on switch A.
Switch A
Switch B
IST
MLT-based SMLT ID 10
Single port SLT ID 10
3 Configure single-port SLT 10 on switch B. Traffic switches over both sides of split trunk.
Switch A
Switch B
IST
Single port SLT ID 10
4 Remove MLT-based SMLT 10 from switch A and delete the associated MLT. All traffic switches over single-port SLT 10 on switch B.
Switch A
Switch B
IST
Single port SLT ID 10
Single port SLT ID 10
5 Configure single-port SLT 10 on switch A. Traffic switches over both sides of split trunk.
Legend
Ethernet Routing Switch 5500 Series

Figure 30: Changing a split trunk from MLT-based SMLT to SLT

Important:

When you perform the steps listed in Figure 30: Changing a split trunk from MLT-based SMLT to SLT on page 101 and you remove the MLT-based SMLTs (steps 2 and 4), physically disable the ports by removing the cables or by shutting the ports down using the ACLI. Otherwise, a loop can form as soon as the SMLT is removed since STP is disabled on the ports.

SMLT and SLT configuration steps

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

❗ **Important:**

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

1. Configure VLANs, including port membership, VLAN IP, and port tagging.
2. Configure STP groups:
    a. Create STP groups.
    b. Assign VLAN membership.
    c. Enable STP groups.
    d. Set STP port participation.
3. Enable Global IP Routing on the devices (always required).
4. If the switches are to be used for Layer 3 routing, enable VRRP on the units (required for Layer 3 only).
5. Configure MLTs on the devices:
    a. Create MLT groups by assigning trunk members.
    b. Disable STP participation on all trunk member ports (required only on edge switch MLT ports that are connected to the SMLT or SLT) .
    c. Enable the MLTs.
6. Configure SMLTs on the devices:
    a. Assign the Peer IP address and VLAN ID to the IST MLT.
    b. Enable the IST.
    c. Create the SMLTs.
    d. Create the SLTs (if applicable).
7. Make IST connections and ensure IST session is running.
8. Make SMLT/SLT connections and check SMLT/SLT status.

✱ **Note:**

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

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

SMLT configuration example with VRRP and OSPF

Figure 31: SMLT configuration example with VRRP and OSPF on page 103 shows an example of aggregation switches configured with SMLT, VRRP, and OSPF. For more information on VRRP and OSPF, see *Avaya Ethernet Routing Switch 5000 Series Configuration — IP Routing Protocols* , NN47200-503.

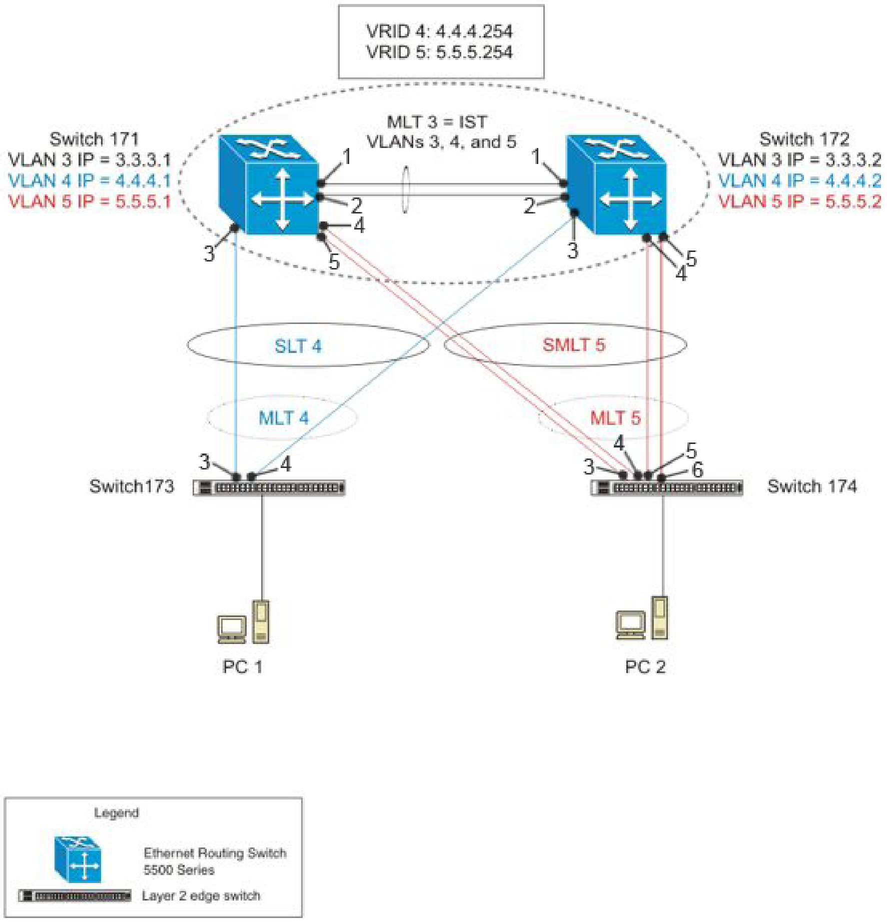


Figure 31: SMLT configuration example with VRRP and OSPF

To configure the example shown in Figure 31: SMLT configuration example with VRRP and OSPF on page 103, you must perform the following tasks:

For aggregation switch 171

1. Create VLANs 3, 4, and 5.
2. Set ports 1-5 as tagging.
3. Assign ports 1 and 2 to VLAN 3.
4. Assign ports 1, 2 and 3 to VLAN 4.
5. Assign ports 1, 2, 4 and 5 to VLAN 5.
6. Set VLAN 3 IP to 3.3.3.1 .
7. Set VLAN 4 IP to 4.4.4.1 .
8. Set VLAN 5 IP to 5.5.5.1 .
9. Enable IP routing globally.
10. Create MLT 3 with ports 1 and 2.
11. Set IST = MLT 3, Peer IP=3.3.3.2, VLAN 3.
12. Configure port 3 as SLT with SMLT ID 4.
13. Create MLT 5 with ports 4 to 5.
14. Set MLT 5 as SMLT 5.
15. Enable VRRP globally.
16. Enable VRRP on VLAN 4 with VRID 4 and VRIP 4.4.4.254.
17. Enable VRRP back up master.
18. Enable VRRP on VLAN 5 with VRID 5 and VRIP 5.5.5.254.
19. Enable VRRP back up master.
20. Enable OSPF globally.
21. Enable OSPF on VLANs 3,4 and 5.

For aggregation switch 172

1. Create VLANs 3, 4, and 5.
2. Set ports 1 to 5 as tagging.
3. Assign ports 1 and 2 to VLAN 3.
4. Assign ports 1, 2 and 3 to VLAN 4.
5. Assign ports 1, 2, 4 and 5 to VLAN 5.
6. Set VLAN 3 IP to 3.3.3.2.
7. Set VLAN 4 IP to 4.4.4.2.
8. Set VLAN 5 IP to 5.5.5.2.
9. Enable IP routing.
10. Create MLT 3 with ports 1 and 2.
11. Set IST = MLT 3, Peer IP=3.3.3.1, VLAN 3.

12. Configure port 3 as SLT with SMLT ID 4.
13. Create MLT 5 with ports 4 to 5.
14. Set MLT 5 as SMLT 5.
15. Enable VRRP globally.
16. Enable VRRP on VLAN 4 with VRID 4 and VRIP 4.4.4.254.
17. Enable VRRP back up master.
18. Enable VRRP on VLAN 5 with VRID 5 and VRIP 5.5.5.254.
19. Enable VRRP back up master.
20. Enable OSPF globally.
21. Enable OSPF on VLAN 3, 4, and 5

For edge switch 173

1. Create Vlan 4.
2. Assign ports 3 to 4 to Vlan 4.
3. Create MLT 4 with ports 3 to 4.
4. Disable STP on MLT 4.

For edge switch 174

1. Create Vlan 5.
2. Assign ports 3 to 6 to Vlan 5.
3. Create MLT 5 with ports 3 to 6.
4. Disable STP on MLT 5.

Detailed configuration commands

Aggregation switch 171 configuration

IST, SMLT and SLT configuration

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

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

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

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

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

```
5520-48T-PWR(config)#mlt 3 member 1-2
5520-48T-PWR(config)#mlt 3 enable
5520-48T-PWR(config)#interface mlt 3
5520-48T-PWR(config-if)#ist enable peer-ip 3.3.3.2 vlan 3
5520-48T-PWR(config-if)#exit
```

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

```
5520-48T-PWR(config)#mlt 5 member 4-5
5520-48T-PWR(config)#mlt 5 enable
5520-48T-PWR(config-if)#interface mlt 5
5520-48T-PWR(config-if)#smlt 5
5520-48T-PWR(config-if)#exit
```

VRRP and OSPF

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

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

Aggregation switch 172 configuration

IST, SMLT and SLT configuration

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

```
5520-48T-PWR(config)#vlan member add 4 3
5520-48T-PWR(config)#vlan member add 5 4,5
5520-48T-PWR(config)#ip routing
```

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

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

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

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

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

```
5520-48T-PWR(config)#mlt 5 member 4-5
5520-48T-PWR(config)#mlt 5 enable
5520-48T-PWR(config-if)#interface mlt 5
5520-48T-PWR(config-if)#smlt 5
5520-48T-PWR(config-if)#exit
```

VRRP and OSPF

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

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

Edge switch 173 configuration (5000 Series)

```
5510-48T(config)#vlan create 4 type port
 5510-48T(config)#vlan port 3-4 tagging enable
5510-48T(config)#vlan member add 4 3-4
```

```
5510-24T(config)#mlt 4 member 3-4
5510-24T(config)#mlt spanning-tree 4 stp all learning disable
5510-24T(config)#mlt 4 enable
```

Edge switch 174 configuration (5000 Series)

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

SLT configuration example with VRRP and OSPF

Figure 32: SLT configuration example with VRRP and OSPF on page 109 shows an example of aggregation switches configured with SLT, VRRP and OSPF. For more information on VRRP and OSPF, see *Avaya Ethernet Routing Switch 5000 Series Configuration — IP Routing Protocols*, NN47200-503.

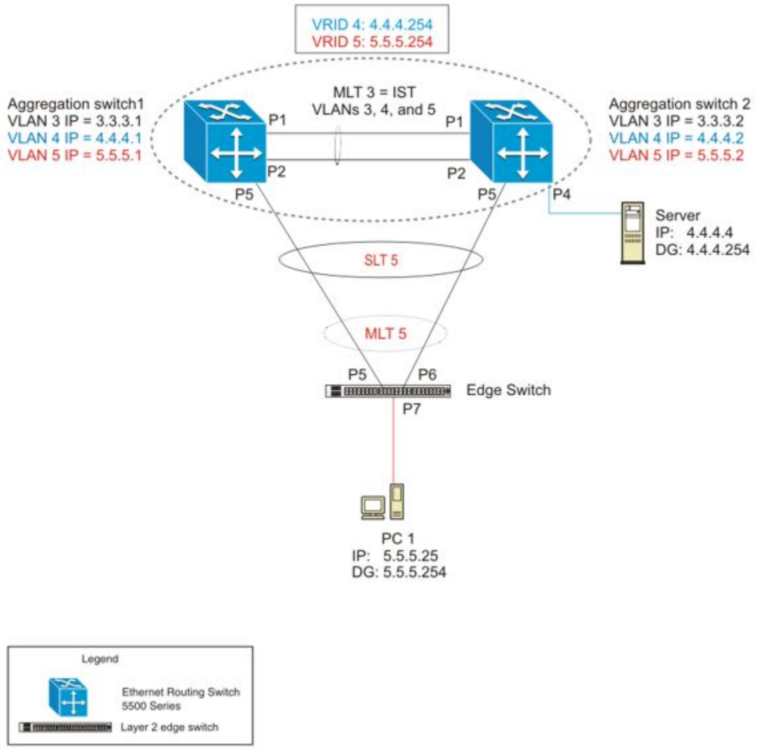


Figure 32: SLT configuration example with VRRP and OSPF

To configure the example shown in Figure 32: SLT configuration example with VRRP and OSPF on page 109, you must perform the following tasks.

For aggregation switch 1:

1. Create VLANs 3, 4, and 5.
2. Set ports 1 to 5 as tagging.
3. Assign ports 1 and 2 to VLAN 3.
4. Assign ports 1 and 2 to VLAN 4.
5. Assign ports 1, 2, and 5 to VLAN 5.
6. Set VLAN 3 IP to 3.3.3.1 .
7. Set VLAN 4 IP to 4.4.4.1 .
8. Set VLAN 5 IP to 5.5.5.1 .
9. Enable IP routing globally.
10. Create MLT 3 with ports 1-2.
11. Set IST = MLT 3, Peer IP=3.3.3.2, VLAN 3.

12. Set port 5 as SLT 5.
13. Enable VRRP globally
14. Enable VRRP on VLAN 4 with VRID 4 and VRIP 4.4.4.254.
15. Enable VRRP back up master.
16. Enable VRRP on VLAN 5 with VRID 5 and VRIP 5.5.5.254 .
17. Enable VRRP back up master.
18. Enable OSPF globally.
19. Enable OSPF on VLANs 3,4 and 5.

For aggregation switch 2:

1. Create VLANs 3, 4, and 5.
2. Set ports 1,2 and 5 as tagging.
3. Assign ports 1 and 2 to VLAN 3.
4. Assign ports 1, 2 and 4 to Vlan 4.
5. Assign ports 1, 2 and 5 to Vlan 5.
6. Set Vlan 3 IP to 3.3.3.2.
7. Set Vlan 4 IP to 4.4.4.2.
8. Set Vlan 5 IP to 5.5.5.2.
9. Enable IP routing.
10. Create MLT 3 with ports 1 and 2.
11. Set IST = MLT 3, Peer IP=3.3.3.1, Vlan 3.
12. Set port 5 as SLT 5.
13. Enable VRRP globally.
14. Enable VRRP on Vlan 4 with VRID 4 and VRIP 4.4.4.254.
15. Enable VRRP back up master.
16. Enable VRRP on Vlan 5 with VRID 5 and VRIP 5.5.5.254.
17. Enable VRRP back up master.
18. Enable OSPF globally.
19. Enable OSPF on Vlan 3, 4 and 5.

For edge switch 1:

1. Create Vlan 5.
2. Set ports 5 and 6 as tagging.
3. Assign ports 5 to 7 to Vlan 5.
4. Create MLT 5 with ports 5 and 6.
5. Disable STP on ports 5 and 6.

Detailed configuration commands

The following sections describe the detailed ACLI commands required to carry out the configuration described in Figure 32: SLT configuration example with VRRP and OSPF on page 109

Aggregation switch 1 configuration

IST, SMLT and SLT configuration

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

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

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

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

```
5520-48T-PWR(config)#mlt 3 member 1-2
5520-48T-PWR(config)#mlt 3 enable
5520-48T-PWR(config)#interface mlt 3
5520-48T-PWR(config-if)#ist enable peer-ip 3.3.3.2 vlan 3
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface fastEthernet 5
5520-48T-PWR(config-if)#smlt 5
5520-48T-PWR(config-if)#exit
```

VRRP and OSPF

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

```
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit
```

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

Aggregation switch 2 configuration

IST, SMLT and SLT configuration

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

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

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

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

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

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

VRRP and OSPF

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

```
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit
```

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

Edge switch configuration (5000 Series)

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

SLPP

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

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

Note:

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

SLPP Guard

Simple Loop Prevention Protocol (SLPP) is used to detect loops in the SMLT network. 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 ERS 5000 in combination with other Avaya switches that support Simple Loop Protection Protocol (SLPP) and Avaya’s Switch Clustering (SMLT) - for example, ERS 4000 Series or ERS 8300 - the SLPP Guard feature provides additional network loop protection.

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: ERS 5000 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 ERS 8300 transmits SLPP packets from that port. With SLPP Guard enabled on ERS 5000 port 1, when ERS 5000 port 1 receives an SLPP packet the system automatically shuts ERS 5000 port 1 down, preventing the possibility of data looping between ERS 5000 port 1 and ERS 8300 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.

Avaya recommends that you enable SLPP Guard only on the edge switches of an SMLT setup and SLPP on the aggregation layer switches.

When an SLPP packet is received on an SLPP Guard enabled port, the port is disabled only if the Ethertype field from the received SLPP packet is equal to the value of the SLPP Guard Ethertype configured on the receiving switch.

Note:

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

LACP over SMLT

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

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

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

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

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

For a configuration example, see LACP over SMLT configuration example on page 397.

SMLT with Routing protocol support

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

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

SMLT consistency with the Ethernet Routing Switch 8800/8600

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

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

IEEE 802.3ad Link Aggregation

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

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

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

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

Link aggregation employs the following principles and concepts:

- A MAC client communicates with a set of ports through an Aggregator, which presents a standard IEEE 802.3 service interface to the MAC client. The Aggregator binds to one or more ports within a system.
- The Aggregator is responsible for distributing frame transmissions from the MAC client to the various ports, and to collect received frames from the ports and pass them to the MAC client transparently.
- A system can contain multiple aggregators, serving multiple MAC clients. A given port will bind to (at most) a single Aggregator at any time. A MAC client is served by a single Aggregator at a time.
- The binding of ports to aggregators within a system is managed by the Link Aggregation Control function for that system, which is responsible for determining which links can be aggregated, aggregating them, binding the ports within the system to an appropriate Aggregator, and monitoring conditions to determine when a change in aggregation is needed.

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

  The LACP uses peer exchanges across the links to determine, on an ongoing basis, the aggregation capability of the various links, and continuously provides the maximum level of aggregation capability achievable between a given pair of systems.
- Each port is assigned a unique, globally administered MAC address.

  The MAC address is used as the source address for frame exchanges that are initiated by entities within the Link Aggregation sublayer itself (for example, LACP and Marker protocol exchanges).
- Each Aggregator is assigned a unique, globally administered MAC address, which is used as the MAC address of the aggregation from the perspective of the MAC Client, both as a source address for transmitted frames and as the destination address for received frames.

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

Link aggregation rules

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

- Link aggregation groups are formed using LACP.
- All ports in a link aggregation group must be connected to the same far-end system.
- All ports in a link aggregation group must be operating in full-duplex mode.
- All ports in a link aggregation group must be configured to the same port speed.

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

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

The failover process is as follows:

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

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

LACP port mode

The IEEE 802.1ax standard specifies that links that are not successful candidates for aggregation (for example, links to devices that cannot perform aggregation, or links that are manually set as non-aggregatable) can continue to operate as individual LACP links. However, LACP-enabled, STP-disabled ports that operate as individual links can potentially cause network loops.

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

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

in the blocking state. This behavior is applied only to LACP-enabled ports that have STP disabled and prevents potential loops from forming in the network.

> **Note:**
>
> The Advance mode is not compatible with IEEE 802.1ax standard LACP.

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

- **Default mode:** The default mode implementation removes the active LACP trunk port from the active trunk configuration, and the port functions as a regular standalone active port. The port state is determined by STP when you enable STP, but is set to forwarding when you disable STP on the port.
- **Advance mode**: In the Advance mode, LACP-enabled ports that have STP disabled remain in the blocking state. This prevents potential loops from forming in the network.

Chapter 6: VLACP Fundamentals

VLACP

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.

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.

VLACP overview

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

Figure 33: Problem description (1 of 2) on page 120 provides an illustration of these limitations. While the Enterprise networks shown can connect their aggregated Ethernet trunk groups through a service provider network connection (for example, through a VPN), far-end failures cannot be signaled with Ethernet-based functions that operate end-to-end through the service provider cloud.

In Figure 33: Problem description (1 of 2) on page 120, the link (between Enterprise switches S1 and S2) extends through the service provider (SP) network.

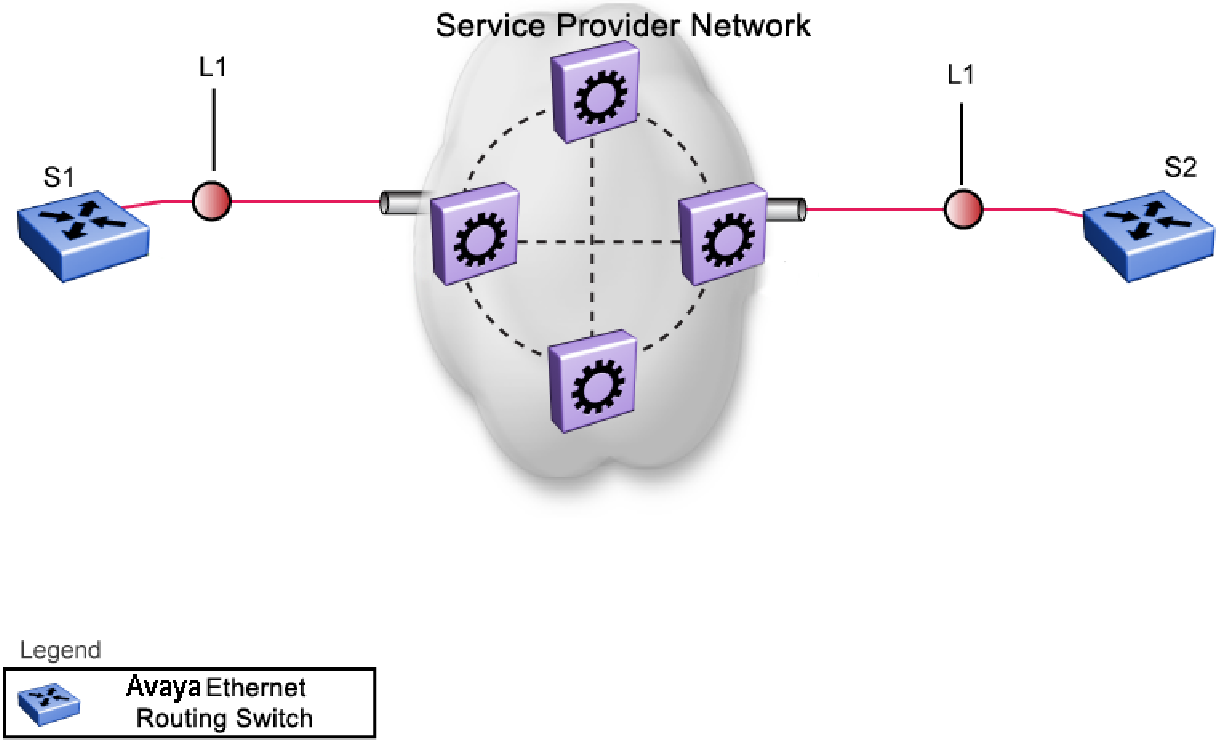


Figure 33: Problem description (1 of 2)

As shown in Figure 34: Problem description (2 of 2) on page 121, if the L2 link on S1 (S1/L1) fails, the link-down failure is not propagated over the SP network to S2. Therefore, S2 continues to send traffic over the S2/L1 link, which is black-holed because the S1/L1 link has failed.

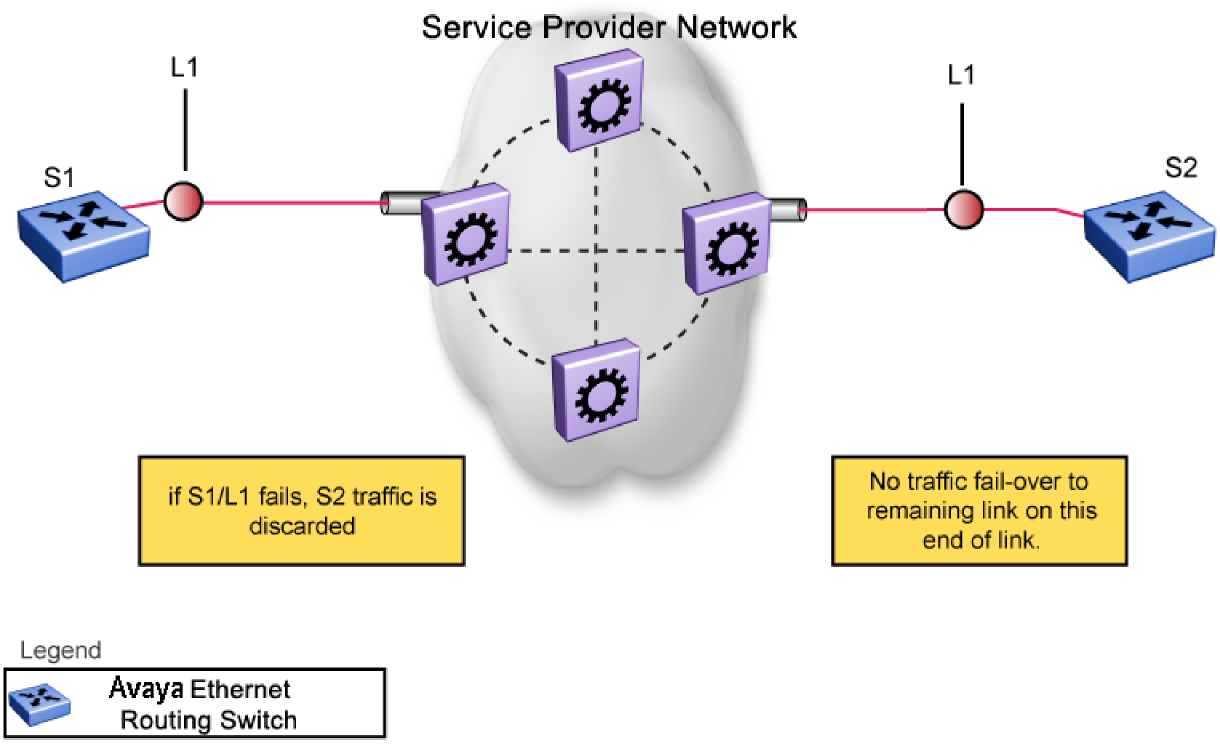

Service Provider Network
L1
S1
L1
S2
if S1/L1 fails, S2 traffic is discarded
No traffic fail-over to remaining link on this end of link.
Legend
Avaya Ethernet Routing Switch

Figure 34: 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 developed VLACP, which is an extension to LACP. 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 34: Problem description (2 of 2) on page 121.

VLACP features

VLACP on the Ethernet Routing Switch 5000 Series provides the following:

- VLACP is configured per port. A port can be an individual port or a member of an MLT.
- When you set VLACP parameters for a trunk port, the settings are applied to all trunk members.
- For VLACP to operate properly, there must be a logical point-to-point connection (Layer 2 tunnel) between the two endpoints.
- VLACP does not work for point-to-multipoint connections.

- On each port that has VLACP enabled, VLACPDUs are sent periodically. If VLACPDUs are not received on a particular link, that link is taken down after a configurable timeout period.
- For the current software release, VLACP is supported on Ethernet interfaces only.
- VLACP can run independently as a port-to-port protocol or on top of MLT or LACP protocol.
- VLACP packets are untagged because they operate at the port level and not the VLAN level.
- The Destination Mac Address used in VLACPDUs is configurable. The MAC Address must be a multicast MAC Address so that it is always flooded. This allows the exchange of VLACPDUs from end to end.
- Both VLACP partners must have same multicast address, timers, and ethertype configured for VLACP to work properly.
- A unicast MAC address (destination MAC address) can be configured per port for end-to-end connectivity between units, when VLACP packets travel through an ISP network.
- The VLACP PDU transmission interval changes when an LACP partner is lost. This aids detection in certain failure scenarios.
- VLACP PDU messages are processed so as to prevent false VLACP state recovery.
- VLACP defaults to an IEEE reserved multicast MAC address for sourcing LACP PDU packets.
- VLACP can be configured on MLT ports only if the MLT directly connects two switches. VLACP doesn't function if another Layer 2 device exists between the switches.

Troubleshooting

Error logs are created for the following failures and errors:

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

Chapter 7: ADAC fundamentals

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

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

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

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

- **Untagged-Frames-Basic**:

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

- **Untagged-Frames-Advanced**:

  Use this mode when you want an advanced configuration and the IP Phones are sending untagged traffic. In this mode, ADAC dynamically configures the Call Server or Uplink port, as applicable, and all telephony ports. All tagging, PVID settings, port vlan membership and traffic prioritization are configured automatically.

- **Tagged Frames:**

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

ADAC operation

The following sections provide detailed explanations of ADAC operation.

Auto-detection of Avaya IP Phones

When a Avaya IP Phone is powered on and connected to a switch, the switch automatically detects the IP Phone and 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 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 is sent (if ADAC traps are enabled) and autoconfiguration is removed. To put the port back into the operational state, disable and then re-enable auto-detection on the affected port. ADAC supports a maximum of 32 devices (both IP phones and non-phones) per port.

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

The detection mechanism can be selected

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

The two methods of auto-detection are by MAC address, or LLDP (IEEE 802.1ab). Auto-detection by MAC address is based on using predefined MAC addresses to determine that the specified port is connected to a Avaya IP phone. For more information and the list of defined MAC address ranges, see Auto-detection by MAC address on page 124.

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 126.

You can enable either of these detection mechanisms or both on individual ports. At least one of these detection methods must be enabled on each port. By default, both detection methods are enabled on Avaya ERS 5000 Series switches.

Auto-detection by MAC address

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

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

Table 18: Default ADAC MAC address ranges on page 125shows a list of the default MAC address ranges.

Table 18: Default ADAC MAC address ranges

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

Lower End	Higher End
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 the default known 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, it does not 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 the MAC address is added to the supported ranges later, 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)

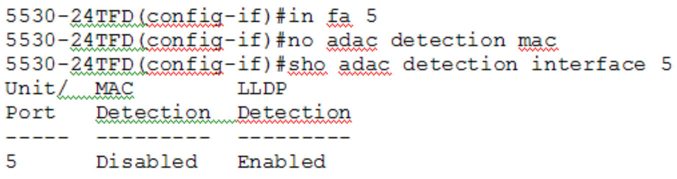
Auto-detection by LLDP extends the auto-detection that relies on MAC addresses. This feature allows devices identified as IP phones through LLDP to be detected by ADAC even if their MAC addresses are outside the list of ADAC MAC address ranges.

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

Detailed configuration example

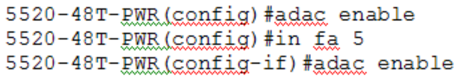
The following commands provide a detailed configuration example.

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



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

- Enable ADAC on port 5 and globally.



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

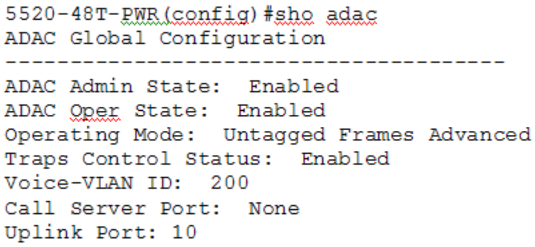
- Define the uplink port, and voice VLAN port, then change operating mode to Untagged Frames Advanced.

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

Note:

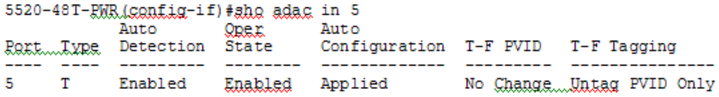
Configure the voice-vlan 200 before setting ADAC; as described in the Voice VLAN Integration on page 31.

- Verify the settings are applied.



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

- Connect your phone on port 5 and verify that the phone is detected and the configuration is applied.



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

Auto-configuration of Avaya IP Phones

You can configure the ADAC port participation independently by enabling or disabling ADAC for specific 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 is applied on the port when the port is operational (operational state is enabled) and if one of these conditions is true:

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

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

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

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

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

Initial user settings

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

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

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

Note:

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

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

Port restrictions

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

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

- part of a trunk (MLT, LAG)
- a Monitor Port in port mirroring
- a NSNA port
- a Telephony port
- the Uplink port
- an EAP port

The **Uplink port** must not be:

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

The **Telephony port** must not be:

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

Operating modes

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

QoS settings used by ADAC

ADAC QoS configuration is applied to:

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

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

- **all-IP-traffic**

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

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

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

Untagged-Frames-Basic operating mode

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

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

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

QoS configuration

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

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

VLAN configuration

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

- Tagging of Telephony ports is set to Untagged.

Untagged-Frames-Advanced operating mode

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

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

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

QoS configuration

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

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

VLAN configuration

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

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

Tagged-Frames operating mode

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

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

QoS configuration

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

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

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

VLAN configuration

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

- Telephony port:
  - Membership = adds to Voice-VLAN; not removed from other VLANs
  - Tagging = UntagPVIDOnly

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

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

Dynamic VLAN auto-configuration

The following describes the details of the ADAC VLAN configuration:

- You must manually create the Voice VLAN to be used by ADAC prior to configuration for ADAC.
- The ADAC ports membership to the ADAC Voice VLAN are dynamic, the settings do not save to NVRAM. The dynamic settings are lost on reboot or when ADAC is disabled.
- From the moment ADAC is enabled on a port configured as a telephony port or a call server port, (but not an uplink port), all VLAN configuration is dynamic (including user configuration). When removing the configuration for a port (for example, when changing a port so that it is no longer a call server port or a telephony port), the configuration from NVRAM is restored. Once restored, the user configuration is permanent again. For an uplink port, any user configuration made while ADAC was enabled on the port is saved.
- For telephony ports, the NVRAM VLAN configuration is restored in two cases: when the ADAC configuration is removed due to the removal of the IP Phone, or when ADAC is disabled for that port.
- The VLAN Configuration Control (VCC) rules, other than those for the Flexible mode, are skipped internally by ADAC configuring VLANs. Any VLAN settings made automatically by ADAC follow the rules of the Flexible mode, regardless of the current value of VCC. Any settings that you modify manually on ADAC ports follow the current VCC mode, as for a non-ADAC port.
- If you change the preset values of Tagging and PVID when ADAC is running in Tagged-Frames mode, future auto-configurations apply the new values. Changing the preset has no effect on current configured Tagging and PVID values.
- You can change the nonADAC VLANs on a port without disabling ADAC.

ADAC and stacking

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

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

If two or more units each have Call Server ports configured in standalone mode and are then joined together in a stack, the Call Server ports with the lowest interface number in the stack are elected as the stack Call Server ports, until the available 8 call-server slots are configured, or all the available call-server ports from all units are elected.

This same scenario occurs for the Uplink port.

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

Call Server Ports or Uplink Ports

If ADAC is operating in either the Untagged-Frames-Advanced or Tagged-Frames operating mode and you reset the unit that provides all the Call Server and Uplink ports, the feature does not remain operational, since a minimum of one call-server or uplink port required in this mode. In this scenario, the feature temporarily disables until the unit with the Call Server and/or Uplink port(s) rejoins the stack and the configuration becomes valid again.

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

Uplink port as part of MLT in a stack

To configure the Uplink port to be part of a distributed MLT in a stack, you must first configure and enable the MLT, and then you can select one of the MLT members as the Uplink port. More ports from the same MLT cannot be configured as different uplink ports.

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 original Uplink port.

After joining the stack, the lowest Uplink port is elected as the original uplink port from the given DMLT.

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

ADAC and LACP enabled on an Uplink port

To set the Uplink port as LACP-enabled, you must first configure and enable LACP on the port, and then you can set the port as the Uplink port. You cannot set up more ports from the same LAG as different Uplink ports.

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

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

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

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

Uplink port as part of LACP in a stack

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

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

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

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

ADAC and EAP configuration

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

You can enable both ADAC and EAP on telephony ports. Users connected behind phone can be authenticated either locally, as non-EAPOL clients or by a RADIUS server as EAPOL or Non-EAPOL clients. Also Guest VLAN is allowed on ports with ADAC and EAPOL/Non-EAPOL enabled

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

- When ADAC is enabled, you cannot enable or disable EAP or EAP Multihost on the port.
- You can enable ADAC on the port only if:
    - EAP is disabled per port

      OR
    - EAP and Multihost are enabled per port

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

EAP makes its own VLAN configurations on a port, depending on whether use of Radius Assigned VLAN, Guest VLAN or Fail Open VLAN are enabled, however, the ADAC VLAN settings for the port are not removed or affected in any way. The port will remain in the voice VLAN configured for ADAC.

ADAC user restrictions

Once ADAC is enabled, you cannot:

- Delete the Voice-VLAN.
- Remove auto-configured ports from Voice-VLAN.
- View or remove any QoS setting made by ADAC (auto-configured settings).
- Set the Voice-VLAN as Management VLAN.

You can:

- Add non-ADAC ports to and remove non-ADAC ports from the Voice-VLAN. (Configuration is static.)
- Change the tagging and PVID of all non-ADAC ports in the Voice-VLAN. (Configuration is static.)
- Change the tagging and PVID of all ADAC-enabled ports in the Voice-VLAN (Configuration is dynamic.)

Disabling ADAC

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

Chapter 8: LLDP fundamentals

The information in this section provides an overview of LLDP fundamentals.

LLDP overview

Release 6.3 software supports the Link Layer Discovery Protocol (LLDP) (IEEE 802.1ab), which enables stations connected to a LAN to advertise their capabilities to each other, enabling the discovery of physical topology information for network management. LLDP-compatible stations can consist of any interconnection device including PCs, IP Phones, switches, and routers. Each LLDP station stores LLDP information in a standard Management Information Base (MIB), making it possible for a network management system (NMS) or application to access the information.

Each LLDP station:

- advertises connectivity and management information about the local station to adjacent stations on the same 802 LAN (802.3 Ethernet with 5000 Series).
- receives network management information from adjacent stations on the same LAN.

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

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

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

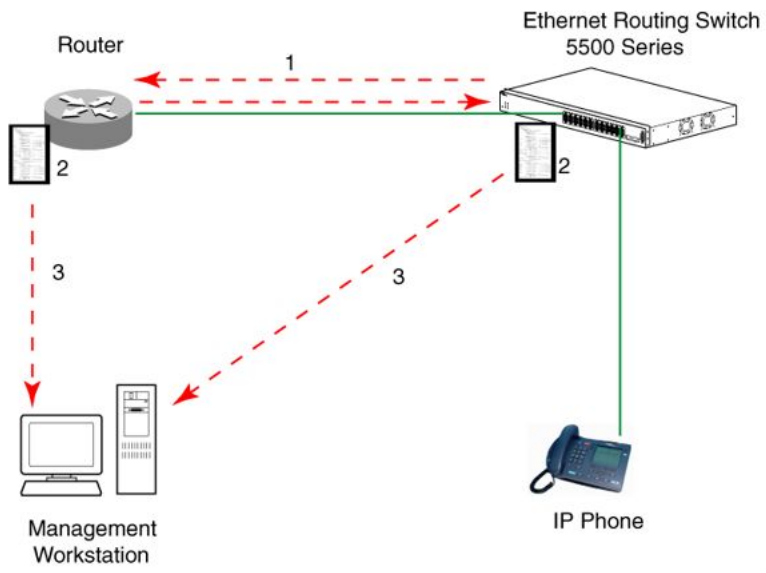


Figure 35: LLDP: how it works

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

LLDP operational modes

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

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

Connectivity and management information

The information fields in each LLDP frame are contained in a Link Layer Discovery Protocol Data Unit (LLDPDU) as a sequence of short, variable length information elements known as TLVs (type, length, value).

Each LLDPDU includes the following four mandatory TLVs:

- **Chassis ID TLV**
- **Port ID TLV**
- **Time To Live TLV**
- **End Of LLDPDU TLV**

The chassis ID and the port ID values concatenate to form a logical MSAP identifier that the recipient uses to identify the sending LLDP agent and port.

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

In addition to the four mandatory TLVs, Release 6.3 software supports the TLV extension set consisting of Management TLVs and organizationally-specific TLVs. Organizationally-specific TLVs are defined by either the professional organizations or the individual vendors that are involved with the particular functionality being implemented. You can specify which of these optional TLVs to include in the transmitted LLDPDUs for each port.

Management TLVs

The optional management TLVs are as follows:

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

IEEE 802.1 organizationally-specific TLVs

The optional IEEE 802.1 organizationally-specifc TLVs are:

- Port VLAN ID TLV contains the local port PVID.
- Port And Protocol VLAN ID TLV contains the VLAN IDs of the port and protocol VLANs that contain the local port.
- VLAN Name TLV contains the VLAN names of the VLANs that contain the local port.
- Protocol Identity TLV advertises the protocol supported. The following values are used for supported protocols on the 5000 Series:
    - Stp protocol {0x00,0x26,0x42,0x42,0x03, 0x00, 0x00, 0x00}
    - Rstp protocol string {0x00,0x27,0x42,0x42,0x03, 0x00, 0x00, 0x02}
    - Mstp protocol string {0x00,0x69,0x42,0x42,0x03, 0x00, 0x00, 0x03}
    - Eap protocol string {0x88, 0x8E, 0x01}
    - Lldp protocol string {0x88, 0xCC}

IEEE 802.3 organizationally-specific TLVs

The optional IEEE 802.3 organizationally-specifc TLVs are:

- MAC/PHY Configuration/Status TLV indicates the autonegotiation capability and the speed and duplex status of IEEE 802.3 MAC/PHYs.
- Power-Via-MDI TLV indicates the capabilities and current status of IEEE 802.3 PMDs that can provide power over twisted-pair copper links.
- Link Aggregation TLV indicates the current link aggregation status of IEEE 802.3 MACs.
- Maximum Frame Size TLV indicates the maximum supported 802.3 frame size.

Organizationally-specific TLVs for MED devices

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

- **Capabilities TLV** enables a network element to advertise the LLDP-MED TLVs it is capable of supporting.
- **Network Policy Discovery TLV** is a fixed length TLV that enables both network connectivity devices and endpoints to advertise VLAN type, VLAN identifier (VID), and Layer 2 and Layer 3 priorities associated with a specific set of applications on a port. In addition, an LLDP-MED endpoint advertises this TLV for supported application types to

enable the discovery of specific policy information and the diagnosis of network policy configuration mismatch issues.

- **Location Identification TLV** allows network connectivity devices to advertise the appropriate location identifier information for an endpoint to use in the context of location-based applications. The Location Identification Discovery extension enables the advertisement of location identifier information to Communication Endpoint Devices (Class III), based on the configuration of the Network Connectivity Device to which it is connected. This is expected to be related to wiremap or similar network topology data, such that the configuration of the Network Connectivity Device can uniquely identify the physical location of the connected MED Endpoint, and hence the correct location identifier information for it to use.
- **Extended Power-via-MDI TLV** enables advanced power management between an LLDP-MED endpoint and network connectivity devices. The Extended Power-via-MDI TLV enables the advertisement of fine grained power requirement details, endpoint power priority, and power status for both endpoint and network connectivity devices.
- **Inventory TLVs** provide switch information. The LLDP Inventory TLVs consist of the following:
    - **LLDP-MED Hardware Revision TLV** allows the device to advertise its hardware revision.
    - **LLDP-MED Firmware Revision TLV** allows the device to advertise its firmware revision.
    - **LLDP-MED Software Revision TLV** allows the device to advertise its software revision.
    - **LLDP-MED Serial Number TLV** allows the device to advertise its serial number.
    - **LLDP-MED Manufacturer Name TLV** allows the device to advertise the name of its manufacturer.
    - **LLDP-MED Model Name TLV** allows the device to advertise its model name

You can also use the **`show sys-info`** command to display information about the Inventory TLVs.

Trasmitting LLDPDUs

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

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

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

TLV system MIBs

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

LLDPDU and TLV error handling

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

Time to live interval

The Time to live interval represents the tx-interval multiplied by the tx-hold-multiplier.

Med fast start

Med fast start provides a burst of LLDPDU when the system initializes an LLDP MED transmission.

802.1AB MED network policies

You can configure 802.1AB MED network policies to dynamically configure voice VLAN, DSCP, priority, and VLAN tagging on the switch for voice traffic received from an IP phone. When you enable LLDP and configure the MED network policies on the switch, the switch sends the network policies to the IP Phone. The IP phone processes the data in the LLDP PDU and transmits the voice traffic with the appropriate VLAN ID, VLAN tagging, DSCP and priority information.

You can configure MED network policies on a switch port that has ADAC enabled. The network policies have priority over the ADAC configuration on the port.

When you enable Automatic QoS, the MED network policy is changed to DSCP 47 (0x2F) from user defined DSCP. The DSCP that is set to a value that it recognizes.

An LLDP compliant IP phone uses the received DSCP when receiving voice traffic so that the traffic is recognized by the Avaya Automatic QoS and is prioritized accordingly. This feature is automatically enabled when Avaya Automatic QoS is enabled.

802.1AB integration

802.1AB integration provides a set of LLDP TLVs for Avaya IP telephone support. You can select which Avaya IP phone support TLVs can be transmitted from individual switch ports by enabling or disabling TLV transmit flags for the port. The TLV transmit flags and TLV configuration operate independently of each other. Therefore, you must enable the transmit flag on a switch port for a specific TLV, before the port can transmit that TLV to an Avaya IP phone.

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

PoE conservation level request TLV

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

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

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

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

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

PoE conservation level support TLV

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

Call server TLV

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

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

The call server TLV supports IPv4 addresses only.

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

File server TLV

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

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

The file server TLV supports IPv4 addresses only.

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

Note:

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

802.1Q framing TLV

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

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

By default, the transmission of the 802.1Q Framing TLV is enabled for all ports.

Tagging mode for this TLV works as follows:

- If “tagged” is selected, the phone will use tagging according to the value received by the phone from the LLDP-MED Network Policy TLV.
- If “non-tagged” is selected, the phone will not tag frames with 802.1Q.
- If “auto” is selected, the phone will attempt what is present in the LLDP-MED. If that fails (no information available), it will try sending priority-tagged frames according to the configuration from the server. If that fails (no configuration for priority on the IP phone), the phone will send traffic untagged.

Phone IP TLV

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

The phone IP TLV supports IPv4 addresses only.

Chapter 9: VLAN Configuration using ACLI

Creating and Managing VLANs using the ACLI

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

This section contains information about the following topics:

Displaying VLAN information

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

Procedure steps

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

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

Variable definitions

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

Variable	Value
	• port - port-based • protocol - protocol-based (see following list)
Protocol Parameter	**Description**
protocol-ipEther2	Specifies an ipEther2 protocol-based VLAN.
protocol-ipx802.3	Specifies an ipx802.3 protocol-based VLAN.
protocol-ipx802.2	Specifies an ipx802.2 protocol-based VLAN.
protocol-ipxSnap	Specifies an ipxSnap protocol-based VLAN.
protocol-ipxEther2	Specifies an ipxEther2 protocol-based VLAN.
protocol-decEther2	Specifies a decEther2 protocol-based VLAN.
protocol-sna802.2	Specifies an sna802.2 protocol-based VLAN.
protocol-snaEther2	Specifies an snaEther2 protocol-based VLAN.
protocol-Netbios	Specifies a NetBIOS protocol-based VLAN.
protocol-xnsEther2	Specifies an xnsEther2 protocol-based VLAN.
protocol-vinesEther2	Specifies a vinesEther2 protocol-based VLAN.
protocol-ipv6Ether2	Specifies an ipv6Ether2 protocol-based VLAN.
protocol-Userdef	Specifies a user-defined protocol-based VLAN.
protocol-RarpEther2	Specifies a RarpEther2 protocol-based VLAN.

Displaying VLAN interface information

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

Procedure steps

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

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

Displaying VLAN port membership

Use the following procedure to display port memberships in VLANs.

Procedure steps

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

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

Setting the management VLAN

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

Procedure steps

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

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

Resetting the management VLAN to default

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

Procedure steps

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

```
default vlan mgmt
```

Displaying Voice VLAN information

Use this procedure to display voice VLAN information.

Procedure steps

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

   ```
   show vlan voice-vlan
   ```

Creating a VLAN

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

Procedure steps

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

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

Variable definitions

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

Variable	Value
	Note: Do not enter a value for this parameter when you are creating multiple VLANs simultaneously.
type	Enter the type of VLAN to create: • port - port-based • protocol - protocol-based (see following list) • voice-vlan - specify as a voice VLAN
protocol-ipEther2	Specifies an ipEther2 protocol-based VLAN.
protocol-ipx802.3	Specifies an ipx802.3 protocol-based VLAN.
protocol-ipx802.2	Specifies an ipx802.2 protocol-based VLAN.
protocol-ipxSnap	Specifies an ipxSnap protocol-based VLAN.
protocol-ipxEther2	Specifies an ipxEther2 protocol-based VLAN.
protocol-decEther2	Specifies a decEther2 protocol-based VLAN.
protocol-snaEther2	Specifies an snaEther2 protocol-based VLAN.
protocol-Netbios	Specifies a NetBIOS protocol-based VLAN.
protocol-xnsEther2	Specifies an xnsEther2 protocol-based VLAN.
protocol-vinesEther2	Specifies a vinesEther2 protocol-based VLAN.
protocol-Userdef <4096-65534>	Specifies a user-defined protocol-based VLAN.
protocol-ipv6Ether2	Specifies an ipv6Ether2 protocol-based VLAN.

Deleting a VLAN

Use the following procedure to delete a VLAN.

Procedure steps

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

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

Disabling a voice VLAN

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

Procedure steps

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

   ```
   no vlan <vid_list> voice-vlan
   ```

Variable definitions

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

Variable	Value
<vid_list>	Enter as an individual VLAN ID to disable a single VLAN or enter as a range or list of VLAN IDs to disable multiple VLANs simultaneously. A VLAN ID can range from 1 to 4094.
voice-vlan	Disable the specified VLAN(s) as a voice VLAN

Modifying VLAN MAC address flooding

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

Procedure steps

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

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

Configuring VLAN name

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

Procedure steps

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

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

Enabling automatic PVID

Use the following procedure to enable the automatic PVID feature.

Procedure steps

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

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

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

Configuring VLAN port settings

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

Procedure steps

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

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

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

Variable definitions

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

Configuring VLAN members

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

Procedure steps

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

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

Variable definitions

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

Configuring VLAN Configuration Control

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

VLAN Configuration Control offers four options for controlling VLAN modification:

- Strict
- Automatic
- AutoPVID
- Flexible

✱ **Note:**

The factory default setting is Strict.

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

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

Displaying VLAN Configuration Control settings

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

Procedure steps

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

```
show vlan configcontrol
```

Modifying VLAN Configuration Control settings

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

Procedure steps

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

```
vlan configcontrol <vcc_option>
```

Variable definitions

Variable	Value
<vcc_option>	This parameter denotes the VCC option to use on the switch. The valid values are: • 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. For more information about these options, refer to Configuring VLAN Configuration Control on page 153.

Managing the MAC address forwarding database table

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

The MAC flush feature is a direct way to flush MAC addresses from the MAC address table. The MAC flush commands allow flushing of:

- a single MAC address (see Removing a single address from the MAC address table on page 157)
- all addresses from the MAC address table (see Clearing the MAC address table on page 156
- a port or list of ports (see Clearing the MAC address table on a FastEthernet interface on page 157)
- a trunk (see Clearing the MAC address table on a trunk on page 157)
- a VLAN (see Clearing the MAC address table on a VLAN on page 157)

MAC flush deletes dynamically learned addresses. MAC flush commands may not be executed instantly when the command is issued. Since flushing the MAC address table is not considered an urgent task, MAC flush commands are assigned the lowest priority and placed in a queue.

The MAC flush commands are supported in ACLI, SNMP, or EDM.

Displaying MAC address forwarding table

Use the following procedure to display the current contents of the MAC address forwarding database table. You can filter the MAC Address table by port number. The MAC address table can store up to 16000 addresses.

Procedure steps

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

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

Variable definitions

Variable	Value
vid <1-4094>	Enter the number of the VLAN for which you want to display the forwarding database. Default is to display the management VLAN’s database.

Variable	Value
aging-time	Displays the time in seconds after which an unused entry is removed from the forwarding database.
address <H.H.H>	Displays a specific MAC address if it exists in the database. Enter the MAC address you want displayed.

Configuring MAC address retention

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

Procedure steps

To configure unseen MAC address retention, use the following command from Global Configuration mode.

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

Variable definitions

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

Setting MAC address retention time to default

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

Procedure steps

To set the MAC address retention time to default, use the following command from Global Configuration mode.

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

Clearing the MAC address table

Use the following procedure to clear the MAC address table.

Procedure steps

To flush the MAC address table, use the following command from Privileged EXEC mode.

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

Clearing the MAC address table on a VLAN

Use the following procedure to flush the MAC addresses for the specified VLAN.

Procedure steps

To flush the MAC address table for a specific VLAN, use the following command from Privileged EXEC mode.

```
clear mac-address-table interface vlan <vlan #>
```

Clearing the MAC address table on a FastEthernet interface

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

Procedure steps

TO clear the MAC address table on a FastEthernet interface, use the following command from Privileged EXEC mode.

```
clear mac-address-table interface FastEthernet <port-list|ALL>
```

Clearing the MAC address table on a trunk

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

Procedure steps

To clear the MAC address table on a trunk, use the following command from Privileged EXEC mode.

```
clear mac-address-table interface mlt <trunk_number>
```

Removing a single address from the MAC address table

Use the following procedure to flush one MAC address from the MAC address table.

Procedure steps

To flush a single MAC address, use the following command from Privileged EXEC mode.

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

IP Directed Broadcasting

IP directed broadcasting takes the incoming unicast Ethernet frame, determines that the destination address is the directed broadcast for one of its interfaces, and then forwards the datagram onto the appropriate network using a link-layer broadcast.

IP directed broadcasting in a VLAN forwards direct broadcast packets in two ways:

- Through a connected VLAN subnet to another connected VLAN subnet.
- Through a remote VLAN subnet to the connected VLAN subnet.

By default, this feature is disabled.

The following ACLI commands are used to work with IP directed broadcasting:

- Enabling IP directed broadcast on page 158

Enabling IP directed broadcast

Use the following procedure to enable IP directed broadcast.

Procedure steps

To enable IP directed broadcast, use the following command from Global Configuration mode.

```
[no] ip directed-broadcast enable
```

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

Chapter 10: STP Configuration using the ACLI

Setting the STP mode using the ACLI

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

Procedure steps

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

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

Configuring STP BPDU Filtering using the ACLI

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

Procedure steps

1. To enable STP BPDU filtering, use the following command from Interface Configuration mode.

   ```
   [no] spanning-tree bpdu-filtering [port <portlist>] [enable]
   [timeout <10-65535 | 0> ]
   ```

   Use the no form of this command to disable.

2. To set the STP BPDU Filtering properties on a port to their default values, use the following command from the Interface Configuration command mode:

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

3. To show the current status of the BPDU Filtering parameters, use the following command from the Privileged EXEC mode:

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

Variable definitions

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

Creating and Managing STGs using the ACLI

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

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

To configure STGs using the ACLI, refer to the following:

Configuring path cost calculation mode

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

Procedure steps

To configure path cost calculation mode, use the following command from Privileged EXEC mode.

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

Configuring STG port membership mode

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

Procedure steps

To configure STG port membership mode, use the following command from Privileged EXEC mode.

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

Displaying STP configuration information

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

Procedure steps

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

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

Variable definitions

Variable	Value
stp <1-8>	Displays specified Spanning Tree Group configuration; enter the number of the group to be displayed.

Variable	Value
config | port | port-mode | vlans	Displays spanning tree configuration for: • config--the specified (or default) Spanning Tree Group • port--the ports within the Spanning Tree Group • port-mode--the port mode • vlans--the VLANs that are members of the specified Spanning Tree Group

Creating a Spanning Tree Group

Use the following procedure to create a Spanning Tree Group.

Procedure steps

To create a Spanning Tree Group, use the following command from Global Configuration mode.

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

Deleting a Spanning Tree Group

Use the following procedure to delete a Spanning Tree Group.

Procedure steps

To delete a Spanning Tree Group, use the following command from Global Configuration mode.

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

Enabling a Spanning Tree Group

Use the following procedure to enable a Spanning Tree Group.

Procedure steps

To enable a Spanning Tree Group, use the following command from Global Configuration mode.

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

Disabling a Spanning Tree Group

Use the following procedure to disable a Spanning Tree Group.

Procedure steps

To disable a Spanning tree Group, use the following command from Global Configuration mode.

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

Configuring STP values

Use the following procedure to set STP values by STG.

Procedure steps

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

```
spanning-tree [stp <1-8>] [forward-time <4-30>] [hello-time
<1-10>] [max-age <6-40>] [priority {0*0000 | 0*1000| 0*2000 |
0*3000 | ... | 0*E000 | 0*F000}] [tagged-bpdu {enable |
disable}] [tagged-bpdu-vid <1-4094>] [multicast-address
<H.H.H>] [add-vlan] [remove-vlan]
```

Variable definitions

Variable	Value
stp <1-8>	Specifies the Spanning Tree Group; enter the STG ID.

Variable	Value
forward-time <4-30>	Enter the forward time of the STG in seconds; the range is 4 -- 30, and the default value is 15.
hello-time <1-10>	Enter the hello time of the STG in seconds; the range is 1 --10, and the default value is 2.
max-age <6-40>	Enter the max-age of the STG in seconds; the range is 6 -- 40, and the default value is 20.
priority {0x000 | 0x1000 | 0x2000 | 0x3000 | .... | 0xE000 | 0xF000}	Sets the spanning tree priority (in Hex); if 802.1T compliant, this value must be a multiple of 0x1000.
tagged-bpdu {enable | disable}	Sets the BPDU as tagged or untagged. The default value for Spanning Tree Group 1 (default group) is untagged; the default for the other groups is tagged.
tagged-bpdu-vid <1-4094>	Sets the VLAN ID (VID) for the tagged BPDU. The default value is 4001 -- 4008 for STG 1 -- 8, respectively.
multicast-address <H.H.H>	Sets the spanning tree multicast address.
add-vlan	Adds a VLAN to the Spanning Tree Group.
remove-vlan	Removes a VLAN from the Spanning Tree Group.

Restoring default Spanning Tree values

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

Procedure steps

To restore Spanning Tree values to default, use the following command from Global Configuration mode.

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

Variable definitions

Variable	Value
stp <1-8>	Disables the Spanning Tree Group; enter the STG ID.

Variable	Value
forward-time	Sets the forward time to the default value of 15 seconds.
hello-time	Sets the hello time to the default value of 2 seconds.
max-age	Sets the maximum age time to the default value of 20 seconds.
priority	Sets spanning tree priority (in Hex); if 802.1T compliant, this value must be a multiple of 0x1000.
tagged-bpdu	Sets the tagging to the default value. The default value for Spanning Tree Group 1 (default group) is untagged; the default for the other groups is tagged.
multicast address	Sets the spanning tree multicast MAC address to the default.

Adding a VLAN to a STG

Use the following procedure to add a VLAN to a specified Spanning Tree Group.

Procedure steps

To add a VLAN to a STG, use the following command from Global Configuration mode.

```
spanning-tree [stp <1-8>] add-vlan <1-4094>
```

Removing a VLAN from a STG

Use the following procedure to remove a VLAN from a specified Spanning Tree Group.

Procedure steps

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

```
spanning-tree [stp <1-8>] remove-vlan <1-4094>
```

Configuring STP and MSTG participation

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

Procedure steps

To configure STP and MSTG participation, use the following command from Interface Configuration mode.

```
[no] spanning-tree [port <portlist>] [stp <1-8>] [learning
{disable | normal | fast}] [cost <1-65535>] [priority]
```

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

Variable definitions

Variable	Value
port <portlist>	Enables the spanning tree for the specified port or ports; enter port or ports you want enabled for the spanning tree. **Note:** If you omit this parameter, the system uses the port number you specified when you issued the interface command to enter the Interface Configuration mode.
stp <1-8>	Specifies the spanning tree group; enter the STG ID.
learning {disable|normal|fast}	Specifies the STP learning mode: • 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 1 -- 65535.
priority	Sets the spanning tree priority for a port as a hexadecimal value. If the Spanning Tree Group is 802.1T compliant, this value must be a multiple of 0x10.

Resetting Spanning Tree values for ports to default

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

Procedure steps

To reset Spanning Tree values to default, use the following command from Interface Configuration mode.

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

Variable definitions

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

Managing RSTP using the ACLI

Use the following command to configure RSTP:

Configuring RSTP parameters

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

Procedure steps

To configure RSTP parameters, use the following command from Global Configuration mode.

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

Variable definitions

Variable	Value
forward-time <4- 30>	Sets the RSTP forward delay for the bridge in seconds; the default is 15.
hello-time <1- 10>	Sets the RSTP hello time delay for the bridge in seconds; the default is 2.
max-age <6 - 40>	Sets the RSTP maximum age time for the bridge in seconds; the default is 20.
pathcost-type {bits16 | bits32}	Sets the RSTP default path cost version; the default is bits32.
priority {0000 | 1000 | ... | F000}	Sets the RSTP bridge priority (in hex); the default is 8000.
tx-hold count	Sets the RSTP Transmit Hold Count; the default is 3.
version {stp-compatible | rstp}	Sets the RSTP version; the default is rstp.

Configuring RSTP on a port

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

Procedure steps

To configure RSTP on a port, use the following command from Interface Configuration mode.

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

Variable definitions

Variable	Value
port <portlist>	Filter on list of ports.
cost <1 - 200000000>	Sets the RSTP path cost on the single or multiple ports; the default is 200000.
edge-port {false | true}	Indicates whether the single or multiple ports are assumed to be edge ports. This parameter sets the Admin value of edge port status; the default is false.
learning {disable | enable}	Enables or disables RSTP on the single or multiple ports; the default is enable.
p2p {auto | force-false | force-true}	Indicates whether the single or multiple ports are to be treated as point-to-point links. This command sets the Admin value of P2P Status; the default is force-true.
priority {00 | 10 |... | F0}	Sets the RSTP port priority on the single or multiple ports; the default is 80.
protocol-migration {false | true}	Forces the single or multiple port to transmit RSTP BPDUs when set to true, while operating in RSTP mode; the default is false.

Displaying RSTP configuration

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

Procedure steps

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

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

Variable definitions

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

Displaying RSTP port configuration

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

Procedure steps

To display RSTP port configuration, use the following command from Privileged EXEC mode.

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

Variable definitions

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

Managing MSTP using the ACLI

Use the following procedures to manage MSTP using the ACLI:

Configuring MSTP parameters

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

Procedure steps

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

```
spanning-tree mstp [max-hop <600 - 4000>] [forward-time <4 -
30>] [max-age <6 - 40>] [pathcost-type {bits16 | bits32}]
[priority {0000 | 1000 | 2000 | ... | F000}] [tx-hold count <1
- 10>] [version {stp-compatible | rstp| mstp}] [add-vlan <1 -
4094>] [remove-vlan <1 - 4094>]
```

Variable definitions

Variable	Value
max-hop <600 - 4000>	Sets the MSTP maximum hop count for the CIST bridge; the default is 2000.
forward-time <4 - 30>	Sets the MSTP forward delay for the CIST bridge in seconds; the default is 15.
max-age <6 - 40>	Sets the MSTP maximum age time for the CIST bridge in seconds; the default is 20.
pathcost-type {bits16 | bits32}	Sets the MSTP default path cost version; the default is bits32.
priority {0000 | 1000| 2000 ... | F000}	Sets the MSTP bridge priority for the CIST Bridge; the default is 8000.
tx-holdcount<1 - 10>	Sets the MSTP Transmit Hold Count; the default is 3.
version {stp-compatible | rstp | mstp}	Sets the MSTP version for the Cist Bridge; the default is mstp.
add-vlan <1 - 4094>	Adds a VLAN to the CIST bridge.
remove-vlan <1 - 4094>	Removes the specified VLAN from the CIST bridge.

Configuring MSTP on a port

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

Procedure steps

To configure MSTP on a port, use the following command from Interface Configuration mode.

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

```
[priority {00 | 10 | < | F0}] [protocol-migration {false |
true}]
```

Variable definitions

Variable	Value
port <portlist>	Enter a list or range of port numbers.
cost <1 - 200000000>	Sets the MSTP path cost on the single or multiple ports for the CIST; the default is 200000.
hello-time <1 - 10>	Sets the MSTP hello time on the single or multiple ports for the CIST; the default is 2.
edge-port {false | true}	Indicates whether the single or multiple ports are assumed to be edge ports. This parameter sets the Admin value of edge port status; the default is false.
learning {disable | enable}	Enables or disables MSTP on the single or multiple ports; the default is enable.
p2p {auto | force-false | force-true}	Indicates whether the single or multiple ports are treated as point-to-point links. This command sets the Admin value of P2P Status; the default is force-true.
priority {00 | 10 |... | F0}	Sets the MSTP port priority on the single or multiple ports; the default is 80.
protocol-migration {false | true}	Forces the single or multiple ports to transmit MSTP BPDUs when set to true, while operating in MSTP mode; the default is false.

Configuring MSTP region parameters

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

Procedure steps

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

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

Variable definitions

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

Configuring MSTP parameters

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

Procedure steps

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

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

Variable definitions

Variable	Value
<1 - 7>	Filter on MSTP instance.
priority {0000 | 1000 |... | F000}	Sets the MSTP priority for the bridge instance; the default is 8000.
add-vlan <1 - 4094>	Maps the specified VLAN and MSTP bridge instance.
remove-vlan <1 - 4094>	Unmaps the specified VLAN and MSTP bridge instance.
map-vlans	Map VLANs in the list to MSTP instance.
enable	Enables the MSTP bridge instances.

Disabling a MSTP bridge instance

Use the following procedure to disable a MSTP bridge instance.

Procedure steps

To disable a MSTP bridge instance, use the following command from Global Configuration mode.

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

Deleting a MSTP bridge instance

Use the following procedure to delete a MSTP bridge-instance.

Procedure steps

To delete a MSTP bridge instance, use the following command from Global Configuration mode.

```
no spanning-tree mstp msti <1 - 7>
```

Displaying MSTP status

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

Procedure steps

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

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

Variable definitions

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

Displaying MSTP Cist port information

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

Procedure steps

To display MSTP Cist port information, use the following command from Privileged EXEC mode.

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

Variable definitions

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

Displaying MSTP MSTI settings

Use the following procedure to display MSTP MSTI settings.

Procedure steps

To display MSTP MSTI settings, use the following command from Global Configuration mode.

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

Variable definitions

Variable	Value
config	Displays the MSTP instance-specific configuration and the VLAN mapping port.
statistics	Displays MSTP instance-specific statistics.
port {config | role | statistics}	Displays MSTP instance-specific port information: • config: displays MSTI port configuration • role: displays MSTI port role information • statistics: displays MSTI port statistics
<1 - 7>	Specifies the MSTI instance for which to display the statistics.

Chapter 11: MLT Configuration using the ACLI

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

Displaying MLT configuration and utilization

Use the following procedure to display Multi-Link Trunking (MLT) configuration and utilization.

Procedure steps

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

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

Job aid: show mlt command output

The following figure displays sample output for the show mlt command.

```
5698TFD-PWR(config)#sh mlt

Id Name         Members       Bpdu   Mode     Status    Type
-- ------------ ------------- ------ -------- --------  ------
1  Trunk #1     NONE          All    Basic    Disabled
2  Trunk #2     81-82,89-90   All    Advance  Enabled   Trunk
3  Trunk #3     NONE          All    Basic    Disabled
4  Trunk #4     NONE          All    Basic    Disabled
5  Trunk #5     91-92         All    Advance  Enabled   Trunk
6  Trunk #6     NONE          All    Basic    Disabled
7  Trunk #7     NONE          All    Basic    Disabled
8  Trunk #8     67-68         All    Advance  Enabled   Trunk
9  Trunk #9     NONE          All    Basic    Disabled
10 Trunk #10    NONE          All    Basic    Disabled
11 Trunk #11    NONE          All    Basic    Disabled
12 Trunk #12    NONE          All    Basic    Disabled
13 Trunk #13    NONE          All    Basic    Disabled
14 Trunk #14    95-96         All    Advance  Enabled   Trunk
15 Trunk #15    NONE          All    Basic    Disabled
```

```
16 Trunk #16    NONE          All    Basic    Disabled
17 Trunk #17    NONE          All    Basic    Disabled
18 Trunk #18    NONE          All    Basic    Disabled
19 Trunk #19    NONE          All    Basic    Disabled
20 Trunk #20    7-8           All    Advance  Enabled   Trunk
21 Trunk #21    93-94         All    Advance  Enabled   Access
22 Trunk #22    NONE          All    Basic    Disabled
23 Trunk #23    NONE          All    Basic    Disabled
24 Trunk #24    11-12         All    Advance  Enabled   Trunk
25 Trunk #25    75-76         All    Advance  Enabled   Trunk
26 Trunk #26    NONE          All    Basic    Disabled
27 Trunk #27    NONE          All    Basic    Disabled
28 Trunk #28    NONE          All    Basic    Disabled
29 Trunk #29    NONE          All    Basic    Disabled
30 Trunk #30    NONE          All    Basic    Disabled
31 Trunk #31    NONE          All    Basic    Disabled
32 Trunk #32    NONE          All    Advance  Disabled
```

Configuring a Multi-Link trunk

Use the following procedure to configure a Multi-Link trunk (MLT).

Procedure steps

To configure a Multi-Link trunk, use the following command from Global Configuration mode.

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

Variable definitions

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

Variable	Value
loadbalance {basic | advance}	Sets the MLT load-balancing mode: - basic: MAC-based load-balancing - advance: IP-based load-balancing

Disabling an MLT

Use the following procedure to disable a Multi-Link trunk (MLT).

Procedure steps

1. To disable an MLT, clearing all port members, use the following command from Global Configuration mode:

   ```
   no mlt [<id>]
   ```

2. To disable an MLT without clearing all port members, use the following command from Global Configuration mode:

   ```
   mlt [<id>] disable
   ```

Displaying MLT properties

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

Procedure steps

To display MLT properties, use the following command from Global Configuration mode.

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

Displaying IP address-based MLT load-balance link calculation

Use this procedure to display MLT hashing information for specific source and destination IP addresses for IP address-based MLTs.

Procedure steps

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

   ```
   show mlt hash-calc <1-32> destination-ip <dest-ip-addr>
   source-ip <src-ip-addr>
   ```

Variable definitions

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

Variable	Value
<1–32>	Specifies the MLT ID.
destination <dest-ip-addr>	Specifies the destination IP address.
source-ip <src—ip-addr>	Specifies the source IP address.

Displaying MAC address-based MLT load-balance link calculation

Use this procedure to display MLT hashing information for specific source and destination IP addresses for MAC address-based MLTs.

Procedure steps

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

   ```
   show mlt hash-calc <1-32> destination-mac <dest-mac-addr>
   source-ip <src-mac-addr>
   ```

Variable definitions

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

Variable	Value
<1–32>	Specifies the MLT ID.
destination <dest-mac-addr>	Specifies the destination MAC address.
source <dest-mac-addr>	Specifies the source MAC address.

Configuring MLT port shutdown when MLT is disabled

The commands listed in following section allow you to enable or disable the shutdown on MLT ports when MLT is disabled.

Enabling shutdown on MLT ports when MLT is disabled

Use the following procedure to enable MLT port shutdown:

Procedure steps

1. Log on to the Global Configuration Mode in ACLI
2. Enter the following command at the command prompt:

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

Variable definitions

Variable	Value
[enable]	Enables the trunk loop prevention on the port.

Disabling MLT port shutdown when MLT is disabled

Use the following procedure to disable a shutdown on MLT ports when MLT is disabled..

Procedure steps

1. Log on to the Global Configuration Mode in ACLI.
2. Enter the following command at the command prompt:

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

Setting default value to the MLT port shutdown when MLT is disabled

Use the following procedure to set the default value to the MLT port shutdown when MLT is disabled.

Procedure steps

1. Log on to the Global Configuration Mode in ACLI.
2. Enter the following command:

   ```
   default mlt shutdown-ports-on-disable
   ```

Displaying the MLT port shutdown status when MLT is disabled

Use the following procedure to display the status of MLT port shutdown when MLT is disabled.

Procedure steps

1. Log on to the PRIV EXEC Mode in ACLI.
2. Enter the following command at the command prompt:

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

Configuring STP participation for MLTs

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

Procedure steps

To configure STP participation for MLTs, use the following command from Global Configuration mode.

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

Variable definitions

Variable	Value
<1 - 32>	Specifies the ID of the MLT to associate with the STG.
stp <1 - 8>	Specifies the spanning tree group.
learning {disable | normal | fast}	Specifies the STP learning mode: • disable -- disables learning • normal -- sets the learning mode to normal • fast -- sets the learning mode to fast

Configuring SMLT using the ACLI

To configure SMLT using the ACLI, refer to the following:

Note:

To configure SMLT on the 5000 Series switch, an Advanced License must be purchased that allows this feature to be used.

Setting command mode to MLT Interface mode

Important:

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

Use the following procedure to set ACLI command mode to MLT Interface mode from which you can configure SMLTs and ISTs.

Note:

You create SLTs from the config-if command mode. For details, see Creating a SLT on a port on page 187.

Procedure steps

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

```
interface mlt [<1-32>]
```

Creating a SMLT

Important:

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

Use the following procedure to create a SMLT from an existing MLT.

Procedure steps

To create a SMLT, use the following command from Interface Configuration mode.

```
smlt <1-32>
```

Note:

Before you can create an SMLT, you must first create and enable an MLT (see Configuring a Multi-Link trunk on page 180).

Creating a IST

Important:

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

Use the following procedure to create a IST from an existing MLT.

Procedure steps

To create a IST, use the following command from MLT Interface Configuration mode.

```
ist [enable] [peer-ip <A.B.C.D>] [vlan <1-4096>]
```

The peer IP address is the IP address of the IST VLAN on the peer aggregation switch. A VLAN created on the redundant aggregation switch must also be created on the second aggregation switch. The IST treats the two switches as a single switch. To allow the two switches to communicate, you must assign an IP address to both VLANs.

Variable definitions

Variable	Value
enable	Enables the IST on the MLT specified by the interface mlt command.
vlan <1-4096>	Specifies a VLAN ID for the IST.
peer-ip <A.B.C.D>	Specifies the peer IP address for the IST.

Creating a SLT on a port

Important:

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

Use the following procedure to create a SLT on a port.

Procedure steps

To create a SLT on a port, use the following command from Interface Configuration mode.

```
smlt [port <portlist>] <1-512>
```

Variable definitions

Variable	Value
port <portlist>	Specifies the port to configure as an SLT.
<1-512>	Specifies the ID for the SLT.

Disabling SMLT

Use the following procedure to disable a SMLT.

Procedure steps

To disable a SMLT, use the following command from Interface Configuration mode.

```
no smlt <1-32>
```

Disabling IST

Use the following procedure to disable a IST and clear the IST settings.

Procedure steps

To disable a IST, use the following command from Interface Configuration mode.

```
no ist [enable] [peer-ip]
```

Variable definitions

Variable	Value
enable	Disables the IST on the MLT specified by the interface mlt command.
vlan <1-4096>	Clears the VLAN ID from the IST.
peer-ip <A.B.C.D>	Clears the peer IP address from the IST.

Disabling a SLT on a port

Use the following procedure to disable a SLT on a port.

Procedure steps

To disable a SLT on a port, use the following command from Interface Configuration mode.

```
no smlt [port <portlist>]
```

Resetting SMLT to default

Use the following procedure to reset a SMLT to default.

Procedure steps

To reset a SMLT to default, use the following command from Interface Configuration mode.

```
default smlt <1-32>
```

Resetting a IST to default

Use the following procedure to reset a IST to default settings.

Procedure steps

To reset a IST to default settings, use the following command from MLT Interface Configuration mode.

```
default ist [enable] [peer-ip]
```

Variable definitions

Variable	Value
enable	Disables the IST on the MLT specified by the interface mlt command.
peer-ip <A.B.C.D>	Clears the peer IP address from the IST.

Resetting a SMLT to default

Use the following procedure to reset SLT settings on a port to default.

Procedure steps

To reset a SMLT to default, use the following command from Interface Configuration mode.

```
default smlt [port <portlist>] <1-512>
```

Displaying IST parameters

Use the following procedure to display the IST parameters on the switch.

Procedure steps

To display IST parameters, use the following command from Privileged EXEC mode.

```
show ist
```

Displaying IST statistics

Use the following procedure to display IST statistics on the switch.

Procedure steps

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

```
show ist stat
```

Displaying SLT and SMLT configurations

Use the following procedure to display SMLT and SLT configurations on the switch.

Procedure steps

To display SLT and SMLT configurations, use the following command from Interface Configuration mode.

```
show smlt [<interface-type>]
```

Variable definitions

Variable	Value
<interface-type>	Interface types are • mlt: Displays only the MLT-based SMLTs mlt id <1-32> • fastethernet: Displays only the SLTs slt-id <1-512>

Configuring SLPP using the ACLI

This section provides procedures used to configure Simple Loop Prevention Protocol (SLPP) using the ACLI.

Configuring SLPP transmitting list

Use the following procedures to add a VLAN to the SLPP transmitting list.

Procedure steps

To add a VLAN to the SLPP transmitting list, use the following command from Global Configuration mode:

```
[no] slpp vid <1-4095>
```

Use the **no** form of this command to remove a VLAN from the list.

Enabling SLPP

Use the following procedure to globally enable SLPP.

Procedure steps

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

```
[no] slpp enable
```

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

Configuring SLPP PDU transmit interval

Use the following procedure to configure the SLPP PDU transmit interval in milliseconds. The default setting is 500 ms.

Procedure steps

To configure the SLPP PDU transmit interval, use the following command from Global Configuration mode:

```
slpp tx-interval <500-5000>
```

Configuring SLPP PDU ether type

Use the following procedure to configure the SLPP PDU ether type value. The default value is 0x8104.

Note:

Values 0x0000 and 0x8100 are disallowed.

Procedure steps

To configure the SLPP ether type value, use the following command from Global Configuration mode:

```
slpp ethertype <0x0 - 0xffff>
```

Configuring SLPP port auto enable

Use the following procedure to configure the auto enable timer for ports shut down by SLPP. If the timeout value is 0 (not active), the port will remain disabled until manually enabled by the user. The default value is 0.

Procedure steps

To configure the auto enable timer, use the following command from Global Configuration mode:

```
slpp timeout <1-65535>
```

Enabling SLPP PDU receive function per port

Use the following procedure to enable the SLPP PDU received function on a port.

Procedure steps

To enable the SLPP PDU received function, use the following command from Global Configuration mode:

```
[no] slpp [port-portList] [packet-rx <enable>]
```

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

Configuring the SLPP PDU receipt threshold

Use the following procedure to configure the number of SLPP PDUs, in the range 1 to 500, that must be received prior to shutting down a port as a result of looping. The default threshold is 5.

Procedure steps

To configure the SLPP PDU receipt threshold, use the following command from Global Configuration mode:

```
[no] slpp [port-portList] [1-500 <enable>]
```

Use the **no** form of this command to reset to default (1).

Configuring SLPP Guard using ACLI

This section provide the procedures to configure Simple Loop Prevention Protocol (SLPP) Guard using the ACLI.

Selecting an SLPP Guard Ethernet type using ACLI

You can 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 <0x0600-0xffff>
   ```

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

   ```
   default slpp-guard ethertype
   ```

Variable definitions

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

Configuring SLPP Guard using ACLI

Use this procedure to configure SLPP Guard for switch ports.

Prerequisites

Log on to the FastEthernet Interface Configuration mode in ACLI.

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. ✱ **Note:** The default value for SLPP-guard Ethernet type is: 0x8102.
[enable]	Enables 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-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.
[no]	Disables SLPP Guard parameters for a port or list of ports. ✱ **Note:** If you use no slpp-guard without parameters (enable or timeout), both settings are disabled, i.e.

Variable	Value
	slpp-guard is disabled and the timeout set to 0 on the specified port(s).

Viewing the SLPP Guard status using ACLI

You can 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

You can view the SLPP Guard configuration status by using the following command:

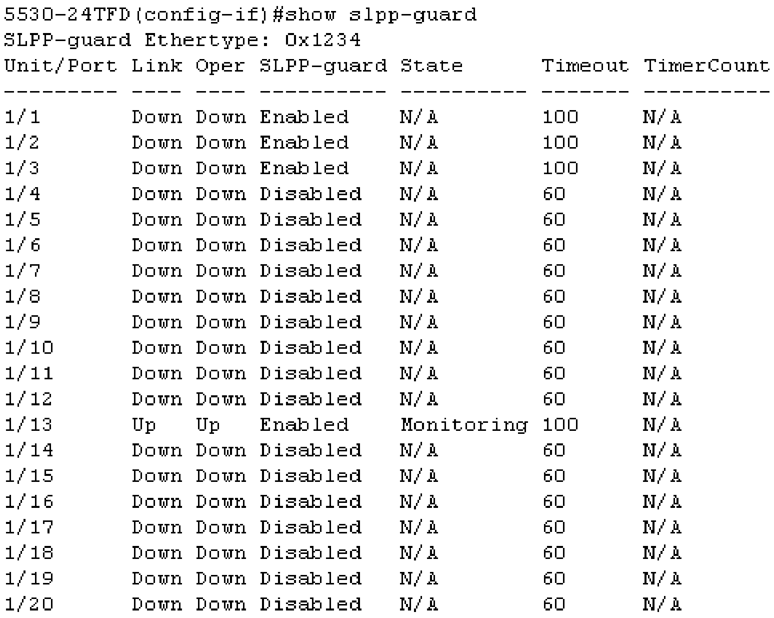
```
show slpp-guard [<portlist>]
```

Variable definitions

Variable	Value
<portlist>	Specifies a list of ports for which to display the SLPP Guard configuration status. If no ports are specified, the configuration status for all ports is displayed.

Job aid: show slpp-guard command output

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



```
5530-24TFD(config-if)#show slpp-guard
SLPP-guard Ethertype: 0x1234
Unit/Port Link Oper SLPP-guard State      Timeout TimerCount
--------- ---- ---- ---------- ---------- ------- ----------
1/1       Down Down Enabled    N/A        100     N/A
1/2       Down Down Enabled    N/A        100     N/A
1/3       Down Down Enabled    N/A        100     N/A
1/4       Down Down Disabled   N/A        60      N/A
1/5       Down Down Disabled   N/A        60      N/A
1/6       Down Down Disabled   N/A        60      N/A
1/7       Down Down Disabled   N/A        60      N/A
1/8       Down Down Disabled   N/A        60      N/A
1/9       Down Down Disabled   N/A        60      N/A
1/10      Down Down Disabled   N/A        60      N/A
1/11      Down Down Disabled   N/A        60      N/A
1/12      Down Down Disabled   N/A        60      N/A
1/13      Up   Up   Enabled    Monitoring 100     N/A
1/14      Down Down Disabled   N/A        60      N/A
1/15      Down Down Disabled   N/A        60      N/A
1/16      Down Down Disabled   N/A        60      N/A
1/17      Down Down Disabled   N/A        60      N/A
1/18      Down Down Disabled   N/A        60      N/A
1/19      Down Down Disabled   N/A        60      N/A
1/20      Down Down Disabled   N/A        60      N/A
```

The following example displays sample output of ports disabled by slpp-guard.

```
5698TFD-PWR (config)#sh slpp-guard 1/31,1/61,2/15,2/86,3/21
SLPP-guard Ethertype: 0xefef
Unit/Port Link Oper SLPP-guard State      Timeout TimerCount
--------- ---- ---- ---------- ---------- ------- ----------
1/31      Down Down Enabled    Blocking   300     218
1/61      Down Down Enabled    Blocking   300     205
2/15      Down Down Enabled    Blocking   300     46
2/86      Down Down Enabled    Blocking   300     46
3/21      Down Down Enabled    Blocking   300     18
```

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.

Link Aggregation Control Protocol over SMLT using the ACLI

These sections describe commands that assist in the configuration of Link Aggregation Control Protocol (LACP) over SMLT. For more information about the procedure to configure LACP over SMLT, see LACP over SMLT configuration example on page 397.

Configuring an SMLT MAC address

Use the following procedure to configure the SMLT MAC address.

Prerequisites

- Configure an SMLT. For more information, see Creating a SMLT on page 186.

Procedure steps

To set the SMLT MAC address, use the following command in Interface Configuration mode:

`lacp smlt-sys-id`*<H.H.H>*

Important:

For information about how to use this command in the procedure to configure LACP over SMLT, see LACP over SMLT configuration example on page 397.

Variable definitions

The following table defines parameters for the **`lacp smlt-sys-id <H.H.H>`** command.

Variable	Value
<H.H.H>	Sets the SMLT MAC address.

Configuring the default SMLT MAC address

Use the following procedure to configure the default SMLT MAC address to return to the MAC address of the switch.

Procedure steps

To configure the default SMLT MAC address, use the following command in Interface Configuration mode:

```
default lacp smlt-sys-id
```

Binding an MLT group to an administrative key and to an SMLT

Use the following procedure y to bind an MLT group to an administrative key and to an SMLT.

Prerequisites

- Configure an SMLT. For more information, see Creating a SMLT on page 186.
- Assign an administrative key to selected ports. For more information, see Configuring the LACP administrative key on page 206
- Enable LACP on the selected ports. For more information, see Configuring LACP operating mode on page 207.

Procedure steps

To bind an MLT group to an administrative key and to an SMLT, use the following command in Global Configuration mode:

```
lacp key <1-4095> mlt <1-32> smlt <1-512>
```

! **Important:**

For more information about how to use this command in the procedure to configure LACP over SMLT, see LACP over SMLT configuration example on page 397.

Variable definitions

The following table defines parameters that you can use to Bind an MLT group to an administrative key and to an SMLT.

Variable	Value
<1-4095>	Sets the administrative key value in the range of 1 to 4095.
mlt <1-32>	Sets the ID of the MLT in the range of 1–32.
smlt <1-512>	Sets the ID of the SMLT in the range of 1–512.

Freeing an MLT group

Use the following procedure to free an MLT group from an administrative key and from an SMLT.

Procedure steps

To free an MLT group from an administrative key and from an SMLT, use the following command in Global Configuration mode:

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

Variable definitions

The following table defines optional parameters that you can use to free an MLT group from an administrative key and from an SMLT.

Variable	Value
<1-4095>	Sets the administrative key value in the range of 1 to 4095

Troubleshooting IST problems

Use the following procedure to troubleshooting IST problems and single-user problems.

Procedure steps

1. Ensure that Global IP Routing is enabled.
2. Ensure that peers can ping each other.
3. Enter the `show ist stat` command to display the IST message count.

   The hello count should increment.
4. Enter the `show mlt` command to display all the MLTs in the switch and their properties, including running type, members, and status. Check the SMLT/SLT numbering: switches connected by SMLT must have the same SMLT IDs.
5. Ensure that the IST is up and running by using the `show ist` command.

6. If the IST is not running, ensure that:
    a. The correct VLAN ID exists on both sides of the IST
    b. The IST configuration contains the correct local and peer IP addresses
7. If IST is running, check whether the SMLT port is operating by using the `show smlt` command.
    a. If the current type is SMLT, the status is correct.
    b. If the current type is NORMAL, the link is running in a normal (single) mode and not in SMLT mode. The reasons for this can be as follows:
        - The remote SMLT link is not operational.
        - The ID is not configured on the other switch. To determine this, check to see whether the SMLT IDs match.
        - The IST is not up and running.

Chapter 12: LACP and VLACP Configuration using the ACLI

This section contains information on the following topics:

Configuring Link Aggregation using the ACLI

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

To configure Link Aggregation using the ACLI, refer to the following:

Displaying LACP system settings

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

Procedure steps

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

```
show lacp system
```

Displaying LACP per port configuration

Use the following procedure to display information on the per-port LACP configuration. Select ports either by port number or by aggregator value.

Procedure steps

To display per port configuration, use the following command from Privileged EXEC mode.

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

Variable definitions

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

Displaying LACP port mode

Use the following procedure to display the current port mode (default or advanced).

Procedure steps

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

```
show lacp port-mode
```

Displaying LACP port statistics

Use the following procedure to displayLACP port statistics. Select ports either by port number or by aggregator value.

Procedure steps

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

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

Variable definitions

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

Clearing LACP port statistics

Use the following procedure to clear existing LACP port statistics.

Procedure steps

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

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

Displaying LACP port debug information

Use the following procedure to display port debug information.

Procedure steps

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

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

Displaying LACP aggregators

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

Procedure steps

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

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

Configuring LACP system priority

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

Procedure steps

To configure system priority, use the following command from Global Configuration mode.

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

Enabling LACP port aggregation mode

Use the following procedure to enable the port aggregation mode.

Procedure steps

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

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

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

Configuring the LACP administrative key

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

Procedure steps

To set the administrative key, use the following command from Interface Configuration mode.

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

Variable definitions

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

Configuring LACP operating mode

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

Procedure steps

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

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

Variable definitions

Variable	Value
port <portList>	The ports for which the LACP mode is to be set.
{active | passive | off}	The type of LACP mode to set for the port. The LACP modes are: • active -- The port will participate as an active Link Aggregation port. Ports in active mode send LACPDUs periodically to the other end to negotiate for link aggregation. • passive -- The port will participate as a passive Link Aggregation port. Ports in passive mode send LACPDUs only when the configuration is changed or when its link partner communicates first. • off -- The port does not participate in Link Aggregation. LACP requires at least one end of each link to be in active mode.

Configuring per port LACP priority

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

Procedure steps

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

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

Variable definitions

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

Configuring LACP periodic transmission timeout interval

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

Procedure steps

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

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

Variable definitions

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

Configuring LACP port mode

Use the following procedure to configure the LACP port mode on the switch.

Procedure steps

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

```
lacp port-mode {default | advance}
```

Variable definitions

Variable	Value
default	Default LACP port mode.
advance	Advanced LACP port mode.

Configuring VLACP using the ACLI

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

Note:

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

Enabling VLACP globally

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

Procedure steps

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

```
[no] vlacp enable
```

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

Configuring VLACP multicast MAC address

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

Procedure steps

To configure the multicast MAC address, use the following command from Global Configuration mode.

```
[no] vlacp macaddress <macaddress>
```

Use the **no** form of this command to delete the address.

Configuring VLACP port parameters

Use the following procedure to configure VLACP parameters on a port.

Procedure steps

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

```
[no] vlacp port <slot/port> [enable | disable] [timeout <long/
short>] [fast-periodic-time <integer>] [slow-periodic-time
<integer>] [timeout-scale <integer>] [funcmac-addr <mac>]
[ethertype <hex>]
```

Use the **no** form of this command to remove parameters.

Variable definitions

Variable	Value
<slot/port>	Specifies the slot and port number.
enable|disable	Enables or disables VLACP.
timeout <long/short>	Specifies whether the timeout control value for the port is a long or short timeout. • long sets the port timeout value to: (timeout-scale value) × (slow-periodic-time value). • short sets the port's timeout value to: (timeout-scale value) × (fast-periodic-time value). For example, if the timeout is set to short while the timeout-scale value is 3 and the fast-periodic-time

Variable	Value
	value is 400 ms, the timer expires after 1200 ms. Default is long.
fast-periodic-time <integer>	Specifies the number of milliseconds between periodic VLACPDU transmissions using short timeouts. The range is 400-20000 milliseconds. Default is 500.
slow-periodic-time <integer>	Specifies the number of milliseconds between periodic VLACPDU transmissions using long timeouts. The range is 10000-30000 milliseconds. Default is 30000.
timeout-scale <integer>	Sets a timeout scale for the port, where timeout = (periodic time) × (timeout scale). The range is 1-10. Default is 3. Note: With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. However, if the timeout-scale is set to less than 3, the port timeout value does not take into account the normal travel time of the VLACPDU. The port expects to receive a VLACPDU at the same moment the partner port sends it. Therefore, the delayed VLACPDU results in the link being blocked, and then enabled again when the packet arrives. To prevent this scenario from happening, set the timeout-scale to a value larger than 3. VLACP partners must also wait 3 synchronized VLACPDUs to have the link enabled. If VLACP partner miss 3 consecutive packets from the other partner, sets the link as VLACP down.
funcmac-addr <mac>	Specifies the address of the far-end switch/stack configured to be the partner of this switch/stack. If none is configured, any VLACP-enabled switch communicating with the local switch through VLACP PDUs is considered to be the partner switch. Note: VLACP has only one multicast MAC address, configured using the vlacp macaddress command, which is the Layer 2 destination address used for the VLACPDUs. The port-specific funcmac-addr parameter does not specify a multicast MAC address, but instead specifies the MAC address of the switch or stack to which this port is sending VLACPDUs. You are not always required to configure funcmac-addr. If

Variable	Value
	not configured, the first VLACP-enabled switch that receives the PDUs from a unit assumes that it is the intended recipient and processes the PDUs accordingly. If you want an intermediate switch to drop VLACP packets, configure the funcmac-addr parameter to the desired destination MAC address. With funcmac-addr configured, the intermediate switches do not misinterpret the VLACP packets.
ethertype <hex>	Sets the VLACP protocol identification for this port. Defines the ethertype value of the VLACP frame. The range is 8101-81FF. Default is 8103.

Displaying VLACP status

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

Procedure steps

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

```
show vlacp
```

Displaying VLACP port configuration

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

Procedure steps

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

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

where **<slot/port>** specifies a port or list of ports.

Among other properties, the **show vlacp interface** command displays a column called HAVE PARTNER , with possible values of yes or no .

If `HAVE PARTNER` is `yes` when `ADMIN ENABLED` and `OPER ENABLED` are `true` , then that port has received VLACPDUs from a port and those PDUs were recognized as valid according to the interface settings.

If `HAVE PARTNER` is `no` , when `ADMIN ENABLED` is `true` and `OPER ENABLED` is `FALSE` , then the partner for that port is down (that port received at least one correct VLACPDU, but did not receive additional VLACPDUs within the configured timeout period). In this case VLACP blocks the port. This scenario is also seen if only one unit has VLACP enabled and the other has not enabled VLACP.

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

✱ **Note:**

If VLACP is enabled on an interface, the interface will not forward traffic unless it has a valid VLACP partner. If one partner has VLACP enabled and the other is not enabled, the unit with VLACP enabled will not forward traffic, however the unit with VLACP disabled will continue to forward traffic.

Chapter 13: ADAC Configuration using ACLI

Configuring ADAC for Avaya IP Phones using ACLI

You can configure ADAC-related settings using the following ACLI commands.

Configuring global ADAC settings

Use the following procedure to configure the global ADAC settings for the device.

Procedure steps

Use the following command from Global Configuration mode.

```
[no] adac [enable] [op-mode <untagged-frames-basic | untagged-
frames-advanced| tagged-frames>] [traps enable] [voice-vlan
<1-4094>] [uplink-port <portlist>] [call-server-port
<portlist>]
```

Variable definitions

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

Variable	Value
	- untagged-frames-basic: IP Phones send untagged frames, and the Voice VLAN is not assigned. - untagged-frames-advanced: IP Phones send untagged frames, and the Voice VLAN is assigned. - tagged-frames: IP Phones send tagged frames.
traps enable	Enables ADAC trap notifications.
voice-vlan *<1-4094>*	Sets the Voice VLAN ID. The assigned VLAN ID must previously be created as a voice-vlan..
uplink-port <*slot/port*>	Sets the Uplink port.
uplink-port <*portlist*>	Sets a maximum of 8 ports as Uplink ports.
call-server-port <*slot/port*>	Sets the Call Server port.
call-server-port <*ports*>	Sets a maximum of 8 ports as Call Server ports.

Restoring default ADAC settings

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

Procedure steps

Use the following command from Global Configuration mode.

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

Variable definitions

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

Variable	Value
traps enable	Restores the default state for ADAC notifications (enabled).
uplink-port	Restores the default Uplink port (none).
voice-vlan	Restores the default Voice-VLAN ID (none).

Configuring ADAC per port settings

Use the following procedure to set the per port ADAC settings for the device.

Procedure steps

Use the following command from Interface Configuration mode.

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

Variable definitions

Variable	Value
port *<portlist>*	Ports to which to apply the ADAC configuration.
enable	Enables ADAC on the port or ports listed.
tagged-frames-pvid *<1-4094>* | *no-change*	Sets Tagged-Frames PVID on the port or ports listed. Use *no-change* to keep the current setting.
tagged-frames-tagging *tagAll* | *tagPvidOnly* | *untagPvidOnly* | *no-change*	Sets Tagged-Frames Tagging to • tagAll • tagPvidOnly • untagPvidOnly Use *no-change* to keep the current setting.

Resetting ADAC per port settings to default

Use the following procedure to set the per port ADAC defaults for the specified ports.

Procedure steps

Use the following command from Interface Configuration mode.

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

Variable definitions

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

Configuring autodetection method

Use the following procedure to set the auto-detection method, by MAC address or using LLDP (IEEE 802.1ab).

Procedure steps

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

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

Variable definitions

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

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.

Resetting autodetection method to default

Use the following procedure to reset the auto-detection method to its defaults. The default is to have both MAC and LLDP enabled.

Procedure steps

To reset the autodetection method to default, use the following command from Interface Configuration mode.

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

Variable definitions

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

Configuring autodetection for ports

Use the following procedure to enable Auto-Detection on specified ports.

Procedure steps

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

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

Restoring ADAC port settings

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

Procedure steps

To restore ADAC port settings, use the following command from Global Configuration mode.

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

Adding a range to ADAC MAC address table

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

Procedure steps

To add a range, use the following command from Global Configuration mode.

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

Use the **no** form of the command to delete a range.

Note:

If the low-end and high-end MAC address values are not provided, the switch deletes all existing MAC address ranges from the switch.

Restoring ADAC MAC range table

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

Procedure steps

To restore the ADAC MAC range table, use the following command in Global Configuration mode.

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

Displaying global ADAC settings

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

Procedure steps

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

```
show adac
```

Displaying ADAC port settings

Use the following procedure to display the ADAC settings for a particular port.

Procedure steps

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

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

Displaying ADAC MAC ranges

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

Procedure steps

To display ADAC MAC ranges, use the following command from Privileged EXEC mode.

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

Displaying configured detection mechanism

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

Procedure steps

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

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

ADAC UFA configuration example

The following figure shows an example of ADAC configured in Untagged-Frames-Advanced (UFA) op-mode. (Call-server-port is used in this example, because the server is directly connected to the 5000 series switch.)

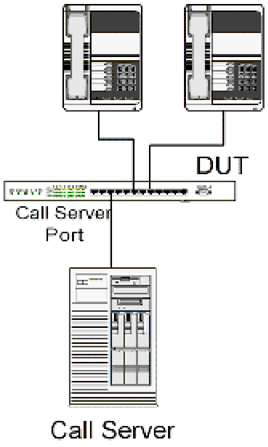


Figure 36: ADAC UFA configuration example

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

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

  - Tagging = Untagged
  - PVID = Voice-VLAN
- Call Server port:
  - Membership = add to Voice-VLAN
  - Tagging = Untagged
  - PVID = Voice-VLAN

To configure the above example, you must perform the following tasks:

1. Create a voice-VLAN.
2. Configure the call-server port.
3. Configure voice-VLAN.
4. Configure Untagged-Frames-Advanced (UFA) op-mode.
5. Enable ADAC on all ports to which IP phones connect.
6. Configure IP phones to send untagged traffic.
7. Enable the LLDP-MED Capabilities TLV on the ports used by IP phones.
8. Enable the LLDP-MED Network Policy TLV for transmission.

   This prevents configuration mismatches by enabling the IP Phone to obtain its policy settings directly from the switch.

ADAC configuration commands

The following section describes the detailed ACLI commands required to carry out the configuration shown in Figure 36: ADAC UFA configuration example on page 222.

```
(config)#vlan create 2 type voice-vlan
(config)#adac  call-server-port  7
(config)#adac  voice-vlan  2
(config)#adac  enable  op-mode  untagged-frames-advanced
(config)#interface  fastEthernet  all
(config)#interface  fastEthernet  16,24 enable
(config-if)#lldp tx-tlv port 16,24 med med-capabilities
(config-if)#lldp tx-tlv port 16,24 med network-policy
```

Verifying new ADAC settings

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

Auto configuration settings

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

```
           Auto       Oper      Auto
Port  Type Detection  State     Configuration T-F PVID  T-F Tagging
----  ---- ---------  -----     ------------- --------  -------------
7      CS  Disabled   Disabled  Applied       No Change Untag PVID Only
16     T   Enabled    Enabled   Applied       No Change Untag PVID Only
24     T   Enabled    Enabled   Applied       No Change Untag PVID Only
```

VLAN settings

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

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

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

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

ADAC settings

```
(config)#show running-config
```

```
 !...
! *** ADAC *** Note information in this section.
!
no adac enable
no adac mac-range-table
interface FastEthernet ALL
adac port 24 enable
no adac port 1-23 enable
exit
adac mac-range-table low-end 00-0A-E4-01-10-20 high-end
00-0A-E4-01-23-A7
adac mac-range-table low-end 00-0A-E4-01-70-EC high-end
00-0A-E4-01-84-73
adac mac-range-table low-end 00-0A-E4-01-A1-C8 high-end
```

```
00-0A-E4-01-AD-7F
adac mac-range-table low-end 00-0A-E4-01-DA-4E high-end
00-0A-E4-01-ED-D5
adac mac-range-table low-end 00-0A-E4-02-1E-D4 high-end
00-0A-E4-02-32-5B
adac mac-range-table low-end 00-0A-E4-02-5D-22 high-end
00-0A-E4-02-70-A9
adac mac-range-table low-end 00-0A-E4-02-D8-AE high-end
00-0A-E4-02-FF-BD
adac mac-range-table low-end 00-0A-E4-03-87-E4 high-end
00-0A-E4-03-89-0F
adac mac-range-table low-end 00-0A-E4-03-90-E0 high-end
00-0A-E4-03-B7-EF
adac mac-range-table low-end 00-0A-E4-04-1A-56 high-end
00-0A-E4-04-41-65
adac mac-range-table low-end 00-0A-E4-04-80-E8 high-end
00-0A-E4-04-A7-F7
adac mac-range-table low-end 00-0A-E4-04-D2-FC high-end
00-0A-E4-05-48-2B
adac mac-range-table low-end 00-0A-E4-05-B7-DF high-end
00-0A-E4-06-05-FE
adac mac-range-table low-end 00-0A-E4-06-55-EC high-end
00-0A-E4-07-19-3B
adac mac-range-table low-end 00-0A-E4-08-0A-02 high-end
00-0A-E4-08-7F-31
adac mac-range-table low-end 00-0A-E4-08-B2-89 high-end
00-0A-E4-09-75-D8
adac mac-range-table low-end 00-0A-E4-09-BB-9D high-end
00-0A-E4-09-CF-24
adac mac-range-table low-end 00-0A-E4-09-FC-2B high-end
00-0A-E4-0A-71-5A
adac mac-range-table low-end 00-0A-E4-0A-9D-DA high-end
00-0A-E4-0B-61-29
adac mac-range-table low-end 00-0A-E4-0B-BB-FC high-end
00-0A-E4-0B-BC-0F
adac mac-range-table low-end 00-0A-E4-0B-D9-BE high-end
00-0A-E4-0C-9D-0D
adac traps enable
adac voice-vlan 2
adac call-server-port 7
no adac uplink-port
adac enable
```

ADAC and EAP configuration commands

The following section describes the ACLI commands to configure ADAC with EAP on the same telephony port, with guest VLAN, Fail Open VLAN and use of RADIUS assigned VLAN enabled for EAPOL and Non-EAPOL clients.

Configure ADAC on the port. The phone is connected on port 2/9.

```
5698TFD-PWR(config)#int fa 2/9
5698TFD-PWR(config-if)#adac enable
```

Configure ADAC globally.

```
5698TFD-PWR(config)#adac voice-vlan 2001
5698TFD-PWR(config)#adac uplink-port 1/1,2/1,3/1
5698TFD-PWR(config)#adac op-mode tagged-frames
5698TFD-PWR(config)#adac enable
```

Enable EAPOL guest VLAN.

```
5698TFD-PWR(config)#vlan create 4000 name Guest_Vlan ty po
5698TFD-PWR(config)#eapol guest-vlan enable vid 4000
```

Enable EAPOL Fail Open VLAN.

```
5698TFD-PWR(config)#vlan create 4003 name Fail_Open_Vlan ty po
5698TFD-PWR(config)#eapol multihost fail-open-vlan enable
5698TFD-PWR(config)#eapol multihost fail-open-vlan vid 4003
```

Make local EAPOL setting on port.

% enable EAPOL on port

```
5698TFD-PWR(config)#eapol status auto
```

% enable EAPOL multihost on port

```
5698TFD-PWR(config)#eapol multihost enable
```

% enable authentication of NEAP users by RADIUS server

```
5698TFD-PWR(config)#eapol multihost radius-non-eap-enable
```

% enable use of RADIUS assigned VLAN for EAPOL users

```
5698TFD-PWR(config)#eapol multihost use-radius-assigned-vlan
```

% enable use of RADIUS assigned VLAN for non-EAPOL users

```
5698TFD-PWR(config)#eapol multihost non-eap-use-radius-assigned-vlan
```

```
5698TFD-PWR(config)#eapol multihost non-eap-mac-max 32
5698TFD-PWR(config)#eapol multihost eap-mac-max 32
5698TFD-PWR(config)#eapol multihost non-eap-phone-enable
5698TFD-PWR(config)#eapol guest-vlan enable vid 4000
```

Enable and configure EAPOL globally.

```
5698TFD-PWR(config)#eapol multihost non-eap-phone-enable
5698TFD-PWR(config)#eapol multihost use-radius-assigned-vlan
5698TFD-PWR(config)#eapol multihost non-eap-use-radius-assigned-vlan
5698TFD-PWR(config)#eapol enable
```

Display ADAC configuration and EAPOL settings.

```
5698TFD-PWR(config)#sh adac interface 2/9
Unit/        Auto       Oper      Auto
Port   Type  Detection  State     Configuration  T-F PVID   T-F Tagging
-----  ----  ---------  --------  -------------  ---------  ---------------
2/9    T     Enabled    Enabled   Applied        No Change  Untag PVID Only

5698TFD-PWR(config)#sh eapol multihost status
Unit/Port Client MAC Address Pae State      Backend Auth State Vid  Pri
--------- ------------------ -------------- ------------------ ---- ---

=========Neap Phones============

2/9       00:1B:4F:6D:E0:62
Total number of authenticated clients: 1

5698TFD-PWR(config)#sh eapol multihost non-eap-mac status
Unit/Port Client MAC Address State                          Vid  Pri
--------- ------------------ ------------------------------ ---- ---
2/9       00:13:20:13:58:0D  Authenticated By RADIUS        N/A  N/A
Total number of authenticated clients: 1
```

Chapter 14: LLDP Configuration using ACLI

Use the following procedures to enable and configure LLDP with ACLI.

Configuring LLDP transmit properties

Use this procedure to set the LLDP transmission parameters.

Procedure steps

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

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

Variable defintions

The following table outlines the parameters of the **lldp** command.

Variable	Value
tx-interval <5–32768>	Sets the interval between successive transmission cycles
tx-hold-multiplier <2–10>	Sets the multiplier for the tx-interval used to compute the Time To Live value for the TTL TLV.
reinit-delay<1–10>	Sets the delay for the reinitialization attempt if the adminStatus is disabled.
tx-delay <1–8192>	Sets the minimum delay between successive LLDP frame transmissions.
notification—interval <5–3600>	Sets the interval between successive transmissions of LLDP notifications.
med—fast—start <1–10>	Sets the MED Fast Start repeat count value.

Configuring LLDP Timers using ACLI

Use this procedure to re-configure LLDP timers from their default values.

Procedure steps

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

   ```
   lldp [msgTxHold][msgTxInterval] [reinitDelay][txDelay][med-fast-start]
   ```

Variable definitions

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

Variable	Value
msgTxHold	Determines TTL value used in an LLDPDU TTL is calculated by multiplying the transmit interval value and the transmit hold value. DEFAULT: 4s
msgTxInterval	Indicates the interval at which LLDP frames are transmitted on behalf of LLDP agent. DEFAULT: 30s
reinitDelay	Indicates the delay from when adminStatus becomes “disabled” until re-initialization. DEFAULT: 2s
txDelay	Indicates delay between successive LLDP frame transmissions initiated by value or status changes in LLDP local systems. RANGE: msgTxInterval x 0.25 DEFAULT: 2s
med-fast-start	Indicates that the LLDP-MED Fast Start mechanism is active for this part. The LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices

Variable	Value
	and does not apply to links between LAN infastructure elements.

Configuring LLDP port parameters

Use this procedure to set the LLDP port parameters.

Procedure steps

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

```
lldp port <portlist> [config notification] [status {rxOnly |
txAndRx | txOnly}]
```

Variable definitions

The following table describes the parameters of the **lldp port** command.

Variable	Value
port <portlist>	Specifies the ports affected by the command.
config notification	Enables notification when new neighbor information is stored or when existing information is removed.
status {rxOnly | txAndRx | txOnly}	Sets the LLDPU transmit and receive status on the ports rxonly: enables LLDPU receive only. txAndRx: enables LLDPU transmit and receive. txOnly: enables LLDPU transmit only.

Configuring management TLVs for LLDP ports

Use the following procedure to set the optional Management TLVs to be included in the LLDPDUs transmitted by each port.

Procedure steps

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

```
lldp tx-tlv [port <portlist>] [local-mgmt-addr] [port-desc]
[sys-cap] [sys-desc] [sys-name]
```

Variable definitions

The following table outlines the parameters of the **lldp tx-tlv** command.

Variable	Value
local-mgmt-addr	Specifies the local management address TLV.
port	Specifies the ports affected by the command.
port-desc	Specifies the port description TLV.
sys-cap	Specifies the system capabilities TLV.
sys-desc	Specifies the system description TLV.
sys-name	Specifies the system name TLV.

Configuring dot1 TLVs for LLDP ports

Use the following procedure to set the optional IEEE 802.1 organizationally-specifc TLVs to be included in the transmitted LLDPDUs.

Procedure steps

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

```
lldp tx-tlv [port <portlist>] dot1 [port-protocol-vlan-id
<vlanlist>] [port-vlan-id] {protocol-identity [EAP] [LLDP]
[STP]} [vlan-name <vlanlist>]
```

Variable definitions

The following table describes the parameters of the **`lldp tx-tlv dot1`** command.

Variable	Value
port <portlist>	Specifies the ports affected by the command.
port-vlan-id	Port VLAN ID TLV.
vlan-name	VLAN Name TLV.
port-protocol-vlan-id	Port and Protocol VLAN ID TLV.
protocol-identity [EAP] [LLDP] [STP]	Protocol Identity TLV.

Configuring dot3 TLVs for LLDP ports

Use the following procedure to set the optional IEEE 802.3 organizationally-specifc TLVs to be included in the transmitted LLDPDUs.

Procedure steps

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

```
lldp tx-tlv [port <portlist>] dot3 [link-aggregation] [mac-
phy-config-status] [maximum-frame-size] [mdi-power-support]
```

Variable definitions

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

Variable	Value
port <portlist>	Specifies the ports affected by the command.
mac-phy-config-status	MAC/Phy Configuration/Status TLV.
mdi-power-support	Power Via MDI TLV.
link-aggregation	Link Aggregation TLV.
maximum-frame-size	Maximum Frame Size TLV.

Configuring TLVs for MED devices

Use the following procedure to set the optional organizationally-specific TLVs for use by MED devices to be included in the transmitted LLDPDUs.

Procedure steps

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

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

Variable definitions

The following table describes the variables associated with the **lldp tx-tlv med** command.

Variable	Value
port <portlist>	Specifies the ports affected by the command.
med-capabilities	MED Capabilities TLV (the other MED TLVs can be enabled for transmission only if MED Capabilities TLV is enabled for transmission).
extendedPSE	Extended PSE TLV.
inventory	Inventory TLVs.
location	Location Identification TLV.
network-policy	Network Policy TLV.

Configuring parameters for LLDP location identification

Use the following procedure to set the coordinate-base parameters for LLDP location identification information.

Procedure steps

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

```
lldp location-identification coordinate-base [altitude]
[datum] [latitude] [longitude]
```

Variable definitions

The following table describes the parameters of the **`lldp location-identification coordinate-base`** command.

Variable	Value
altitude [+ | -] [0-4194303.fracti on] [meters | floors]	Altitude, in meters or floors.
datum [NAD83/MLLW | NAD83/NAVD88 | WGS84]	Reference datum The valid options are: • NAD83/MLLW: North American Datum 1983, Mean Lower Low Water • NAD83/NAVD88: North American Datum 1983, North American Vertical Datum of 1988 • WGS84: World Geodesic System 1984, Prime Meridian Name: Greenwich
latitude [0-90.00] [NORTH | SOUTH]	Latitude in degrees, and relative to the equator.
longitude [0-180.00] [EAST | WEST]	Longitude in degrees, and relative to the prime meridian.

Configuring LLDP civic address parameters

Use the following procedure to set the LLDP civic address parameters.

Procedure steps

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

```
ldp location-identification civic-address country-code
[additional-code] [additional-information] [apartment]
[block] [building] [city] [city-district ] [county] [floor]
```

```
[house-number] [house-number-suffix] [landmark] [leading-
street-direction] [name] [p.o.box] [place-type] [postal-
community-name] [postal/zip-code] [room-number] [state]
[street] [street-suffix] [trailing-street-suffix]
```

Variable definitions

The following table describes the parameters of the **`lldp location-identification civic-address`** command.

Variable	Value
`additional-code`	Additional code
`additional-information`	Additional location information
`apartment`	Unit (apartment, suite)
`block`	Neighborhood, block
`building`	Building (structure)
`city`	City, township, shi (JP)
`city-district`	City division, city district, ward
`country-code`	Country code value (2 capital letters)
`county`	County, parish, gun (JP), district (IN)
`floor`	Floor
`house-number`	House number
`house-number-suffix`	House number suffix
`landmark`	Landmark or vanity address
`leading-street-direction`	Leading street direction
`name`	Residence and office occupant
`p.o.box`	Post office box
`place-type`	Office
`postal-community-name`	Postal community name
`postal/zip-code`	Postal/Zip code
`room-number`	Room number
`state`	National subdivisions (state, canton, region)
`street`	Street

Variable	Value
`street-suffix`	Street suffix
`trailing-street-suffix`	Trailing street suffix

Configuring the LLDP emergency call service emergency location identification number

Use the following procedure to set the LLDP emergency call service - emergency location identification number (ECS-ELIN).

Procedure steps

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

   ```
   lldp location-identification ecs-elin <ecs-elin>
   ```

   Note:

   `<ecs-elin>` specifies a 10 to 25 digit numerical string.

Setting LLDP transmission parameters to default values

Use the following procedure to set the LLDP transmission parameters to their default values.

Procedure steps

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

   ```
   default lldp [tx-interval ] [tx-hold-multiplier ] [reinit-
   delay] [tx-delay] [notification-interval] [med-fast-start]
   ```

   Note:

   If no parameters are specified, the **`default lldp`** sets all parameters to their default parameters.

Variable definitions

The following table outlines the parameters of the **`default lldp`** command.

Table 19: show lldp port command parameters

Variable	Value
`tx-interval`	Sets the retransmit interval to the default value. DEFAULT: 30
`tx-hold-multiplier`	Sets the transmission multiplier to the default value. DEFAULT: 4
`reinit-delay`	Sets the reinitialize delay to the default value. DEFAULT: 2
`tx-delay`	Sets the transmission delay to the default value. DEFAULT: 2
`notification-interval`	Sets the notification interval to the default value. DEFAULT: 5
`med-fast-start`	sets the MED Fast Start repeat count value to the default value. DEFAULT: 4

Setting port parameters to default values

Use the following procedure to set the port parameters to their default values.

Procedure steps

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

```
default lldp port <portlist> [config notification] [status]
```

Variable definitions

The following table outlines the parameters of the **`default lldp port`** command.

Variable	Value
`port <portlist>`	Specifies the ports affected by the command.
`config notification`	Sets the config notification to its default value (disabled)
`status`	Sets the LLDPU transmit and receive status to the default value (txAndRx)

Setting Management TLVs to default values

Use the following procedure to set the LLDP Management TLVs to the default values.

Procedure steps

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

```
default lldp tx-tlv [port <portlist>][port-desc] [sys-name]
[sys-desc] [sys-cap] [local-mgmt-addr]
```

Variable definitions

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

Variable	Value
`port <portlist>`	Specifies the ports affected by the command.
`port-desc`	Port description TLV. DEFAULT: true (included)
`sys-name`	System name TLV. DEFAULT: true (included)
`sys-desc`	System description TLV DEFAULT:

Variable	Value
	true (included)
`sys-cap`	System capabilities TLV DEFAULT: true (included)
`local-mgmt-addr`	Local management address TLV DEFAULT: true (included)

Setting the IEEE 802.1 organizationally-specific TLVs to default values

Use the following procedure to set the optional IEEE 802.1 organizationally-specifc TLVs to the default values.

Procedure steps

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

```
default lldp tx-tlv [port <portlist>] dot1 [port-vlan-id]
[vlan-name ] [port-protocol-vlan-id] [protocol-identity
[EAP] [LLDP] [STP] ]
```

Variable definitions

The following table outlines the parameters of the **`default lldp tx-tlv dot1`** command.

Variable	Value
`port <portlist>`	specifies the ports affected by the command
`port-vlan-id`	Port VLAN ID TLV. DEFAULT: false (not included)
`vlan-name`	VLAN Name TLV. DEFAULT: none
`port-protocol-vlan-id`	Port and Protocol VLAN ID TLV. DEFAULT: none

Variable	Value
`protocol-identity [EAP] [LLDP] [STP]`	Protocol Identity TLV. DEFAULT: none

Setting the IEEE 802.3 organizationally-specific TLVs to default values

Use the following procedure to set the optional IEEE 802.3 organizationally-specifc TLVs to the default values.

Procedure steps

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

   ```
   default lldp tx-tlv [port <portlist>] dot3 [mac-phy-config-status] [mdi-power-support] [link-aggregation][maximum-frame-size]
   ```

Variable definitions

The following table outlines the parameters of the **`default lldp tx-tlv dot3`** command.

Variable	Value
`port <portlist>`	Specifies the ports affected by the command.
`mac-phy-config-status`	MAC/Phy Configuration/Status TLV. DEFAULT: false (not included)
`mdi-power-support`	Power Via MDI TLV. DEFAULT: true (included) ✱ **Note:** For non-PoE ports, default is false and cannot be set to true.
`link-aggregation`	Link Aggregation TLV. DEFAULT: false (not included)

Variable	Value
`maximum-frame-size`	Maximum Frame Size TLV. DEFAULT: false (not included)

Setting optional TLVs for MED devices to default values

Use the following procedure to set the optional organizationally-specifc TLVs for MED devices to the default values.

Procedure steps

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

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

Variable definitions

The following table outlines the parameters of the **`default lldp tx-tlv med`** command.

Variable	Value
`port <portlist>`	Specifies the ports affected by the command.
`med-capabilities`	MED Capabilities TLV. DEFAULT: true (included)
`extendedPSE`	Extended PSE TLV. DEFAULT: true (included) **Note:** For non-PoE ports, default is false and cannot be set to true.
`inventory`	Inventory TLVs. DEFAULT: true (included)
`location`	Location Identification TLV. DEFAULT: true (included)

Variable	Value
`network-policy`	Network Policy TLV. DEFAULT: true (included)

Disabling LLDP features on the port

Use the following procedure to disable LLDP features on the port.

Procedure steps

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

```
no lldp [port <portlist>] [config notification] [status]
```

Configuring Management TLVs

Use the following procedure to specify that the optional Management TLVs are not included in the transmitted LLDPDUs.

Procedure steps

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

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

Configuring the IEEE 802.1 TLVs

Use the following procedure to specify that the optional IEEE 802.1 TLVs are not included in the transmitted LLDPDUs.

Procedure steps

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

```
no lldp tx-tlv [port <portlist>] dot1 [port-vlan-id] [vlan-name] [port-protocol-vlan-id] [protocol-identity [EAP] [LLDP] [STP] ]
```

Configuring the IEEE 802.3 TLVs

Use the following procedure to specify that the optional IEEE 802.3 TLVs are not included in the transmitted LLDPDUs.

Procedure steps

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

   ```
   no lldp tx-tlv [port <portlist>] dot3 [mac-phy-config-status] [mdi-power-support] [link-aggregation][maximum-frame-size]
   ```

Configuring optional TLVs for MED devices

Use the following procedure to specify that the optional Management TLVs are not included in the transmitted LLDPDUs.

Procedure steps

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

   ```
   no lldp tx-tlv [port <portlist>] med [med-capabilities] [extendedPSE] [inventory] [location] [network-policy]
   ```

Note:

The transmit flag for med-capabilities TLV can be set to false only if the transmit flags for all the other MED TLVs are set to false.

Displaying configuration data for LLDP

Use the following procedure to display the LLDP parameters.

Procedure steps

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

```
show lldp [local-sys-data {dot1 | dot3 | med | detail}]
[mgmt-sys-data] [rx-stats] [tx-stats] [stats] [pdu-tlv-size]
[tx-tlv {dot1 | dot3 | med }] [neighbor { dot1 [vlan-names |
protocol-id] } | [dot3] | { med [capabilities] [network-
policy] [location] [extended-power] [inventory] } |
[detail] ] [neighbor-mgmt-addr]
```

Variable definitions

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

Variable	Value
`local-sys-data {dot1 | dot3 | med | detail}`	Displays the organizationally-specific TLV properties on the local switch: • dot1: displays the 802.1 TLV properties • dot3: displays the 802.3 TLV properties • med: displays the MED TLV properties • detail: displays all organizationally specific TLV properties To display the properties of the optional management TLVs, include only the local-sys-data parameter in the command.
`mgmt-sys-data`	Displays the local management system data.
`rx-stats`	Displays the LLDP receive statistics for the local system.
`tx-stats`	Displays the LLDP transmit statistics for the local system.
`stats`	Displays the LLDP table statistics for the remote system.
`pdu-tlv-size`	Displays the different TLV sizes and the number of TLVs in an LLDPDU.
`tx-tlv {dot1 | dot3 | med }`	Displays which TLVs are transmitted from the local switch in LLDPDUs:

Variable	Value
	• dot1: displays status for 802.1 TLVs • dot3: displays status for 802.3 TLVs • med: displays status for MED TLVs To display the transmission status of the optional management TLVs, include only the tx-tlv parameter in the command.
`neighbor { dot1 [vlan-names	protocol-id] }	[dot3]	{ med [capabilities] [network-policy] [location] [extended-power] [inventory] }	[detail]`	Displays the neighbor TLVs: • dot1: displays 802.1 TLVs: - vlan-names: VLAN Name TLV - protocol-id: Protocol Identity TLV • dot3: displays 802.3 TLVs • med: displays MED TLVs: - capabilities: Capabilities TLV - network-policy: Network Policy Discovery TLV - location: Location Identification TLV - extended-power: Extended Power-via-MDI TLV - inventory: Inventory TLVs • detail: displays all TLVs
`[neighbor-mgmtaddr]`	Displays the LLDP neighbor management address.

Configuring LLDP MED policies for switch ports

Use the following procedure to configure LLDP Media Endpoint Devices (MED) policies.

Procedure steps

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

```
lldp med-network-policies [port <portList>] {voice|voice-
signaling} [dscp <0-63>] [priority <0-7>] [tagging {tagged|
untagged}] [vlan-id <1-4094>]
```

Variable definitions

The following table describes the parameters of the **`lldp med-network-policies`** command.

Variable	Value
`port <portlist>`	Specifies the port or ports on which to configure LLDP MED policies.
`voice`	Specifies voice network policy.
`voice-signaling`	Specifies voice signalling network policy.
`dscp <0–63>`	Specifies the value of the Differentiated Service Code Point (DSCP) that is associated with the selected switch port or ports. RANGE: 0–63
`priority <0–7>`	Specifies the value of the 802.1p priority that applies to the selected switch port or ports. RANGE: 0–7
`tagging {tagged | untagged}`	Specifies the type of VLAN tagging to apply on the selected switch port or ports. • tagged — uses a tagged VLAN • untagged — uses an untagged VLAN or does not support port-based VLANs. If you select untagged, the system ignores the VLAN ID and priority values, and recognizes only the DSCP value.
`vlan-id <1–4094>`	Specifies the VLAN identifier for the selected port or ports. RANGE: 1–4094 If you select priority tagged frames, the system recognizes only the 802.1p priority level and uses a value of 0 for the VLAN ID of the ingress port.

Setting lldp med-network-policies to the default values

Use the following procedure to return lldp med-network-policies to the default values.

Procedure steps

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

```
default lldp med-network-policies [port <portList>] {voice|
voice-signaling}
```

Variable definitions

The following table describes the parameters of the **`default lldp med-network-policies`** command.

Variable	Value
`port <portlist>`	Specifies the port or ports on which to configure default LLDP MED policies.
`voice`	Specifies the default voice network policy.
`voice-signaling`	Specifies the default voice signalling network policy.

Disabling LLDP MED policies for switch ports

Use the following procedure to disable LLDP MED policies for switch ports.

Procedure steps

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

```
no lldp med-network-policies [port <portlist>] {voice|voice-
signaling}
```

Variable definitions

The following table describes the parameters of the **`no lldp med-network-policies`** command.

Variable	Value
`port <portlist>`	Specifies the port or ports on which to disable LLDP MED policies.
`voice`	Specifies the voice network policy to disable.
`voice-signaling`	Specifies the voice signalling network policy to disable.

Viewing lldp med-network-policies

Use the following procedure to display LLDP MED policy information for switch ports.

Procedure steps

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

```
show lldp med-network-policies [port <portlist>] {voice|
voice-signaling}
```

Variable definitions

The following table describes the parameters of the **`show lldp med-network-policies`** command.

Variable	Value
`port <portlist>`	Specifies the port or ports for which to display LLDP MED policy information.
`voice`	Displays the voice network policy for which to display information.
`voice-signaling`	Specifies the voice signalling network policy to disable.

Configuring LLDP

Use this procedure to configure the LLDP as shown in LLDP configuration example on page 251.

Important:

If a switch is reset while energy-saver is activated, the PoE power saving calculation may not accurately reflect the power saving, and in some cases may display zero savings. This is because the switch did not have sufficient time to record PoE usage between the reset of the switch and energy-saver being reactivated. When energy saver is next activated, the PoE power saving calculation will be correctly updated.

Procedure steps

1. Modify the default LLDP Tx interval from (the default 30 second value) to 60 seconds.

   Notice that if any modification is detected in the LLDP local-sys-data before the Tx interval expires, an LLDPDU is immediately sent on all active links in order to update the peers neighbor tables.
2. Enable the Port Description TLV for transmission. (contains the description of the LLPD sending port)
3. Enable the System Name TLV for transmission. (contains the name of the LLDP device)
4. Enable the System Description TLV for transmission. (contains the description of the LLDP device)
5. Enable the System Capabilities TLV for transmission. (contains the capabilities of the LLDP device)
6. Enable the Management Address TLV for transmission. (contains the management address of the LLDP device)
7. Enable the Port VLAN ID TLV for transmission. (contains the PVID of the LLDP sending port)
8. Enable the Port And Protocol VLAN ID TLV for transmission. (indicates the Port and Protocol VLANs to which the LLDP sending port belongs to).
9. Enable the VLAN Name TLV for transmission. (indicates the names of the VLANs to which the LLDP sending port belongs to)
10. Enable the Protocol Identity TLV for transmission. (indicates the supported protocols by the LLDP sending port)
11. Enable the MAC/PHY Configuration/Status TLV for transmission. (indicates the IEEE 802.3 duplex and bitrate capabilities and settings of the LLDP sending port)
12. Enable the Power Via MDI TLV for transmission. (indicates the MDI power support capabilities of the LLDP sending port)

13. Enable the Link Aggregation TLV for transmission. (indicates the link aggregation capability and status of the LLDP sending port)
14. Enable the Maximum Frame Size TLV for transmission. (indicates the maximum frame size that could be handled by the LLDP sending port)
15. Configure the location information for the LLDP-MED Location Identification TLV.

    There are three coordinate sets available for location advertisement.
16. Enable the LLDP-MED Capabilities TLV for transmission. (indicates the supported LLDP-MED TLVs and the LLDP-MED device type of the LLDP sending device)

    MED TLVs are transmitted only if MED-Capabilities TLV is transmitted
17. Enable the Network Policy TLV for transmission. (advertises the available MED applications available on the LLDP sending device and the policies required to use the applications)
18. Enable the Location Identification TLV for transmission. (indicates the physical location of the LLDP sending port; three coordinate sets are available to configure and send)
19. Enable the Extended Power-via-MDI TLV for transmission. (provides detailed informations regarding the PoE parameters of the LLDP sending device)
20. Enable the Inventory – Hardware Revision TLV for transmission. (indicates the hardware revision of the LLDP sending device)
21. Enable the Inventory – Firmware Revision TLV for transmission. (indicates the firmware revision of the LLDP sending device)
22. Enable the Inventory – Software Revision TLV for transmission. (indicates the software revision of the LLDP sending device)
23. Enable the Inventory – Serial Number TLV for transmission. (indicates the serial number of the LLDP sending device)
24. Enable the Inventory – Manufacturer Name TLV for transmission. (indicates the manufacturer name of the LLDP sending device)
25. Enable the Inventory – Model Name TLV for transmission. (indicates the model name of the LLDP sending device)

Note:

The switch only transmits LLDP MED information if the neighbor is a MED-capable unit.

LLDP configuration example

By default, LLDP is enabled for Tx and Rx on all switch ports. The default value for the LLDP Tx interval is 30 seconds (LLDPDUs are sent at 30 seconds). With the default settings, only the mandatory TLVs are sent, but the switch can receive any LLDP Core, DOT1, DOT3 or MED TLV from its peers.

shows an example of LLDP configuration. For this example, the router is connected to the ERS 5000 Series port 1 and the IP Phone uses port 13.

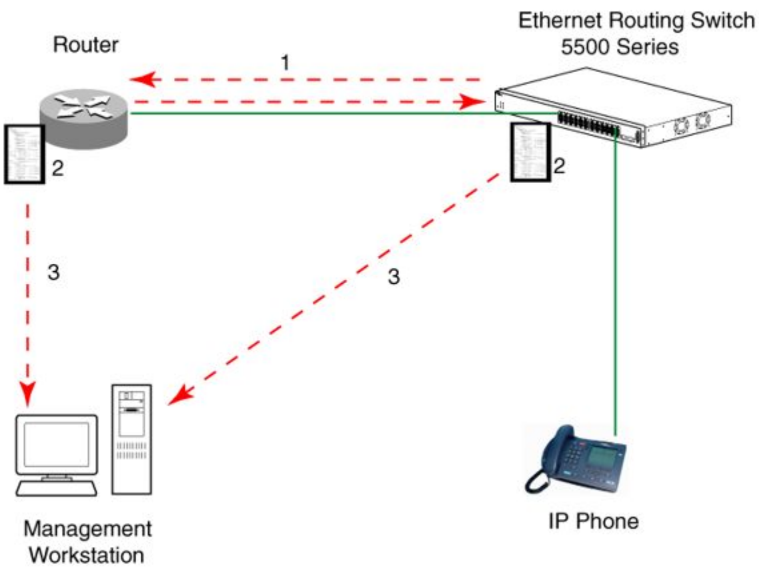


Figure 37: LLDP configuration example

Detailed configuration commands

Aggregation switch 171 configuration

IST, SMLT and SLT configuration

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

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

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

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

```
5520-48T-PWR(config-if)#ip address 5.5.5.1 255.255.255.0
5520-48T-PWR(config-if)#exit
```

```
5520-48T-PWR(config)#mlt 3 member 1-2
5520-48T-PWR(config)#mlt 3 enable
5520-48T-PWR(config)#interface mlt 3
5520-48T-PWR(config-if)#ist enable peer-ip 3.3.3.2 vlan 3
5520-48T-PWR(config-if)#exit
```

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

```
5520-48T-PWR(config)#mlt 5 member 4-5
5520-48T-PWR(config)#mlt 5 enable
5520-48T-PWR(config-if)#interface mlt 5
5520-48T-PWR(config-if)#smlt 5
5520-48T-PWR(config-if)#exit
```

VRRP and OSPF

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

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

Aggregation switch 172 configuration

IST, SMLT and SLT configuration

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

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

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

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

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

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

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

```
5520-48T-PWR(config)#mlt 5 member 4-5
5520-48T-PWR(config)#mlt 5 enable
5520-48T-PWR(config-if)#interface mlt 5
5520-48T-PWR(config-if)#smlt 5
5520-48T-PWR(config-if)#exit
```

VRRP and OSPF

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

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

Edge switch 173 configuration (5000 Series)

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

Edge switch 174 configuration (5000 Series)

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

Modifying the default LLDP Tx interval

Use this procedure to modify the default LLDP Tx interval.

Procedure steps

Use the following command from Global Configuration mode:

```
lldp tx-interval 60
```

Checking the new LLDP global settings

Use this procedure to show LLDP global settings.

Procedure steps

Use the following command from Global Configuration mode:

```
show lldp
```

Enabling all LLDP Core TLVs for transmission on the router and IP Phone ports

Use this procedure to enable all LLDP Core TLVs for transmission on the route and IP Phone ports.

Procedure steps

Use the following command from Global Configuration mode:

```
interface fastEthernet 1,13

lldp tx-tlv port 1,13 port-desc

lldp tx-tlv port 1,13 sys-name

lldp tx-tlv port 1,13 sys-desc

lldp tx-tlv port 1,13 sys-cap
lldp tx-tlv port 1,13 local-mgmt-addr
```

Checking the LLDP settings of the router and IP Phone ports

Use this procedure to check the LLDP settings of the router and IP Phone ports.

Procedure steps

Use the following command from Interface Configuration mode:

```
show lldp port 1,13 tx-tlv
```

Enabling all LLDP DOT1 TLVs for transmission on the router and IP Phone ports

Use this procedure to enable all LLDP DOT1 TLVs for transmission on the router and IP Phone ports.

Procedure steps

Use the following command from Interface Configuration mode:

```
lldp tx-tlv port 1,13 dot1 port-vlan-id
lldp tx-tlv port 1,13 dot1 port-protocol-vlan-id
lldp tx-tlv port 1,13 dot1 vlan-name
lldp tx-tlv port 1,13 dot1 protocol-identity EAP
LLDP STP
```

Checking the LLDP settings of the router and IP Phone ports

Use this procedure to check the LLDP setting of the router and IP Phone ports.

Procedure steps

Use the following command from Interface Configuration mode:

```
show lldp port 1,13 tx-tlv dot1
```

Enabling all LLDP DOT3 TLVs for transmission on the router and IP Phone ports

Use this procedure to enable all LLDP DOT3 TLVs for transmission on the router and IP Phone ports.

Procedure steps

Use the following command from Interface Configuration mode:

```
lldp tx-tlv port 1,13 dot3 mac-phy-config-status
lldp tx-tlv port 1,13 dot3 mdi-power-support
lldp tx-tlv port 1,13 dot3 link-aggregation
lldp tx-tlv port 1,13 dot3 maximum-frame-size
```

Checking the LLDP settings of the router and IP Phone ports

Use this procedure to check the LLDP settings of the router and IP Phone ports.

Procedure steps

Use the following command from Interface Configuration mode:

```
show lldp port 1,13 tx-tlv dot3
```

Enabling all LLDP MED TLVs for transmission on the router and IP Phone ports

Use this procedure to enable all LLDP MED TLVs for transmission on the router and IP Phone ports.

Note:

The first three commands are required to configure the location identification for the LLDP-MED Location Identification TLV.

Procedure steps

Use the following command from Interface Configuration mode:

```
lldp location-identification civic-address country-code US city
Boston
```

```
lldp location-identification coordinate-base altitude 3 floors
lldp location-identification ecs-elin 1234567890
lldp tx-tlv med port 1,13 med-capabilities
lldp tx-tlv med port 1,13 network-policy
lldp tx-tlv med port 1,13 location
lldp tx-tlv med port 1,13 extendedPSE
lldp tx-tlv med port 1,13 inventory
```

Checking the new LLDP settings of the router and IP Phone ports

Use this procedure to check the new LLDP settings of the router and IP Phone ports.

Procedure steps

Use the following command from Interface Configuration mode:

```
show lldp tx-tlv med
```

802.1AB Integration configuration

Use the procedures in this section to configure the LLDP TLVs for Avaya IP telephone support.

Configuring the PoE conservation level request TLV using ACLI

Use this procedure to request a specific power conservation level for an Avaya IP phone connected to a switch port.

Procedure steps

1. Log on to the Interface Configuration mode in ACLI.
2. At the command prompt, enter the following command to configure PoE conservation level TLVs for connected Avaya IP phones

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

   OR

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

   to set the PoE conservation level TLVs for connected Avaya IP phones.

Important:

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

Variable definitions

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

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

Viewing the switch PoE conservation level request TLV configuration using ACLI

Use this procedure to display Poe conservation level request configuration for local switch ports.

Procedure steps

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

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

Variable definitions

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

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

Configuring the switch call server IP address TLV using ACLI

Use this procedure to define the local call server IP addresses that switch ports advertise to Avaya IP phones.

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

Important:

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

Procedure steps

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

   ```
   lldp vendor-specific avaya call-server [<1–8>]<A.B.C.D> [[<1–
   8>] <A.B.C.D>] [[<1–8>] <A.B.C.D>]
   ```

   OR

   `default lldp vendor-specific avaya call-server <1–8>` to delete call server IPv4 addresses configured on the switch.

Variable definitions

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

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

Viewing Avaya IP phone call server IP address TLV information using ACLI

Use this procedure to display call server IP address information received on switch ports from an Avaya IP phone.

Procedure steps

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

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

Variable definitions

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

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

Viewing the switch file server IP address TLV configuration using ACLI

Use this procedure to define the local file server IP addresses that switch ports advertise to Avaya IP phones.

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

Note:

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

Important:

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

Procedure steps

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

   ```
   lldp vendor-specific avaya file-server [<1–4>] <A.B.C.D>
   [[<1–4>] <A.B.C.D>] [[<1–4>] <A.B.C.D>]
   ```

   OR

   ```
   default lldp vendor-specific avaya file-server <1–4>
   ```

   to delete file server IPv4 addresses configured in the switch.

   Note:

   To delete all file-server ip addresses configured on DUT use command `default lldp vendor-specific avaya file-server`.

Variable definitions

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

Variable	Value
<1–4>	Specifies the file server number.

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

Configuring the 802.1Q framing TLV using ACLI

Use this procedure to configure the frame tagging mode for exchanging Layer 2 priority tagging information between the switch and an Avaya IP phone.

Procedure steps

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

   ```
   lldp [port <portlist>]vendor-specific avaya dot1q-framing
   [tagged | non-tagged | auto]
   ```

   OR

   ```
   default [port <portlist>]vendor-specific avaya dot1q-framing
   ```
   to set the Layer 2 frame tagging mode to default.

Variable definitions

The following table describes the parameters for the **`lldp vendor-specific avaya dot1q-framing`** command.

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

Variable	Value
	based on server configuration. If that fails, traffic is transmitted untagged. DEFAULT: Auto

Viewing Avaya IP phone 802.1Q Framing TLV information using ACLI

Use this procedure to display Layer 2 frame tagging mode information received on switch ports from connected Avaya IP phones.

Procedure steps

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

```
show lldp [port <portlist>] neighbor vendor-specific avaya
dot1q-framing
```

Variable definitions

The following table describes the parameters for the **show lldp neighbor vendor-specific avaya dot1q-framing** command.

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

Viewing Avaya IP phone file server IP address TLV information using ACLI

Use this procedure to display information about file server IP address received on switch ports from Avaya IP phones.

Procedure steps

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

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

Variable definitions

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

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

Chapter 15: VLANs Configuration using Enterprise Device Manager

The following sections detail how to create and manage a VLAN using the Enterprise Device Manager (EDM).

Displaying VLAN configuration

Use this procedure to display basic VLAN configuration

Procedure steps

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

Variable definitions

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

Table 20: VLAN Basic tab parameters

Variable	Value
Id	The VLAN ID for the VLAN.
Name	Name of the VLAN.
Ifindex	Indicates the interface index.
Type	Indicates the type of VLAN: byPort or byProtocolId.
VoiceEnabled	Indicates whether VLAN is a voice VLAN (true) or not (false).
PortMembers	Ports that are members of the VLAN.
ActiveMembers	Set of ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met.
StgId	Identifies the spanning tree group to which the VLAN belongs. This field is only available when the switch is running in Avaya STPG mode.

Variable	Value
VrfId	Identifies the numerical ID for the VRF instance. Value ranges from 0 to 3.
VrfName	Identifies the alphanumeric identifier (name) assigned to the VRF instance.
MstpInstance	This field is only available when the switch is running in MSTP mode.
ProtocolId	Protocol for protocol-based VLANs. This value is taken from the Assigned Numbers RFC. For port-based VLANs, None is the displayed value.
UserDefinedPid	When rcVlanProtocolId is set to usrDefined(15) in a protocol-based VLAN, this field represents the 16-bit user-defined protocol identifier.
Encap	The type of encapsulation. Options are ethernet2 and llc.
MacAddress	The unique hardware address of the device.
Routing	Specifies whether routing is enabled (true) or disabled (false) on the VLAN.

Creating a VLAN

Use this procedure to create a new VLAN. To add or remove ports from the VLAN, you must modify the VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **VLANs**.
3. Select the **Basic** tab.
4. Click **Insert**.

   The Insert Basic dialog box appears with the Type field set to byPort.
5. Enter the identifier for the VLAN in the **Id** field. This value must be a unique number between 2 and 4094.
6. Optionally, enter a name for the VLAN in the **Name** field.
7. Enter the value of the Spanning Tree Group to which the VLAN will belong in the **StgId** field.
8. When in Avaya STPG mode, use the **StgId** menu to choose the spanning tree group to which the VLAN is to belong. When in MSTP mode, use the **MstpInstance** list to select the CIST or MSTI instance to which the VLAN is to belong.
9. Select the type of VLAN in the **Type** field.

   a. If the VLAN is to be port-based, select the **byPort** option button.

   b. If the VLAN is to be protocol-based, select the **byProtocolId** option button. This selection enables the **ProtocolId** field. From this field select the protocol on which this VLAN will be based. If it is to be based on a user-defined protocol, select the **usrDefined** option button and enter the custom PID in the **UserDefinedPid** field.

10. If the VLAN is to be a voice VLAN, select the **VoiceEnabled** button.

11. Click **Insert**.

Modifying a VLAN

Use this procedure to modify a VLAN's name, member ports, or routing status without recreating the VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VALN tree, click **VLANs**.
3. Select the **Basic** tab.
4. To modify the VLAN name, double-click in the **Name** field.
5. To modify the Routing status, double-click in the **Routing** field and select from the drop-down list.
6. To modify VLAN member ports, in the row that represents the VLAN that is to be modified, double-click in the **PortMembers** field.

   The Port Members screen appears.
7. Click the buttons that correspond to the ports that are to be added or deleted from the VLAN. Click **All** to select all switch ports.
8. Click **OK**.
9. Click **Apply**.

Deleting VLANs

Use this procedure to delete a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **VLANs**.
3. Select the **Basic** tab.
4. Select the VLAN to be deleted.

5. Click **Delete**.
6. Select **Yes** to confirm.

Clearing DHCP statistics counters on a VLAN

Use this procedure to clear DHCP statistics counters.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **VLANs**.
3. Select the **Basic** tab.
4. Highlight the VLAN for which DHCP statistics counters are to be cleared.
5. Click **IP**.

   The IP VLAN screen appears.
6. Select the **DCHP** tab.
7. From the **DHCP** tab, select **clear** in the **ClearCounters** field and press **Apply**.

Variable definitions

The following table outlines the parameters of the **DHCP Graph** button.

Table 21: DHCP Graph button parameters

Variable	Value
NumRequests	The total number of DHCP requests seen on this interface.
NumReplies	The total number of DHCP replies seen on this interface.

Configuring VLAN Snoop

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

For information on the IGMP snooping feature, refer to *Avaya Ethernet Routing Switch 5000 Series Configuration — IP Routing Protocols*, NN47200-503.

Procedure steps

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

Variable definitions

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

Table 22: VLAN Snoop tab parameters

Variable	Value
Id	Specifies the ID of the VLAN.
ReportPorxyEnable	A flag to note whether IGMP Report Proxy is enabled on this VLAN.
Enable	A flag to note whether IGMP Snooping is enabled on this VLAN.
Robustness	Allows tuning for the expected packet loss on a subnet. If a subnet is expected to be *lossy*, the Robustness variable may be increased. IGMP is robust to (Robustness - 1) packet losses.
QueryInterval	Specifies the interval (in seconds) between IGMP Host-Query packets transmitted on this interface.
MRouterPorts	Specifies the set of ports in this VLAN that provide connectivity to an IP Multicast router.
Ver1MRouterPorts	Specifies the version 1 ports in this VLAN that provide connectivity to an IP Multicast router.
Ver2RouterPorts	Specifies the version 2 ports in this VLAN that provide connectivity to an IP Multicast router.
ActiveMRouterPorts	Specifies the active ports.
ActiveQuerier	Specifies the IP address of multicast querier router
QuerierPort	Specifies the port on which the multicast querier router was heard.
MRouterExpiration	Specifies the multicast querier router aging time out

Configuring VLAN Ports

Use this procedure to configure VLAN ports.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **VLANs**.
3. Select the **Ports** tab.
4. Click **Apply** after making any changes.

Variable definitions

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

Table 23: VLAN Ports tab parameters

Variable	Value
Index	Specifies the port number.
VlanIds	Specifies the VLAN IDs of which this port is a member.
DiscardUntaggedFrames	This field only applies to trunk ports. It acts as a flag used to determine how to process untagged frames received on this port. When the flag is set, the frames are discarded by the forwarding process. When the flag is reset, the frames are assigned to the VLAN specified by rcVlanPortDefaultVlanId.
FilterUnregisteredFrames	This field only applies to access ports. It acts as a flag used to determine how to process unregistered frames received on this port. When the flag is set, the frames are discarded by the forwarding process. When the flag is reset, the frames are processed normally.
DefaultVlanId	Indicates the VLAN ID assigned to untagged frames received on a trunk port.
PortPriority	Specifies the port priority value from the list as a value between 0 and 7.
Tagging	Indicates the type of VLAN port. A trunk port can be a member of more than one VLAN. An access port can be a member of only VLAN, if no membership conflict exists. There are four types of VLAN port: • tagAll(trunk) • untagAll(access) • tagPvidOnly • untagPvidOnly

VLAN NSNA Configuration

This section contains information about VLAN NSNA Configuration.

Viewing VLAN NSNA

Use this procedure to display VLAN NSNA information.

Procedure steps

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

Variable definitions

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

Table 24: VLAN NSNA tab parameters

Variable	Value
Id	Specifies the VLAN identification number.
NsnaColor	Specifies the NSNA VLAN color.
FilterSetName	Specifies the filter set name. **Note:** NsnaColor field must be only red, yellow, or green.
YellowSubnetType	Specifies the Ethernet type for the Yeloow VLAN subnet. **Note:** NsnaColor field must be set to yellow.
YellowSubnet	Specifies the Yellow VLAN subnet. **Note:** NsnaColor field must be set to yellow.
YellowSubnetMask	Specifies the Yellow VLAN subnet mask. **Note:** NsnaColor field must be set to yellow..

Configuring NSNA per VLAN

Use this procedure to configure NSNA on a VLAN basis.

> ❗ **Important:**
>
> VLANs that you plan to configure as NSNA VLANs must be empty (that is, they have no port members assigned). NSNA VLANs cannot be associated with non-NSNA ports; therefore you cannot assign non-NSNA ports manually to enabled NSNA VLANs.
>
> Dumb and static devices that cannot authenticate through tunnel guard can be connected to NSNA dynamic ports. To ensure network access for these devices, add the MAC addresses to the SNAS MAC database.

For more information about NSNA, refer to *Avaya Ethernet Routing Switch 5000 Series Configuration - Security*, NN47200-501.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **VLANs**.
3. Select the **NSNA** tab.
4. Select a VLAN to modify.
5. Double click the **NsnaColor** field. A menu appears.
6. Select one of the following options from the menu:
    - none
    - red
    - green
    - yellow
    - voip

    > ❗ **Important:**
    >
    > Although each switch can have multiple Yellow, Green, and VoIP VLANs, each switch must have only one Red VLAN.
7. In the other columns, enter parameters compatible with the NsnaColor selection.
8. Click **Apply**.

Deleting an NSNA VLAN

Use this procedure to delete an NSNA VLAN.

Prerequisites

- NSNA must be globally disabled before you can delete an NSNA VLAN.

Use the following procedure to delete an NSNA VLAN:

Procedure steps

1. From the navigation tree, double-click **Security**.
2. From the Security tree, click **NSNA**.
3. Select the **Globals** tab.
4. Clear the **Enabled** check box.
5. From the navigation tree, double-click **VLAN**.
6. From the VLAN tree, double click **VLANs**.
7. Select the **NSNA** tab.
8. Select the VLAN to delete and double click the **NsnaColor** field.
9. From the list, select **none**.
10. Click **Apply**.
11. Select the **Basic** tab.
12. Select the VLAN to delete (the VLAN for which the NsnaColor was changed to none).
13. Click **Delete**.

Filtering an NSNA VLAN

Use this procedure to filter an NSNA VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **VLANs**.
3. Select the **NSNA** tab.
4. Click **Filter**.
5. Set the filter parameters.
6. Click **Filter**.

Variable definitions

The following table outlines the parameters of the **MAC Multicast Filter Table** tab.

Table 25: MAC Multicast Filter Table tab parameters

Variable	Value
AllowedAddressVlanId	Specifies the allowed address of the VLAN ID.
AllowedAddressMacAddr	Specifies the allowed address for the MAC address.

Enabling AutoPVID

Use this procedure to enable AutoPVID functionality on the switch.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, click **Chassis**.
4. Select the **System** tab.
5. In the **AutoPVID** field, select **enabled**.
6. Click **Apply**.

MAC address table maintenance

You can flush the MAC address table using Enterprise Device Manager. For more information about the MAC address table, see Managing the MAC address forwarding database table on page 155.

Flushing the MAC address table

Use this procedure to flush dynamically learned MAC addresses from the MAC address forwarding table:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, click **Bridge**.
3. Select the **MAC Flush** tab.
4. Click **FlushMacAddrTableAll** or type the MAC address, VLAN, trunk, port, or portlist in the corresponding box.
5. Click **Apply**.

Variable definitions

Table 26: MAC Flush tab parameters

Variable	Value
FlushMacAddrTableAll	Flushes all MAC addresses from MAC address table.
FlushMacAddrTableByPortlist	Flushes the MAC addresses for port(s) specified from the MAC address table.
FlushMacAddrTableByVlan	Flushes the MAC addresses for the VLAN specified from the MAC address table.
FlushMacAddrTableByTrunk	Flushes the MAC addresses for the Multi-Link Trunk specified from the MAC address table.
FlushMacAddrTableByAddress	Flushes the specified MAC addresses from MAC address table.

Selecting VLAN configuration control

Use this procedure to select configuration control for a VLAN.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, click **VLANs**.
3. In the work area, click the **Settings** tab.
4. In the **ManagementVlanID** box, type a value.
5. In the **VlanConfigControl** section, click a button.
6. On the toolbar, click **Apply**.

Variable Definitions

Use the data in this table to select VLAN configuration control.

Variable	Value
ManagementVlanId	Specifies the identifier of the management VLAN. Values range from 1 to 4094.

Variable	Value
VlanConfigControl	Specifies the VLAN configuration control options. The available options are: • automatic—This selection automatically adds an untagged port to a new VLAN and automatically removes it from any previous VLAN membership. The PVID of the port is automatically changed to the VID of the VLAN it joins. Since the port is first added to the new VLAN and then removed from any previous membership, the Spanning Tree Group participation of the port is not disabled as long as the VLANs involved are in the same Spanning Tree Group. • autopvid—This selection functions in the same manner as previous AutoPVID functionality. When an untagged port is added to a new VLAN, the port is added to the new VLAN and the PVID assigned to the new VID without removing it from any previous VLAN memberships. Using this option, an untagged port can have membership in multiple VLANs. • flexible—This selection functions in a similar manner to disabling AutoPVID functionality. When this option is used, an untagged port can belong to an unlimited number of VLANs. 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.

Chapter 16: Spanning Tree Configuration using Enterprise Device Manager

The following sections detail how to create and manage an STP using the Enterprise Device Manager (EDM). STP creation and management is performed in the Spanning Tree folder.

Setting the STP mode

Use this procedure to set the STP operational mode:

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, click **Globals**.
4. In the **SpanningTreeAdminMode** field, select the STP mode.
5. Click **Apply**.
6. Click **Yes** to the warning message reminding you that you must reset the switch for the change to take effect.
7. Click **Close**.
8. To reset the switch, choose **Edit > Chassis**.
9. From the **System** tab, choose the **reboot** option and click **Apply**.

Variable definitions

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

Table 27: Spanning Tree Globals tab parameters

Variable	Value
SpanningTreeAdminMode	Indicates the desired spanning-tree mode of the system.

Variable	Value
SpanniingTreeOperMode	This object indicates the current spanning-tree mode of the system.

Resetting the switch

Use this procedure to reset the switch.

Procedure steps

1. From the navigation pane, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, click **Chassis**.
4. In the work area, click the **System** tab.
5. In the ReBoot section, click the **bootPrimary** radio button.
6. On the toolbar, click **Apply**.

Configuring STP BPDU filtering for specific ports

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.

STP BPDU-Filtering is not supported on MLT ports.

1. On the **Device Physical View** select a port, or use Ctrl-click to select more than one port.
2. Right-click the port or group of ports.
3. From the drop-down menu, click **Edit**.
4. On the work area, click the **STP BPDU-Filtering** tab.
5. If you selected a group of ports on the Device Physical View, perform the following actions for each port in the list:
    - To select a port to edit, click the cell in the **rcPortIndex** column.
    - In the port row, double-click the cell in the **Admin Enabled** column.
    - Click the arrow to reveal the list.
    - Select a value from the list—**true** to enable STP BPDU filtering for the port, or **false** to disable STP BPDU filtering for the port.

- In the port row, double-click the cell in the **Timeout** column.
- Type a value in the dialog box.

6. If you selected a single port on the Device Physical View:
    - Click the **AdminEnabled** checkbox.
    - Enter a value in the **Timeout** box.
7. On the toolbar, click **Apply**.

Variable definitions

The following table outlines the parameters of the **STP BPDU-Filtering** tab.

Table 28: STP BPDU-Filtering tab parameters

Variable	Value
rcPortIndex	Indicates the switch and port number.
AdminEnabled	Enables and disables BPDU filtering on the port.
OperEnabled	Indicates the current operational status of BPDU filtering on the port: true (enabled) or false (disabled).
Timeout	When BPDU filtering is enabled, this parameter indicates the time, in 1/100 seconds, during which the port remains disabled after it receives a BPDU. The port timer is disabled if this value is set to 0. The default value is 12000 (120 seconds).
TimerCount	Displays the time remaining for the port to stay in the disabled state after receiving a BPDU.

Spanning Tree STG configuration

Configuring STG Global properties

Use this procedure to configure the STG global properties.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **STG**.

4. Select the **Globals** tab.
5. Select the STP path cost calculation mode:
6. Select the STP port mode:
7. Check the SpanningTreeAdminCompatibility box to enable 802.1d port learning.
8. Click **Apply**.

Variable definitions

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

Table 29: STG Globals tab parameters

Variable	Value
SpanningTreePathCostCalculationMode	Specifies the current spanning-tree path cost calculation mode. The value ieee802dot1dCompatible is valid only when the switch is running in Avaya STPG mode.
SpanningTreePortMode	Specifies the STG port membership mode for all Spanning Tree Groups on the switch.
SpanningTreeAdminCompatibility	Specifies whether the learning mode of a port stays in the Forwarding state or changes to the Disabled state when the port operation status goes down. If the box is checked, the port goes to the disabled state when down.
SpanningTreeOperCompatibility	Specifies the operational compatibility mode for features controlled by the associated object.

Creating an STG

Use this procedure to create a Spanning Tree Group.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, click **STG**.
4. Click the **Configuration** tab.
5. Click **Insert**.
6. In the fields provided, fill in the information for the new STG.
7. Click **Insert**.

Variable definitions

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

Table 30: STG Configuration tab parameters

Variable	Value
Id	Enter an integer between 1 and 8 that identifies the STG; 1 is the default STG.
BridgeAddress	Displays the MAC address used by this bridge; it is usually the smallest MAC address of all ports in the bridge.
NumPorts	Displays the number of ports controlled by this bridging entity.
ProtocolSpecification	Displays the version of spanning tree that is running.
Priority	Enter the first two octets of the 8-octet bridge ID; the range is 0 to 65 535.
BridgeMaxAge	Enter the maximum time you want to allow before the specified STG times out, in seconds; the range is 600 to 4 000.
BridgeHelloTime	Enter the maximum time between hellos, in seconds; the range is 100 to 1 000.
BridgeForwardDelay	Enter the maximum delay in forwarding, in seconds; the range is 400 to 3 000.
EnableStp	Enables or disables the spanning tree group.
TaggedBpduAddress	The address for the tagged BPDU.
TaggedBpduVlanId	Enter the VLAN ID for tagged BPDUs.

Adding a VLAN to an STG

When using Enterprise Device Manager, a VLAN can only be added to an STG at the time the VLAN is created.

Ensure the STG already exists, and use the procedure Creating a VLAN on page 266.

Moving a VLAN between STGs

You cannot use Enterprise Device Manager to move VLANs between STGs on the Avaya Ethernet Routing Switch 5000 Series. Instead, delete the VLAN to be moved and add a replacement VLAN in the STG to which you want to move the VLAN.

Deleting an STG

Use this procedure to delete an STG.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, click **STG**.
4. On the **Configuration** tab, select the STG to be deleted.
5. Click **Delete**.

Displaying STG Status

Use this procedure to display the status of an STG.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, click **STG**.
4. Select the **Status** tab.

Variable definitions

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

Table 31: STG Status tab parameters

Variable	Value
Id	Displays the STG ID.
BridgeAddress	Displays the MAC address used by this bridge.
NumPorts	Displays the number of ports controlled by this bridging entity.
ProtocolSpecification	Displays the version of spanning tree that is running.
TimeSinceTopology Change	Displays the time, in hundredths of seconds, since the last topology change.
TopChanges	Displays the number of topology changes since the switch was reset.
DesignatedRoot	Displays the MAC address of the STP designated root.

Variable	Value
RootCost	Displays the cost of the path to the root.
RootPort	Displays the port number of the port with the lowest-cost path from this bridge to the root bridge.
MaxAge	Displays the maximum age, in hundredths of a second, of STP information learned from any port in the network before the information is discarded.
HelloTime	Displays the amount of time, in hundredths of seconds, between Hello messages.
HoldTime	Displays the interval, in hundredths of seconds, during which no more than two Hello messages can be transmitted.
ForwardDelay	Displays the interval, in hundredths of seconds, during which the switch stays in Listening or Learning mode, before moving to Forwarding mode. This value is also used to age dynamic entries in the Forwarding Database.

Displaying STG ports

Use this procedure to display the STG port status.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, click **STG**.
4. Select the **Ports** tab.

Variable definitions

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

Table 32: STG Ports tab parameters

Variable	Value
Port	Indicates the switch position in a stack and port number. For a standalone switch, the default value of 1 is used for the switch position.
StgId	Displays the STG ID number assigned to the port.
Priority	Specifies the port priority

Variable	Value
State	Displays the STP state of the port: Disabled, Blocking, Listening, Learning, Forwarding.
EnableStp	Enables or disables STP on the port: True is enabled, and False is disabled.
FastStart	Enables or disables Fast Start STP on the port: True is enabled, and False is disabled.
AdminPathCost	Sets the PathCost value. The field displays 0 if no user-configured value exists.
PathCost	Displays the contribution of this port to the cost path of the spanning tree root.
DesignatedRoot	Displays the MAC address of the STP designated root.
DesignatedCost	Displays the path cost of the designated port of the segment connected to this port.
DesignatedBridge	Displays the MAC address of the designated bridge this port considers the designated bridge for this segment.
DesignatedPort	Displays the port ID of the designated bridge for this port segment.
ForwardTransitions	Displays the number of times the port transitioned from STP Learning to Forwarding state.

Configuring STG port properties

Use this procedure to display STG port properties.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, click **Ports**.
4. Select the **STG** tab.

Variable definitions

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

Table 33: Chassis Ports tab parameters

Variable	Value
Port	Specifies the port number.
StgId	The spanning tree group ID to which the VLAN belongs.
Priority	The value of the priority field that is contained in the first (in network byte order) octet of the (2-octet long) Port ID. The other octet of the Port ID is derived from the value of dot1dStpPort.
State	The current port state as defined by application of the Spanning Tree Protocol. This state controls the action a port takes when it receives a frame. If the bridge detects a port that is malfunctioning, it places that port into the broken state. For ports that are disabled (see EnableStp), this object has a value of Disabled.
EnableStp	Select True or False to enable or disable STP.
FastStart	Select True or False to enable or disable FastStart.
AdminPathCost	The administrative value of the PathCost. This is the value that has been configured by the user, or 0 if no user-configured value exists. If you specify the path cost in the PathCost field, the value in this field is modified as well.
PathCost	The contribution of this port to the cost of paths toward the spanning tree root, which includes this port. The IEEE 802.1D-1990 standard recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN.
DesignatedRoot	The unique Bridge Identifier of the bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached.
DesignatedCost	The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs.
DesignatedBridge	The Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port segment.
DesignatedPort	The Port Identifier of the port on the Designated Bridge for this port segment.
ForwardTransitions	The number of times this port has transitioned from the Learning state to the Forwarding state.

Rapid Spanning Tree Protocol

The Rapid Spanning Tree protocol (RSTP or IEEE 802.1w) reduces the recovery time after a network breakdown. It also maintains a backward compatibility with the IEEE 802.1d which was the Spanning Tree implementation prior to RSTP. In certain configurations, the recovery time of RSTP can be reduced to less than 1 second.

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

Note:

You can access the RSTP menu command only after the switch is operating in the RSTP mode.

Viewing RSTP general information

Use this procedure to view general information about Rapid Spanning Tree Protocol (RSTP) when RSTP is in active mode.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, click **RSTP**.
4. Select the **Globals** tab.

Variable definitions

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

Table 34: RSTP Globals tab parameters

Variable	Value
PathCostDefault	Sets the version of the Spanning Tree default Path Costs that the Bridge uses. The value of 16-bit uses the 16-bit default Path Costs from IEEE Std. 802.1D-1998. A value of 32-bit uses the 32-bit default Path Costs from IEEE Std. 802.1t.
TXHoldCount	The value used by the Port Transmit state machine to limit the maximum transmission rate. The value can range from 1 to 10.
Version	The version of the Spanning Tree Protocol the bridge is currently running:

Variable	Value
	• 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	The value of the writable portion of the Bridge Identifier comprising the first two octets. The values that are set for Priority must be in steps of 4096.
BridgeMaxAge	The value in 1/100 seconds that all bridges use for MaxAge when this bridge acts as the root. The value must be a multiple of 100. The range is 600 to 4000.
BridgeHelloTime	The value in 1/100 seconds that all bridges use for HelloTime when this bridge acts as the root. The value must be a multiple of 100. The range is 100 to 1000.
BridgeForward Delay	The value in 1/100 seconds that all bridges use for ForwardDelay when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of BridgeMaxAge. The value must be a multiple of 100. The range is 400 to 3000.
DesignatedRoot	The unique identifier of the Bridge recorded as the Root in the Configuration BPDUs that are transmitted by the Designated Bridge for the segment to which the port is attached. Reference IEEE 802.1D-1990: Section 4.5.5.4.
RootCost	The cost of the path to the root as seen from this bridge.
RootPort	The port number of the port that offers the lowest cost path from this bridge to the root bridge.
MaxAge	The maximum age of Spanning Tree Protocol information learned from the network on any port before being discarded. The maximum age is specified in units of hundredths of a second. This is the actual value that the bridge uses.
HelloTime	The amount of time required for transmission of the configuration BPDUs by the node on any port when it is the root of the spanning tree or trying to become the root. This is specified in units of hundredths of a second. This is the actual value that the bridge uses.
ForwardDelay	This time value, measured in units of hundredths of a second, controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state.
RstpUpCount	The number of times the RSTP Module has been enabled. A trap is generated on the occurrence of this event.

Variable	Value
RstpDownCount	The number of times the RSTP Module has been disabled. A trap is generated on the occurrence of this event
NewRootIdCount	The number of times this Bridge has detected a Root Identifier change. A trap is generated on the occurrence of this event.
TimeSinceTopologyChange	The time (in hundredths of a second) since the TcWhile Timer for any port in this Bridge was non-zero for the Common Spanning Tree context.
TopChanges	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.

Displaying RSTP ports information

Use this proceudre to view RSTP ports information.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, click **RSTP**.
4. Select the **Ports** tab.

Variable definitions

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

Table 35: RSTP Ports tab parameters

Variable	Value
Port	The port number.
State	Used to identify a port state in this RSTP instance. The port state is cataloged as discarding, learning, and forwarding.
Priority	The value of the priority field which is contained in the first (in network byte order) octet of the (2 octet long) Port ID.
PathCost	The contribution of this port to the cost of paths towards the spanning tree root.
ProtocolMigration	Indicates the Protocol migration state of this port. Set this field to true to force the port to transmit RSTP BPDUs. Note: If this field is set to true and the port receives an 802.1d type BPDU, the port again begins transmitting 802.1d BPDUs.

Variable	Value
AdminEdgePort	The administrative value of the Edge Port parameter. A value of true indicates that this port is assumed to be an edge-port and a value of false indicates that this port is assumed to be a nonedge-port.
OperEdgePort	The operational value of the Edge Port parameter. The object is initialized to false on reception of a BPDU.
AdminPointToPoint	The administrative point-to-point status of the LAN segment attached to this port. • A value of forceTrue indicates that this port is always treated as being connected to a point-to-point link. • A value of forceFalse indicates that this port is treated as having a shared media connection. • A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means.
OperPointToPoint	The operational point-to-point status of the LAN segment attached to this port. This field indicates whether a port is considered to have a point-to-point connection. The value is determined by management or by auto-detection.
Participating	This field specifies whether a port is participating in the 802.1w protocol.
DesignatedRoot	The bridge identifier of the old root of the Spanning Tree as determined by the Spanning Tree Protocol as executed by this node.
DesignatedCost	The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received BPDUs.
DesignatedBridge	The Bridge Identifier of the bridge which this port considers to be the Designated Bridge for this port segment.
DesignatedPort	The Port Identifier for the port segment which is on the Designated Bridge.
ForwardTransitions	The number of times this port has transitioned from the Learning state to the Forwarding state.

Displaying RSTP status

Use this procedure to view RSTP status.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, click **RSTP**.
4. Select the **Status** tab.

Variable definitions

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

Table 36: RSTP Status tab parameters

Variable	Value
Port	The port number.
Role	A role represents a functionality characteristic or capability of a resource to which policies are applied.
OperVersion	This indicates whether the Port is operationally in the RSTP mode or the STP-compatible mode; that is, whether the Port is transmitting RSTP BPDUs or Config/TCN BPDUs.
EffectivePortState	This is the effective Operational state of the port. This object is set to true only when the port is operationally up in the interface manager and when the force Port State and specified port state for this port is enabled. Otherwise, this object is set to false.

Graphing RSTP port statistics

Use this procedure to display RSTP port statistics.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, click **RSTP**.
4. Select the **Status** tab.
5. Select a port and click **Graph** to get the statistics for the selected port.

Variable definitions

The following table outlines the parameters of the **RSTP Graph** dialog box.

Table 37: RSTP Graph dialog box parameters

Variable	Value
RxRstBpduCount	The number of RST BPDUs that have been received on the port.
RxConfigBpduCount	The number of Config BPDUs that have been received on the port.
RxTcnBpduCount	The number of TCN BPDUs that have been received on the port.
TxRstBpduCount	The number of RST BPDUs that have been transmitted by this port.
TxConfigBpduCount	The number of Config BPDUs that have been transmitted by this port.
TxTcnBpduCount	The number of TCN BPDUs that have been transmitted by this port.
InvalidRstBpduRxCount	The number of invalid RSTP BPDUs that have been received on this port.
InvalidConfigBpduRxCount	The number of invalid Configuration BPDUs that have been received on this port.
InvalidTcnBpduRxCount	The number of invalid TCN BPDUs that have been received on this port.
ProtocolMigrationCount	The number of times this Port has migrated from one STP protocol version to another. The relevant protocols are STP-COMPATIBLE and RSTP.

Multiple Spanning Tree Protocol

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

In the MSTP mode, the 5000 Series switches support a maximum of one Common and Internal Spanning Tree (CIST) and seven Multiple Spanning Tree Instances (MSTI).

Within the CIST, the Internal Spanning Tree component is used only by devices from the same region (for which a regional root is elected). The Common (External) Spanning Tree component of the CIST is used by devices from different regions or between devices with different STP modes.

Note:

you can access the MSTP menu command only when the switch is operating in the MSTP mode.

Displaying MSTP general information

Use this procedure to view MSTP information.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, click **MSTP**.
4. Select the **Globals** tab.

Variable definitions

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

Table 38: MSTP Globals tab parameters

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.
MaxHopCount	Specifies the Maximum Hop Count value in 1/100 seconds. The value must be a multiple of 100. The range is 100 to 4000.
NoOfInstancesSupported	Indicates the maximum number of spanning tree instances supported.
MstpUpCount	Specifies the number of times the MSTP Module is enabled. A trap is generated on the occurrence of this event.
MstpDownCount	Specifies the number of times the MSTP Module is disabled. A trap is generated on the occurrence of this event.
ForceProtocolVersion	Signifies the version of the Spanning Tree Protocol that the bridge is currently running.

Variable	Value
	• 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	The bridge address is generated when events like protocol up or protocol down occurs.
Root	The bridge identifier of the root of the common spanning tree as determined by the Spanning Tree Protocol as executed by this node. This value is used as the CIST Root Identifier parameter in all Configuration BPDUs originated by this node.
RegionalRoot	The bridge identifier of the root of the Multiple Spanning Tree region as determined by the Spanning Tree Protocol as executed by this node. This value is used as the CIST Regional Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
RootCost	Specifies the cost of the path to the CIST Root as seen from this bridge.
RegionalRootCost	Specifies the cost of the path to the CIST Regional Root as seen from this bridge.
RootPort	Indicates the port number of the port which offers the lowest path cost from the bridge to the CIST Root Bridge
BridgePriority	Indicates the value of the writable portion of the Bridge Identifier comprising the first two octets. The values that are set for Bridge Priority must be in steps of 4096.
BridgeMaxAge	Specifies the value in hundredths of a second that all bridges use for MaxAge when this bridge acts as the root. The value must be a multiple of 100. The range is 600 to 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 to 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.

Variable	Value
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	Specifes the time, in hundredths of a second, since the TcWhile Timer for any port in this Bridge was non-zero for the Common Spanning Tree context.
NewRootBridgeCount	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.
TopChanges	Specifies the number of times that at least one non-zero TcWhile Timer occurred on this Bridge for the Common Spanning Tree context.
RegionName	Specifies the region name of the configuration. By default, the Region Name is equal to the Bridge Mac Address.
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.
RegionVersion	Denotes the version of the MST Region.
ConfigDigest	Signifies the Configuration Digest value for this Region. This is an MD5 digest value and hence must always be 16 octets long.
RegionConfigChange Count	Specifies the number of times a Region Configuration Identifier Change is detected. A trap is generated when this event occurs.

Displaying CIST port information

Use this procedure to display the CIST port information.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, click **MSTP**.
4. Select the **CIST Port** tab.

Variable definitions

The following table outlines the parameters of the **CIST Port** tab.

Table 39: MSTP CIST Port tab parameters

Variable	Value
Port	Identifies 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	Displays the four most significant bits of the Port Identifier of the Spanning Tree instance. It can be modified by setting the CistPortPriority value. The values that are set for Port Priority must be in steps of 16.
DesignatedRoot	Specifies the unique Bridge Identifier of the bridge. 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	Displays the contribution of this port to the cost of paths towards the CIST Regional Root.
ProtocolMigration	Indicates the Protocol migration state of this port. When operating in MSTP mode, set this field to true to force the port to transmit MSTP BPDUs without instance information. **Note:** If this field is set to true and the port receives an 802.1d BPDU, the port begins transmitting 802.1d BPDUs. If the port receives an 802.1w BPDU, it begins transmitting 802.1w BPDUs.
AdminEdgeStatus	Specifies the administrative value of the Edge Port parameter. A value of true indicates that this port can be assumed to be an edge-port, and a value of false indicates that this port can be assumed to be a nonedge-port.

Variable	Value
OperEdgeStatus	Signifies the operational value of the Edge Port parameter. This value is initialized to the value of AdminEdgeStatus and set to false when the port receives a BPDU.
AdminP2P	Displays the administrative point-to-point status of the LAN segment attached to this port. A value of 0 indicates that this port is always treated as being connected to a point-to-point link. A value of 1 indicates that this port is treated as having a shared media connection. A value of 2 indicates that this port is considered to have a point-to-point link if it is an Aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation, or by management means.
OperP2P	Indicates the operational point-to-point status of the LAN segment attached to the port. It also indicates whether a port is considered to have a point-to-point connection. The value is determined by management or by auto-detection, as described in the AdminP2P object.
HelloTime	Displays the amount of time between the transmission of Configuration BPDUs transmitted by this node on the port. 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	Displays the effective operational state of the port for CIST. This is set to true only when the port is operationally up in the Interface level and Protocol level for CIST. This is set to false for all other times.
State	Displays the current state of the port as defined by the Common Spanning Tree Protocol.
ForcePortState	Displays the current state of the port which can be changed to either Disabled or Enabled for the base Spanning Tree instance.
SelectedPortRole	Displays the selected port role for the Spanning Tree instance.
CurrentPortRole	Displays the current port role for the Spanning Tree instance.

Graphing CIST Port statistics

Use this procedure to display CIST Port statistics

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, click **MSTP**.
4. Select the **CIST Port** tab.
5. Select a port and click Graph to get the statistics for the CIST Port.

Variable definitions

The following table outlines the parameters of the **CIST Port** tab.

Table 40: CIST Port Graph dialog box parameters

Variable	Value
ForwardTransitions	Displays the number of times this port transitioned to the Forwarding State.
RxMstBpduCount	Displays the number of MST BPDUs received on this port.
RxRstBpduCount	Displays the number of RST BPDUs received on this port.
RxConfigBpduCount	Displays the number of Configuration BPDUs received on this port.
RxTcnBpduCount	Displays the number of TCN BPDUs received on this port.
TxMstBpduCount	Displays the number of MST BPDUs transmitted from this port.
TxRstBpduCount	Displays the number of RST BPDUs transmitted from this port.
TxConfigBpduCount	Displays the number of Configuration BPDUs transmitted from this port.
TxTcnBpduCount	Displays the number of TCN BPDUs transmitted from this port.
InvalidMstBpduRxCount	Displays the number of Invalid MST BPDUs received on this port.
InvalidRstBpduRxCount	Displays the number of Invalid RST BPDUs received on this port.
InvalidConfigBpdu RxCount	Displays the number of Invalid Configuration BPDUs received on this port.
InvalidTcnBpduRxCount	Displays the number of Invalid TCN BPDUs received on this port.
ProtocolMigrationCount	Displays the number of times this port has migrated from one STP protocol version to another. The relevant migration

Variable	Value
	protocols are STP-COMPATIBLE and RSTP/MSTP. A trap is generated when the port migrates.

Displaying MSTI Bridges

Use this procedure to view the MSTI Bridges information.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, click **MSTP**.
4. Select the **MSTI Bridges** tab.

Variable definitions

The following table outlines the parameters of the **MSTI Bridges** tab.

Table 41: MSTP MSTI Bridges tab parameters

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	Specifies 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.

Variable	Value
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

Use this procedure to insert MSTI Bridges.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, click **MSTP**.
4. Select the **MSTI Bridges** tab.
5. Click the **Insert** button.
6. Type the instance id.
7. Click **Insert**.

Deleting MSTP MSTI Bridges

Use this procedure to delete MSTI bridges.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, click **MSTP**.
4. Select the **MSTI Bridges** tab.
5. Click on one or multiple MSTI Bridges.

6. Click **Delete**.
7. Click **Yes** to confirm you wish to delete the MSTI Bridge(s).

Associating a VLAN with the CIST or an MSTI instance

Use this procedure to associate a VLAN with the CIST or an MSTI instance:

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **VLANs**.
3. Select the **Basic** tab.
4. Click **Insert**.
5. In the **MstpInstance** field, select the CIST or an MSTI instance from the menu.
6. Populate the other fields as required.
7. Click **Insert**.

Modifying VLAN CIST or MSTI association

Use this procedure to modify an existing VLAN association with a CIST or MSTI:

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **VLANs**.
3. Select the **Basic** tab.
4. Double-click in the **MstpInstance** field.
5. Select the CIST option or one of the MSTI options and click **Apply**.

Viewing MSTP MSTI Ports

Use this procedure to view MSTI Port information.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **MSTP**.
4. Select the **MSTI Port** tab.

Variable definitions

The following table outlines the parameters of the **MSTI Port** tab.

Table 42: MSTP MSTI Port tab parameters

Variable	Value
Port	Denotes the port number.
BridgeInstance	The number of times a Spanning Tree instance was deleted. A Trap is generated when this event occurs.
State	Indicates the current state of the port as defined by the Multiple Spanning Tree Protocol. The state of a port can be Forwarding or Discarding (Blocking).
ForcePortState	Signifies the current state of the port which can be changed to either Disabled or Enabled for the specific Spanning Tree instance.
PathCost	Specifies the contribution of this port to the cost of paths towards the MSTI Root which includes this port.
Priority	Indicates the four most significant bits of the Port Identifier for a given Spanning Tree instance. This value can be modified independently for each Spanning Tree instance supported by the Bridge. The values set for Port Priority must be in steps of 16.
DesignatedRoot	Specifies the unique Bridge Identifier of the bridge recorded as the MSTI Regional Root in the configuration BPDUs that are transmitted.
DesignatedBridge	Identifies the unique Bridge Identifier of the bridge which this port considers to be the Designated Bridge for the port segment.
DesignatedPort	Identifies 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 MSTP MSTI Port Statistics

Use this procedure to display MSTI Port statistics.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **Spanning Tree**.
3. From the Spanning Tree folder, double-click **MSTP**.
4. Select the **MSTI Port** tab.
5. Select a port and click **Graph** to get the statistics for the MSTI Port.

Variable definitions

The following table outlines the parameters of the **MSTI Port Graph** dialog box.

Table 43: MSTP MSTI Port Graph dialog box parameters

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 17: MLT Configuration using Enterprise Device Manager

You can create and manage Multi-Link trunks using the following Enterprise Device Manager (EDM) screens:

MultiLink Trunks configuration

Use the information in this section to create a MultiLink Trunk (MLT) and to modify existing MLT port memberships.

Configuring Multi-Link Trunks

Use this procedure to display and configure MLTs.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **MLT/LACP**.
3. Select the **MultiLink Trunks** tab.
4. To select a trunk to create, click the trunk ID.
5. In the trunk row, double-click the cell in the **Name** column.
6. In the field, type a name for the MLT, or accept the default name.
7. In the trunk row, double-click the cell in the **PortMembers** column.
8. From the list, select multiple ports to add to the trunk.
9. Click **OK**.
10. In the trunk row, double-click the cell in the **Loadbalance(Mode)** column.
11. From the list, select a load balancing mode.
12. In the trunk row, double-click in the **Enable** column.
13. From the list, select **true** to enable the MLT, or **false** to disable the MLT.
14. To create additional MLTs, repeat steps 4 to 13.
15. Click **Apply**.

Variable definitions

The following table outlines the parameters of the **MultiLink Trunks** tab.

Table 44: MLT/LACP MultiLink Trunks tab parameters

Variable	Value
ID	Specifies the MLT identification number (assigned consecutively).
PortType	Specifies the port type: • Access • trunk • UntagPvidOnly • TagPvidOnly
Name	Specifies the name given to the MLT.
PortMembers	Specifies the ports assigned to the MLT.
VlanIds	Specifies the VLANs assigned to the MLT.
Loadbalance(Mode)	Specifies the MLT load balancing mode: • basic (MAC-based load balancing) • advanced (IP-based load balancing)
Enable	Specifies whether the Multi-Link trunk is active.
MltType	Specifies the type of MLT: • normalMLT • istMLT • splitMLT
RunningType	Displays the current MLT operational type: • normalMLT • istMLT • splitMLT
SmltId	Specifies the assigned SMLT ID. Both ends of the SMLT must have the same SMLT ID. The SmltId field is used when the MltType is splitMLT. The SmltId value should be 0 if the MltType is not splitMLT.

Filtering the Multi-Link Trunks tab display

Use this procedure to filter the display of the Multi-Link Trunks tab to display selected types of MLT.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **MLT/LACP**.
3. Select the **MultiLink Trunks** tab.
4. Click **Filter**.
5. Set the properties, and click **Filter**.

Adding MLT Ports

Use this procedure to add ports to an MLT.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **MLT/LACP**.
3. Select the **MultiLink Trunks** tab.
4. Click **Filter**.
5. Set the properties, and click **Filter**.
6. Double-click in the **PortMembers** field for the MLT to which ports are to be added.
7. Click on the buttons that represent the ports that are to be added to the MLT. For the 5000 Series, up to 8 same-type ports can belong to a single MLT
8. Click **OK**.
9. Click **Apply**.

Disabling MLT ports on Shutdown

Use this procedure to configure the system to disable MLT ports on shutdown.

1. From the navigation tree, click **VLAN**.
2. From the VLAN tree, click **MLT/LACP**.
3. Select the **Globals** tab.

4. Select the **MltDisablePortsOnShutdown** check box.
5. In the SmltSysId field, enter the LACP system ID for SMLT (MAC address).
6. On the tool bar, click **Apply**.

Table 45: Variable definitions

Variable	Value
MltDisablePortsOnShutdown	Specifies whether the function is enabled or disabled.
SmltSysId	Specifies the MAC address of the LACP system ID for SMLT.

Configuring SMLT

This section describes how to use Enterprise Device Manager (EDM) to configure Split Multi-Link Trunking (SMLT).

Note:

To configure SMLT on the 5000 Series switch, an Advanced License must be purchased that allows this feature to be used.

Adding an MLT-based SMLT

Use this procedure to add an MLT-based SMLT.

Important:

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

You can create an SMLT from the MultiLink Trunks tab by selecting the MLT type as SMLT and then specifying an SMLT ID.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **MLT/LACP**.
3. Select the **MultiLink Trunks** tab.
4. From the displayed list of MLTs, choose an available MLT to configure as an SMLT.
5. In the row containing the desired MLT, double-click the **PortMembers** field.

6. Click the ports to include in the MLT-based SMLT.

   For the 5000 Series, up to eight same-type ports can belong to a single MLT.
7. Click **OK**.
8. Double-click the **MltType** field and choose **splitMLT** from the list.
9. In the **SmltId** field, type an unused SMLT ID (1 - 32).

   Note:

   The corresponding SMLTs between aggregation switches must have matching SMLT IDs. The same ID number must be used on both sides.
10. Click **Apply**.

Viewing SLTs configured on your switch

Use this procedure to view the SLTs configured on your switch.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **MLT/LACP**.
3. Select the **Single Port SMLT** tab.

Variable definitions

The following table outlines the parameters of the **Single Port SMLT** tab.

Table 46: MLT/LACP Single Port SMLT tab parameters

Variable	Value
Index	Displays the index number.
SmltId	Displays the ID number of the SLT (1 - 512).
RunningType	Read only field that displays the current port operational type: • normal • smlt (single port Split MLT)

Configuring an SLT

Use this procedure to configure an SLT.

Important:

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

Ports that are already configured as MLT or MLT-based SMLT cannot be configured as a single port SLT. You must first remove the split trunk and then reconfigure the ports as an SLT.

Procedure steps

1. From the Device Physical View, double-click a port.
2. Select the **SMLT** tab.

   Note:

   If the MltId field is not zero, this indicates that the port is already configured as an MLT or MLT-based SMLT. If so, you cannot configure an SLT on the port.
3. Click **Insert.**
4. In the **SmltId** field, enter an unused SMLT ID number from 1 to 512.

   To view the SMLT IDs that are already in use on your switch, see Viewing SLTs configured on your switch on page 307.
5. Click **Insert**.

Variable definitions

The following table outlines the parameters of the **Port X/X** tab.

Table 47: Edit Port X/X tab parameters

Variable	Value
Index	Indicates the index number for the port.
MltId	Read only field displaying either a value between 1 and 32 indicating that the port is part of an MLT or a value of 0 indicating the port has no MLT assigned and that it can be configured for SLT.
SmltId	Specifies the Split MLT ID, an integer from 1 to 512.

Deleting an SLT

Use this procedure to delete an SLT.

Procedure steps

1. From the Device Physical View, double-click a port.
2. Select the **SMLT** tab.
3. Select the Port SLT.
4. Click **Delete** .
5. Click **Close**.

Configuring an IST MLT

Use this procedure to configure an IST MLT.

> **Important:**
>
> For SMLT to function properly, you must manually disable STP on all SMLT, IST, and SLT ports in all spanning tree groups or instances to which the ports belong. From Release 6.2 onwards, STP is automatically disabled by software on all SMLT ports. You must also disable STP on all edge switch MLT ports that are connected to the SMLT or SLT.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **MLT/LACP**.
3. Select the **MultiLink Trunks** tab.
4. In the row containing the desired MLT, double-click the **PortMembers** field.
5. Select the ports to include in the MLT and click **OK**.

   For the 5000 Series, up to eight same-type ports can belong to a single MLT.
6. Double-click the **Enable** field and choose **true**.
7. Double-click the **MltType** field and choose **istMLT** from the list.
8. Click **Apply**.
9. Select any field in the IST MLT row and click the **istMlt** button.
10. In the **PeerIp** field, enter a peer IP address.
11. In the **VlanId** field, enter a VLAN ID.
12. In the **SessionEnable** field, click **enable**.
13. Click **Apply**.

Variable definitions

The following table describes the IST MLT parameters .

Table 48: MLT/LACP IST MLT parameters

Variable	Value
PeerIp	Indicates the IST MLT peer IP address.
VlanId	Specifies an IST VLAN ID number from 1 to 4095.
SessionEnable	Displays the Enable/disable IST functionality.
Session Status	Displays the status: up or down

Removing an IST MLT

Use this procedure to remove an existing IST MLT from your switch.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **MLT/LACP**.
3. Select the **MultiLink Trunks** tab.
4. Change the **MltType** field for the IST from **istMLT** to **normalMLT**.
5. Click **Apply**.

Viewing IST statistics

Use this procedure to view IST statistics on an interface.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **MLT/LACP**.
3. Select the **Ist/SMLT Stats** tab.

Variable definitions

The following table outlines the parameters of the **Ist/SMLT Stats** tab.

Table 49: MLT/LACP Ist/SMLT Stats tab parameters

Variable	Value
SmltIstDownCnt	Specifies the number of IST down messages.
SmltHelloTxMsgCnt	Specifies the number of hello messages transmitted.

Variable	Value
SmltHelloRxMsgCnt	Specifies the number of hello messages received.
SmltLearnMacAddrTxMsgCnt	Specifies the number of learn MAC address messages transmitted.
SmltLearnMacAddrRxMsgCnt	Specifies the number of learn MAC address messages received.
SmltMacAddrAgeOutTxMsgCnt	Specifies the number of MAC address aging out messages transmitted.
SmltMacAddrAgeOutRxMsgCnt	Specifies the number of MAC address aging out messages received.
SmltMacAddrAgeExpTxMsgCnt	Specifies the number of MAC address age expired messages transmitted.
SmltMacAddrAgeExpRxMsgCnt	Specifies the number of MAC address age expired messages received.
SmltStgInfoTxMsgCnt	Specifies the number of SMLT STG info messages transmitted.
SmltStgInfoRxMsgCnt	Specifies the number of SMLT STG info messages received.
SmltDelMacAddrTxMsgCnt	Specifies the number of deleted MAC address messages transmitted.
SmltDelMacAddrRxMsgCnt	Specifies the number of deleted MAC address messages received.
SmltSmltDownTxMsgCnt	Specifies the number of SMLT down messages transmitted.
SmltSmltDownRxMsgCnt	Specifies the number of SMLT down messages received.
SmltSmltUpTxMsgCnt	Specifies the number of SMLT up messages transmitted.
SmltSmltUpRxMsgCnt	Specifies the number of SMLT up messages received.
SmltSendMacTblTxMsgCnt	Specifies the number of send MAC table messages transmitted.
SmltSendMacTblRxMsgCnt	Specifies the number of send MAC table messages received.
SmltIgmpTxMsgCnt	Specifies the number of IGMP messages transmitted.
SmltIgmpRxMsgCnt	Specifies the number of IGMP messages received.
SmltPortDownTxMsgCnt	Specifies the number of port down messages transmitted.
SmltPortDownRxMsgCnt	Specifies the number of port down messages received.
SmltReqMacTblTxMsgCnt	Specifies the number of request MAC table messages transmitted.
SmltReqMacTblRxMsgCnt	Specifies the number of request MAC table messages received.

Variable	Value
SmltRxUnknownMsgTypeCnt	Specifies the number unknown SMLT messages received.

Chapter 18: LACP and VLACP Configuration using Enterprise Device Manager

LACP Configuration

You can use the following sections to configure LACP using the following Enterprise Device Manager.

Configuring the LACP port compatibility mode

Use this procedure to open to configure the LACP port compatibility mode

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **MLT/LACP**.
3. Select the **Globals** tab.

Variable definitions

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

Table 50: MLT/LACP LACP Globals tab parameters

Variable	Value
CompatibilityMode	Specifies the port compatibility mode for LACP: • default • advanced

Configuring Link Aggregation Groups

Us this procedure to configure Link Aggregation Groups.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **MLT/LACP**.
3. Select the **LACP** tab.

Variable definitions

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

Table 51: MLT/LACP LACP tab parameters

Variable	Value
Index	Specifies the unique identifier allocated to this Aggregator by the local System. This attribute identifies an Aggregator instance among the subordinate managed objects of the containing object. This value is read-only.
MacAddress	Specifies the MAC address used by this bridge when it must be referred to in a unique fashion.
AggregateOrIndividual	A read-only Boolean value indicating whether the Aggregation Port can Aggregate (TRUE) or can only operate as an Individual link (FALSE).
ActorLagID	Specifies the combined information of ActorSystemPriority, ActorSystemID, and ActorOperKey in ActorSystemPriority-ActorSystemID-ActorOperKey format.
ActorSystemPriority	A 2-octet read-write value indicating the priority value associated with the Actor's System ID.
ActorSystemID	Specifies a 6-octet read-only MAC address value that defines the value of the System ID for the System that contains this Aggregation Port.
ActorOperKey	Specifies the current operational value of the Key for the Aggregation Port. This is a 16-bit read-only value.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation Port. This is a 16-bit read-write value.
PartnerLagID	Specifies the combined information of PartnerSystemPriority, PartnerSystemID, and PartnerOperKey in PartnerSystemPriority-PartnerSystemID-PartnerOper Key format.

Variable	Value
PartnerSystemPriority	Specifies a 2-octet read-only value that indicates the priority value associated with the Partner's System ID.
PartnerSystemID	Specifies a 6-octet read-only MAC address value consisting of the unique identifier for the current protocol Partner of this Aggregator. A value of zero indicates that no known Partner exists. If the aggregation is manually configured, this System ID value is assigned by the local System.
PartnerOperKey	Specifies the current operational value of the Key for the Aggregator's current protocol Partner. This is a 16-bit read-only value.
CollectorMaxDelay	Specifies the value of this 16-bit read-write attribute defines the maximum delay, in tens of microseconds, that can be imposed by the Frame Collector between receiving a frame from an Aggregator Parser, and either delivering the frame to its MAC Client or discarding the frame.

Configuring LACP ports

Use this procedure to view or edit the LACP Ports.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **MLT/LACP**.
3. Select the **LACP Ports** tab.

Variable definitions

The following table outlines the parameters of the **LACP Ports** tab.

Table 52: LACP Ports tab parameters

Variable	Value
Index	Indicates the ifIndex of the port
AdminEnabled*	Specifies the current administrative setting for the port. A value of true means the port is set to participate in LACP. A value of false means the port is set to not participate in LACP.
operEnabled	Specifies 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
AggregateOrIndividual	A read-only Boolean value indicating whether the Aggregator represents an Aggregate (true) or an Individual link (false).
ActorSystemPriority	Specifies a 2-octet read-write value used to define the priority value associated with the Actor's System ID.
ActorSystemID	Specifies a 6-octet read-only MAC address value that defines the value of the System ID for the system that contains this Port.
ActorAdminKey	Indicates the current administrative value of the Key for the Aggregation Port.
ActorOperKey	Indicates the current operational value of the Key for the Aggregation Port.
SelectedAggID	Specifies the identifier value of the Aggregator that this Aggregation Port has currently selected. Zero indicates that the Aggregation Port has not selected an Aggregator, either because it is in the process of detaching from an Aggregator or because no suitable Aggregator exists for it to select.
AttachedAggID	Specifies the identifier value of the Aggregator that this Aggregation Port is currently attached to. Zero indicates that the Aggregation Port is not currently attached to an Aggregator. This value is read-only.
ActorPort	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
ActorPortPriority	Specifies the priority value assigned to this Aggregation Port. This 16-bit value is read-write.
ActorAdminState*	Specifies a string of 8 bits, corresponding to the administrative values of Actor_State as transmitted by the Actor in LACPDUs.
ActorOperState	Specifies a string of 8 bits, corresponding to the current operational values of Actor_State as transmitted by the Actor in LACPDUs.
PartnerOperPort	Specifies the operational port number assigned by the port's protocol partner. This value is read-only.

*To set the LACP modes, you must ensure that the LACP port properties are set according to the desired mode, as follows:

- LACP mode Off = **AdminEnabled** field cleared (disabled)
- LACP mode Passive = **AdminEnabled** field selected (enabled)
- LACP mode Active = **AdminEnabled** field selected (enabled) and **ActorAdminState** options **lacpActive** and **aggregation** selected

Mapping the LACP key mapping

Use this procedure to map the LACP key mapping.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **MLT/LACP**.
3. Select the **LACP key mapping** tab.

Variable definitions

The following table outlines the parameters of the **LACP key mapping** tab.

Table 53: MLT/LACP LACP key mapping tab parameters

Variable	Value
LacpKeyValue	Specifies the value of the LACP administration key.
MltId	Specifies the ID of the MLT.
SmltId	Specifies the ID of the SMLT.

VLACP Configuration

You can use the following sections to configure VLACP using the following Enterprise Device Manager.

Viewing VLACP Global information

Use this procedure to view VLACP information for the switch.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **MLT/LACP**.
3. Select the **VLACP Global** tab.

Variable definitions

The following table outlines the parameters of the **VLACP Global** tab.

Table 54: MLT/LACP VLACP Global tab parameters

Variable	Value
Enable	Enables or disables VLACP on the switch.
MulticastMACAddress	Identifies a multicast MAC address used exclusively for VLACPDUs. Default is 01:80:c2:00:11:00.

VLACP tab for ports

Use the following procedure to view the VLACP tab for ports:

Procedure steps

1. In the Device Physical View, double-click a Port.

   The Port X/X dialog box appears with the Interface tab displayed.
2. Select the VLACP tab.

If you want to configure multiple ports, you can access the VLACP tab on the MLT/LACP tab.

Variable definitions

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

Table 55: Port X/X VLACP tab parameters

Variable	Value
AdminEnable	Enables or disables VLACP on a port. The default value is False.
OperEnable	Indicates whether VLACP is operationally enabled or disabled. This is a read-only field.
FastPeriodicTimer	Specifies the number of milliseconds between periodic transmissions using short timeouts. Valid values range from 400-20000 with a default of 500.

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	Sets a timeout scale for the port, where timeout = (periodic time) * (timeout scale). The range is 1-10. Default is 3. Note: With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. However, if the timeout-scale is set to less than 3, the port timeout value does not take into account the normal travel time of the VLACPDU. The port expects to receive a VLACPDU at the same moment the partner port sends it. Therefore, the delayed VLACPDU results in the link being blocked, and then enabled again when the packet arrives. To prevent this scenario from happening, set the timeout-scale to a value larger than 3. If a VLACP partner does not receive a VLACPDU during (periodic time)*(timeout scale) the system sets the link as VLACP down.
EtherType	Specifies VLACP protocol identification. The ID value is a 4-digit Hex number, with a default of 8103.
EtherMacAddress	The default value is 00:00:00:00:00:00 and it can be configured with the MAC address of the switch or stack to which this port is sending VLACPDUs. It cannot be configured as a multicast MAC. Note: VLACP has only one multicast MAC address, configured using the MulticastMACAddress field in the VLACP Global tab, which is the Layer 2 destination address used for the VLACPDUs. The port-specific EtherMACAddresss parameter does not specify a multicast MAC address, but instead specifies the MAC address of the switch or stack to which this port is sending VLACPDUs. You are not always required to configure EtherMACAddresss. If not configured, the first VLACP-enabled switch that receives the PDUs from a unit assumes that it is the intended recipient and processes the PDUs accordingly. If you want an intermediate switch to drop VLACP packets, configure the EtherMACAddresss field with the desired destination MAC address. With EtherMACAddresss configured, the intermediate switches do not misinterpret the VLACP packets.
PortState	Identifies whether the VLACP port state is up or down. This is a read-only field.

Chapter 19: SLPP Configuration using Enterprise Device Manager

This chapter provides procedures used to configure Simple Loop Prevention Protocol (SLPP) using Device Manager.

Configuring SLPP transmitting list

Use this procedure to add a VLAN to the SLPP transmitting list.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **SLPP**.
3. Select the **VLANs** tab.
4. Under the **SlppEnable** heading, select the VLAN you want to add.
5. Double click to select True (enabled) or False (disabled).
6. Click **Apply**.
7. Click **Close**.

Enabling SLPP

Use this procedure to globally enable SLPP.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **SLPP**.
3. Select the **Global** tab.
4. Select the **GlobalEnable** checkbox.
5. Click **Apply**.
6. Click **Close**.

Configuring SLPP PDU transmit interval

Use this procedure to configure the SLPP PDU transmit interval in milliseconds.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **SLPP**.
3. Select the **Global** tab.
4. In the **TransmissionInterval** text box, enter the value, in milliseconds, for the transmit interval in the range 500 to 5000. The default is 500.
5. Click **Apply**.
6. Click **Close**.

Configuring SLPP PDU ether type

Use this procedure to configures the SLPP PDU ether type value:

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, double-click **SLPP**.
3. Select the **Global** tab.
4. In the **EtherType** text box, enter the value for ether type. The default SLPP PDU ether type value is 0x8102 Values 0x0000 and 0x8100 are disallowed.
5. Click **Apply**.
6. Click **Close**.

Configuring SLPP port auto enable

Use this procedure to configure the auto enable timer for ports shut down by SLPP.

Procedure steps

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

3. Select the **Global** tab.
4. In the **PortsReEnableTimeout** text box, enter the value, in seconds, for the timeout in the range 0 to 65535.
5. Click **Apply**.
6. Click **Close**.

Enabling SLPP PDU received function per port

Use this procedure to enable the SLPP PDU received function on a port.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **SLPP**.
3. Select the **Ports** tab.
4. Under the **SlppEnable** heading, select the port you want to enable.
5. Double click to select True (enabled) or False (disabled).
6. Click **Apply**.
7. Click **Close**.

Configuring the SLPP PDU receipt threshold

Use this procedure to enable the SLPP PDU received function on a port:

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **SLPP**.
3. Select the **Ports** tab.
4. Under the **PktRxThreshold** heading, select the port you want to modify.
5. Double click and enter the value for the threshold in the range 1 to 500.
6. Click **Apply**.
7. Click **Close**.

Configuring SLPP Guard using Enterprise Device Manager

This section provides the procedures to configure Simple Loop Prevention Protocol (SLPP) Guard using EDM.

Selecting an SLPP Guard Ethernet type using EDM

Use this procedure to select an SLPP Guard Ethernet type for the 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 **Global** tab.
4. Type a value in the **SlppGuardEtherType** box.
5. On the toolbar, click **Apply**.

Configuring SLPP Guard using EDM

You can use this procedure to configure SLPP Guard 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.
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 definitions

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 reenables 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 definitions

Variable	Value
<portlist>	Specifies a list of ports for which to display the SLPP Guard configuration status. If no ports are specified, the configuration status for all ports is displayed.

Chapter 20: ADAC Configuration using Enterprise Device Manager

You can configure ADAC-related settings through EDM using the following procedures.

Configuring ADAC settings

Use this procedure to configure the global ADAC settings.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, click **ADAC**.
4. Select the **ADAC** tab.
5. Select the **AdminEnable** field to enable ADAC.
6. Choose the Operating Mode.
7. In the **NotificationControlEnable** field, enable or disable trap notifications.
8. Enter the Voice VLAN ID, Call Server port, and Uplink port.
9. Click **Apply**.

Variable definitions

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

Table 56: ADAC tab parameters

Variable	Value
AdminEnable	Enables and disables ADAC.
OperEnable	Indicates ADAC operational state: true is enabled and false is disabled.

Variable	Value
	Note: If AdminEnable is True and OperEnable is False, this indicates an error condition such as missing Uplink and Call Server ports.
OperatingMode	Sets the ADAC operation mode: • 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 and disables ADAC trap notifications.
VoiceVLAN	Sets the Voice VLAN ID.
CallServerPort	Sets the Call Server port. The Ethernet Routing Switch 5000 Series supports up to 8 Call Server ports.
UplinkPort	Sets the Uplink port. The Ethernet Routing Switch 5000 Series supports up to 8 Uplink ports.
MacAddrRangeControl	Provides two options for configuring the MAC address range table: • clearTable: clears the MAC address range table. • defaultTable: sets the MAC address range table to its default values.

Configuring ADAC MAC address ranges using EDM

Use this procedure to add MAC address ranges to the ADAC MAC address range table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, click **ADAC**.
3. Select the **ADAC MAC Ranges** tab.
4. Click **Insert**.
5. In the **MacAddrRangeLowEndIndex** field, enter the low-end of the MAC address range to add.

6. In the **MacAddrRangeHighEndIndex** field, enter the high-end of the MAC address range to add.
7. Click **Insert**.

The following table outlines the parameters of the **ADAC MAC Ranges** tab.

Table 57: Variable definitions

Variable	Value
MacAddrRangeLowEndIndex	The MAC address for the low end of the MAC address range.
MacAddrRangeHighEndIndex	The MAC address for the high end of the MAC address range.

Deleting MAC address ranges using Device Manager

Use this procedure to delete MAC address ranges from the ADAC MAC address range table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, click **ADAC**.
3. Select the **ADAC MAC Ranges** tab.
4. Select the desired range to delete.
5. Click **Delete**.

Configuring ADAC settings on a port

Use this procedure to configure ADAC settings on a port.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, click **ADAC**.
3. Select the **ADAC** tab.
4. To enable ADAC for the port, select the **AdminEnable** check box. To disable ADAC for the port, clear the **AdminEnable** check box.
5. Select the **ADAC Ports** tab.
6. In the **TaggedFramesPvid** box, type a number between 0 and 4094, where 0 means "no change."

7. Click on the **TaggedFramesTagging** setting required.
8. Select **MacDetectionEnable** or **LldpDetectionEnable** or select them both to enable the detection methods on the port.
9. Click **Apply**.

Variable definitions

The following table outlines the parameters of the **ADAC Ports** tab.

Table 58: ADAC Ports tab parameters

Variable	Value
AdminEnable	Enables or disables ADAC for the port.
OperEnable	Indicates ADAC operational state: true is enabled and false is disabled. **Note:** If OperEnable is False and AdminEnable is True, then Auto-Detection/Auto-Configuration is disabled. This can occur due to a condition such as reaching the maximum number of devices supported per port.
ConfigStatus	(Read only) Describes the ADAC status for the port: • configApplied means that the ADAC configuration is applied to this port. • configNotApplied means that the ADAC configuration is not applied to this port.
TaggedFramesPVID	Unique PVID between 1 and 4094. A value of 0 indicates that Auto-Configuration cannot change the PVID for the respective port.
TaggedFramesTagging	Choose • tagAll to tag all frames • tagPvidOnly to tag frames by the unique PVID • untagPvidOnly to untag frames by the unique PVID • noChange to accept frames without change
AdacPortType	Describes how ADAC classifies the port: • telephony (when Auto-Detection is enabled for the port) • callServer • uplink • none

Variable	Value
MacDetectionEnable	True indicates that Auto-Detection of Avaya IP Phones, based on MAC address, is enabled on the interface. False indicates that Auto-Detection of Avaya IP Phones, based on MAC address, is disabled on the interface. NOTE: MacDetectionEnable cannot be set to false if no other supported detection mechanism is enabled on the port.
LldpDetectionEnable	True indicates that Auto-Detection of Avaya IP Phones, based on 802.1ab is enabled on the interface. False indicates that Auto-Detection of Avaya IP Phones, based on 802.1ab, is disabled on the interface. NOTE: LldpDetectionEnable cannot be set to False if no other supported detection mechanism is enabled on the port.

Chapter 21: Bridge configuration using Enterprise Device Manager

Bridge information displays the MAC Address Table for the switch.

Displaying basic system bridge information

Use this procedure to display basic system bridge information, including the MAC address, type, and number of ports participating in the bridge.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, click **Bridge**.
3. Select the **Base** tab.

The following table outlines the parameters for the **Base** tab.

Table 59: Variable definitions

Variable	Value
BridgeAddress	Indicates the MAC address of the bridge when it is referred to in a unique fashion. This address must be the smallest MAC address of all ports that belong to the bridge and needs to be unique. When concatenated with dot1dStpPriority, a unique bridge ID is formed that is then used in the Spanning Tree Protocol.
NumPorts	Indicates the number of ports controlled by the bridging entity.
Type	Indicates the type of bridging this bridge can perform. If the bridge is actually performing a certain type of bridging, this fact is indicated by entries in the port table for the given type.

Viewing transparent bridge information

Use this procedure to display information about learned forwarding entries discards and to configure the aging time.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, click **Bridge**.
3. Select the **Transparent** tab.
4. Click **Apply** if the **AgingTime** field is modified.

The following table outlines the parameters for the **Transparent** tab.

Table 60: Variable definitions

Variable	Value
LearnedEntryDiscards	Indicates the number of Forwarding Database entries learned that have been discarded due to insufficient space in the Forwarding Database. If this counter increases, it indicates that the Forwarding Database is becoming full regularly. This condition affects the performance of the subnetwork. If the counter has a significant value and is not presently increasing, it indicates that the problem has occurred but is not persistent.
AgingTime	Indicates the time-out period in seconds for aging out dynamically learned forwarding information. **Note:** The 802.1D-1990 specification recommends a default of 300 seconds.

Viewing forwarding bridge information

Use this procedure to display information about bridge forwarding status.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, click **Bridge**.
3. Select the **Forwarding** tab.
4. To select specific bridge port status information display criteria, click **Filter**.

5. Select filtering criteria.
6. Click **Filter**.

The following table outlines the parameters for the **Forwarding** tab.

Table 61: Variable definitions

Variable	Value
Id	Specifies the VLAN identifier.
Address	Specifies the unicast MAC address for which the bridge has forwarding or filtering information.
Port	Indicates the port number. The source address mut be equal to the value of the corresponding instance of dot1dTpFdbAddress A value of "0" indicates that the port number has not been learned, so the bridge does have the forwarding/filtering information for this address (located in the dot1dStaticTable). You must assign the port value to this object whenever it is learned even for addresses for which the corresponding value of dot1dTpFdbStatus is not learned.
Status	The values of this field include: • invalid: Entry is no longer valid, but has not been removed from the table. • learned: Value of the corresponding instance of dot1dTpFdbPort was learned and is being used. • self: Value of the corresponding instance of dot1dTpFdbAddress represents an address of the bridge. The corresponding instance of dot1dTpFdbPort indicates that a specific port on the bridge has this address. • mgmt(5): Value of the corresponding instance of dot1dTpFdbAddress is also the value of an existing instance of dot1dStaticAddress. • other: None of the preceding. This includes instances where some other MIB object (not the corresponding instance of dot1dTpFdbPort or an entry in the dot1dStaticTable) is being used to determine if a frames addressed to the value of dot1dTpFdbAddress are being forwarded.

Chapter 22: LLDP configuration using Enterprise Device Manager

Use the following procedures to configure and view LLDP global and transmit properties for local and neighbor systems.

Configuring LLDP transmit properties

Use this procedure to configure LLDP transmit properties and view remote table statistics.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **LLDP**.
5. Select the **Globals** tab.

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

Table 62: Variable definitions

Variable	Value
lldpMessageTxInterval	Specifies the interval (in seconds) at which LLDP frames are transmitted on behalf of this LLDP agent.
lldpMessageTx HoldMultiplier	Specifies the time-to-live value expressed as a multiple of the object. The actual time-to-live value used in LLDP frames, transmitted on behalf of this LLDP agent, is expressed by the following formula: TTL = min(65535, (lldpMessageTxInterval *lldpMessageTxHoldMultiplier)) For example, if the value of lldpMessageTxInterval is 30, and the value of lldpMessageTxHoldMultiplier is 4, the value 120 is encoded in the TTL field in the LLDP header.
lldpReinitDelay	Indicates the delay (in seconds) from when the LLDP Port AdminStatus of a particular port is disabled until reinitialization begins.
lldpTxDelay	Indicates the delay (in seconds) between successive LLDP frame transmissions initiated by value or status changes in the

Variable	Value
	LLDP local systems MIB. The recommended value for the lldpTxDelay is set by the following formula: 1 <= lldpTxDelay <= (0.25 * lldpMessageTxInterval)
lldpNotificationInterval	Controls the transmission of LLDP notifications. The agent must not generate more than one lldpRemTablesChange notification-event in the indicated period, where a *notification-event* is the "transmission of a single notification PDU type to a list of notification destinations." If additional changes in lldpRemoteSystemsData object groups occur within the indicated throttling period, these trap-events must be suppressed by the agent. An NMS must periodically check the value of lldpStatsRemTableLastChangeTime to detect any missed lldpRemTablesChange notification-events, for example, due to throttling or transmission loss. If notification transmission is enabled for particular ports, the suggested default throttling period is 5 seconds.
RemTablesLast ChangeTime	Specifies the value of the sysUpTime object (defined in IETF RFC 3418) at the time an entry is created, modified, or deleted in tables associated with the lldpRemoteSystemsData objects, and all LLDP extension objects associated with remote systems. An NMS can use this object to reduce polling of the lldpRemoteSystemsData objects.
RemTablesInserts	Specifies the number of times the complete set of information advertised by a particular MSAP is inserted into tables contained in lldpRemoteSystemsData and lldpExtensions objects. The complete set of information received from a particular MSAP is inserted into related tables. If partial information cannot be inserted for a reason such as lack of resources, all of the complete set of information is removed. This counter is incremented only once after the complete set of information is successfully recorded in all related tables. Any failures occurring during insertion of the information set, which result in deletion of previously inserted information, do not trigger any changes in lldpStatsRemTablesInserts because the insert is not completed yet or in lldpStatsRemTablesDeletes, because the deletion is only a partial deletion. If the failure is the result of a lack of resources, the lldpStatsRemTablesDrops counter is incremented once.
RemTablesDeletes	Specifies the number of times the complete set of information advertised by a particular MSAP is deleted from tables contained in lldpRemoteSystemsData and lldpExtensions objects. This counter is incremented only once when the complete set of information is completely deleted from all related tables. Partial deletions, such as a deletion of rows associated with a particular MSAP, from some tables, but not from all tables, are not allowed, and thus, do not change the value of this counter.

Variable	Value
RemTablesDrops	Indicates the number of times the complete set of information advertised by a particular MSAP can not be entered into tables contained in lldpRemoteSystemsData and lldpExtensions objects because of insufficient resources.
RemTablesAgeouts	Indicates the number of times the complete set of information advertised by a particular MSAP is deleted from tables contained in lldpRemoteSystemsData and lldpExtensions objects because the information timeliness interval has expired. This counter is incremented only once when the complete set of information is completely invalidated (aged out) from all related tables. Partial aging, similar to deletion case, is not allowed, and thus, does not change the value of this counter.
FastStartRepeatCount	Indicates the number of times the fast start LLDPDU is sent during the activation of the fast start mechanism defined by LLDP-MED.

Viewing LLDP remote properties

Use this procedure view LLDP properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **LLDP**.
5. Select the **Neighbor** tab.

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

Table 63: Variable definitions

Variable	Value
TimeMark	Specifies the TimeFilter for this entry. See the TimeFilter textual convention in IETF RFC 2021 for details about TimeFilter.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Specifies an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign

Variable	Value
	monotonically increasing index values to new entries, starting with one, after each reboot.
ChassisIdSubtype	Specifies the type of encoding used to identify the remote system chassis: • chassisComponent • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • local.
ChassisId	Specifies the remote chassis ID.
SysCapSupported	Identifies the system capabilities supported on the remote system.
SysCapEnabled	Identifies the system capabilities that are enabled on the remote system.
SysName	Specifies the remote system name.
SysDesc	Specifies the remote system description.
PortIdSubtype	Specifies the type of encoding used to identify the remote port. • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • agentCircuitId • local
PortId	Specifies the remote port ID.
PortDesc	Specifies the remote port description.

Configuring LLDP ports

Use this procedure to set the optional TLVs to include in the LLPDUs transmitted by each port.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **LLDP**.
5. Select the **Port** tab.

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

Table 64: Variable definitions

Variable	Value
PortNum	Specifies the port number.
AdminStatus	Specifies the administratively desired status of the local LLDP agent: • txOnly: the LLDP agent transmits LLDP frames on this port and does not store any information about the remote systems to which it is connected. • rxOnly: the LLDP agent receives but does not transmit LLDP frames on this port. • txAndRx: the LLDP agent transmits and receives LLDP frames on this port. • disabled: the LLDP agent does not transmit or receive LLDP frames on this port. If the port receives remote systems information which is stored in other tables before AdminStatus is disabled, the information ages out.
NotificationEnable	Controls, for each port, whether notifications from the agent are enabled. • true: indicates that notifications are enabled • false: indicates that notifications are disabled.
TLVsTxEnable	Sets the optional Management TLVs to be included in the transmitted LLDPDUs: • portDesc: Port Description TLV • sysName: System Name TLV

Variable	Value
	• sysDesc: System Description TLV • sysCap: System Capabilities TLV Note: The Local Management tab controls Management Address TLV transmission.
VLANTxEnable(dot1)	Specifies whether the IEEE 802.1 organizationally defined port VLAN TLV transmission is included in the transmitted LLDPDUs.
TLVsTxEnable(dot3)	Sets the optional IEEE 802.3 organizationally defined TLVs to be included in the transmitted LLDPDUs: • macPhyConfigStatus: MAC/PHY configuration/status TLV • powerViaMDI: Power over MDI TLV • linkAggregation: Link Aggregation TLV • maxFrameSize: Maximum-frame-size TLV.
CapSupported(med)	Identifies which MED system capabilities are supported on the local system.
TLVsTxEnable(med)	Sets the optional organizationally defined TLVs for MED devices to include in the transmitted LLDPDUs: • capabilities: Capabilities TLVs • networkPolicy: Network Policy TLVs • location: Emergency Communications System Location TLVs • extendedPSE: Extended PoE TLVs with PSE capabilities • inventory: Hardware Revision, Firmware Revision, Software Revision, Serial Number, Manufacturer Name, Model Name, and Asset ID TLVs.
NotifyEnable(med)	A value of true enables sending the topology change traps on this port. A value of false disables sending the topology change traps on this port.

Displaying LLDP transmit statistics

Use this procedure to view LLDP transmit statistics by port.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **LLDP**.
5. Select the **TX Stats** tab.

The following table outlines the parameters of the **TX Stats** tab.

Table 65: Variable definitions

Variable	Value
PortNum	Specifies the port number.
FramesTotal	Specifies the number of LLDP frames transmitted by this LLDP agent on the indicated port.

Graphing LLDP transmit statistics

Use this procedure To graph LLDP transmit statistics.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **LLDP**.
5. Select the **TX Stats** tab.
6. Click **Graph**.
7. Highlight a data column to graph.
8. Click one of the graph buttons.

Displaying LLDP receive statistics

Use this procedure to view LLDP receive statistics by port.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **LLDP**.
5. Select the **RX Stats** tab.

The following table outlines the parameters of the **RX Stats** tab.

Table 66: Variable definitions

Variable	Value
PortNum	Specifies the port number.
FramesDiscardedTotal	Specifies the number of LLDP frames received on the port and discarded for any reason. This counter provides an indication that LLDP header formatting problems exist with the local LLDP agent in the sending system, or that LLDPDU validation problems exist with the local LLDP agent in the receiving system.
FramesErrors	Specifies the number of invalid LLDP frames received on the port, while the LLDP agent is enabled.
FramesTotal	Specifies the number of valid LLDP frames received on the port, while the LLDP agent is enabled.
TLVsDiscardedTotal	Specifies the number of LLDP TLVs discarded for any reason.
TLVsUnrecognizedTotal	Specifies the number of LLDP TLVs received on a given port that are not recognized by this LLDP agent on the indicated port. An unrecognized TLV is referred to as the TLV whose type value is in the range of reserved TLV types (000 1001 - 111 1110) in Table 9.1 of IEEE 802.1AB-2004. An unrecognized TLV can be a basic management TLV from a later LLDP version.
AgeoutsTotal	Represents the number of age-outs that occurred on a given port. An age-out is "the number of times the complete set of information advertised by a particular MSAP is deleted from tables contained in lldpRemoteSystemsData and lldpExtensions objects because the information timeliness interval has expired." This counter is similar to lldpStatsRemTablesAgeouts, except that it is on a for each-port basis. This enables NMS to poll tables associated with the lldpRemoteSystemsData objects and all LLDP extension objects associated with remote systems on the indicated port only. This counter is set to zero during agent initialization. When the admin status for a port changes from disabled to rxOnly, txOnly or txAndRx, the counter associated with the same port is reset to 0. The agent also flushes all remote system

Variable	Value
	information associated with the same port. This counter is incremented only once when the complete set of information is invalidated (aged out) from all related tables on a particular port. Partial aging is not allowed, and thus, does not change the value of this counter.

Graphing LLDP receive statistics

Use this procedure to graph LLDP receive statistics.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **LLDP**.
5. Select the **RX Stats** tab.
6. Click **Graph**.
7. Highlight a data column to graph.
8. Click one of the graph buttons.

Viewing LLDP local system properties

Use this procedure to view LLDP local system properties.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **LLDP**.
5. Select the **Local System** tab.

The following table outlines the parameters of the **Local System** tab.

Table 67: Variable definitions

Variable	Value
ChassisIdSubtype	Specifies the type of encoding used to identify the local system chassis: • chassisComponent • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • local
ChassisId	Specifies the chassis ID
SysName	Specifies the local system name
SysDesc	Specifies the local system description
SysCapSupported	Identifies the system capabilities supported on the local system
SysCapEnabled	Identifies the system capabilities that are enabled on the local system
DeviceClass	Specifies the local MED device class
HardwareRev	Specifies the vendor-specific hardware revision string as advertised by the local device
FirmwareRev	Specifies the vendor-specific firmware revision string as advertised by the local device
SoftwareRev	Specifies the vendor-specific software revision string as advertised by the local device
SerialNum	Specifies the vendor-specific serial number as advertised by the local device
MfgName	Specifies the vendor-specific manufacturer name as advertised by the local device
ModelName	Specifies the vendor-specific model name as advertised by the local device
AssetID	Specifies the vendor-specific asset tracking identifier as advertised by the local device
DeviceType	Defines the type of Power-via-MDI (Power over Ethernet) advertised by the local device:

Variable	Value
	• pseDevice: indicates that the device is advertised as a Power Sourcing Entity (PSE). • pdDevice: indicates that the device is advertised as a Powered Device (PD) • none: indicates that the device does not support PoE
PSEPowerSource	Defines the type of PSE Power Source advertised by the local device: • primary: indicates that the device advertises its power source as primary • backup: indicates that the device advertises its power source as backup
PDPowerReq	Specifies the value of the power required (in units of 0.1 watts) by a Powered Device (PD)
PDPowerSource	Defines the type of power source advertised as in use by the local device: • fromPSE: indicates that the device advertises its power source as received from a PSE • local: indicates that the device advertises its power source as local • localAndPSE: indicates that the device advertises its power source as using both local and PSE power
PDPowerPriority	Defines the priority advertised as required by this PD: • critical: indicates that the device advertises its power priority as critical, see RFC 3621 • high: indicates that the device advertises its power priority as high, see RFC 3621 • low: indicates that the device advertises its power priority as low, see RFC 3621

Viewing LLDP local port properties

Use this procedure to view LLDP port properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **LLDP**.
5. Select the **Local System** tab.

The following table outlines the parameters of the **Local Port** tab.

Table 68: Variable definitions

Variable	Value
PortNum	Specifies the port number.
PortIdSubtype	Specifies the type of port identifier encoding used in the associated PortId object. • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • agentCircuitId • local.
PortId	Iidentifies the port component associated with a given port in the local system.
PortDesc	Identifies the 802 LAN station port description associated with the local system. If the local agent supports IETF RFC 2863, the PortDesc object has the same value as the ifDescr object.

Viewing LLDP management properites

Use this procedure to view LLDP management properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.

4. From the 802.1AB tree, click **LLDP**.
5. Select the **Local Management** tab.

The following table outlines the parameters of the **Local Management** tab.

Table 69: Variable definitions

Variable	Value
AddrSubtype	Specifies the type of management address identifier encoding used in the associated Addr object.
Addr	Specifies the string value used to identify the management address component associated with the local system. This address is used to contact the management entity.
AddrLen	Specifies the total length of the management address subtype and the management address fields in LLDPDUs transmitted by the local LLDP agent. The management address length field is needed so that the receiving systems that do not implement SNMP are not required to implement an iana family numbers/ address length equivalency table to decode the management address.
AddrIfSubtype	Identifies the numbering method used to define the interface number associated with the remote system. • unknown • ifIndex • systemPortNumber
AddrIfId	Identifies the interface number of the management address component associated with the local system.
AddrOID	Identifies the type of hardware component or protocol entity associated with the management address advertised by the local system agent.
AddrPortsTxEnable	Identifies the ports on which the local system management address TLVs are transmitted in the LLPDUs.

Viewing LLDP remote management properties

Use this procedure to view LLDP management properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.

3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **LLDP**.
5. Select the **Neighbor Mgmt Address** tab.

The following table outlines the parameters of the **Neighbor Mgmt Address** tab.

Table 70: Variable definitions

Variable	Value
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Identifies an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
AddrSubtype	Specifies the type of encoding used in the associated Addr object.
Addr	Identifies the management address associated with the remote system.
AddrIfSubtype	Identifies the numbering method used to define the interface number associated with the remote system. • unknown • ifIndex • systemPortNumber
AddrIfId	Identifies the interface number of the management address component associated with the remote system.
AddrOID	Identifies the type of hardware component or protocol entity associated with the management address advertised by the remote system agent.

Viewing LLDP organizationally-specific properties

Use this procedure to view Organizationally-specific properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.

3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **LLDP**.
5. Select the **Organizational Defined Info** tab.

The following table outlines the parameters of the **Organizational Defined Info** tab.

Table 71: Variable definitions

Variable	Value
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Specifies an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
OrgDefInfoOUI	Specifies the Organizationally Unique Identifier (OUI), as defined in IEEE 802-2001, is a 24 bit (three octets) globally unique assigned number referenced by various standards, of the information received from the remote system.
OrgDefInfoSubtype	Identifies the subtype of the organizationally defined information received from the remote system. The subtype value is required to identify different instances of organizationally defined information that cannot be retrieved without a unique identifier that indicates the particular type of information contained in the information string.
OrgDefInfoIndex	Represents an arbitrary local integer value used by this agent to identify a particular unrecognized organizationally defined information instance, unique only for the OrgDefInfoOUI and lldpRemOrgDefInfoSubtype of the same remote system. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot. It is unlikely that the lldpRemOrgDefInfoIndex will wrap between reboots.
OrdDefInfo	Identifies the organizationally defined information of the remote system. The encoding for this object is the same as that defined for SnmpAdminString TC.

LLDP Port dot1 configuration using Enterprise Device Manager

Use the following procedures to configure the LLDP Port dot1 dialog box and view IEEE 802.1 LLDP information.

Related topics:

Viewing LLDP VLAN ID properties on page 352
Viewing LLDP protocol VLAN properties on page 353
Viewing LLDP VLAN Name properties on page 353
Viewing LLDP protocol properties on page 354
Viewing LLDP VLAN ID properties on page 355
Viewing LLDP Neighbor Protocol VLAN properties on page 355
Viewing LLDP VLAN Name properties on page 356
Viewing LLDP Neighbor Protocol properties on page 357

Viewing LLDP VLAN ID properties

Use this procedure to view LLDP VLAN ID properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **Port dot1**.
5. Select the **Local VLAN Id** tab.

The following table outlines the parameters of the **Local VLAN Id** tab.

Table 72: Variable definitions

Variable	Value
PortNum	Specifies the port number.
VlanId	Specifies the local port VLAN ID. A value of zero is used if the system does not know the PVID.

Viewing LLDP protocol VLAN properties

Use this procedure to view LLDP Protocol VLAN properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **Port dot1**.
5. Select the **Local Protocol VLAN** tab.

The following table outlines the parameters of the **Local Protocol VLAN** tab.

Table 73: Variable definitions

Variable	Value
PortNum	Specifies the port number.
ProtoVlanId	Specifies the ID of the port and protocol VLANs associated with the local port. A value of zero is used if the system does not know the protocol VLAN ID (PPVID).
ProtoVlanSuported	Indicates whether the local port supports port and protocol VLANs.
ProtoVlanEnabled	Indicates whether the port and protocol VLANs are enabled on the local port.
ProtoVlanTxEnable	Indicates whether the corresponding local port and protocol VLAN information are transmitted from the port.

Viewing LLDP VLAN Name properties

Use this procedure to view LLDP VLAN Name properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **Port dot1**.
5. Select the **Local VLAN Name** tab.

The following table outlines the parameters of the **Local VLAN Name** tab.

Table 74: Variable definitions

Variable	Value
PortNum	Specifies the port number.
VlanId	Specifies the integer value used to identify the IEEE 802.1Q VLAN IDs with which the given port is compatible.
VlanName	Indicates the string value used to identify the VLAN name identified by the VLAN ID associated with the given port on the local system. This object contains the value of the dot1QVLANStaticName object (defined in IETF RFC 2674) identified with the given lldpXdot1LocVlanId.
VlanNameTxEnable	Indicates whether the corresponding Local System VLAN name instance is transmitted from the port.

Viewing LLDP protocol properties

Use this procedure to view LLDP protocol properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **Port dot1**.
5. Select the **Local Protocol** tab.

The following table outlines the parameters of the **Local Protocol** tab.

Table 75: Variable definitions

Variable	Value
PortNum	Specifies the port number.
ProtocolIndex	Specifies an arbitrary local integer value used by this agent to identify a particular protocol identity.
ProtocolId	Specifies the octet string value used to identify the protocols associated with the given port of the local system.
ProtocolTxEnable	Indicates whether the corresponding Local System Protocol Identity instance is transmitted on the port.

Viewing LLDP VLAN ID properties

Use this procedure to view LLDP VLAN ID properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **Port dot1**.
5. Select the **Neighbor VLAN Id** tab.

The following table outlines the parameters of the **Neighbor VLAN Id** tab.

Table 76: Variable definitions

Variable	Value
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Specifies an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
VlanId	Specifies the port VLAN identifier associated with the remote system. If the remote system does not know the PVID or does not support port-based VLAN operation, the value is zero.

Viewing LLDP Neighbor Protocol VLAN properties

Use this procedure to view LLDP VLAN ID properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **Port dot1**.
5. Select the **Neighbor Protocol VLAN** tab.

The following table outlines the parameters of the **Neighbor Protocol VLAN** tab.

Table 77: Variable definitions

Variable	Value
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Specifies an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
ProtoVlanId	Specifies the ID of the port and protocol VLANs associated with the remote port. A value of zero is used if the system does not know the protocol VLAN ID (PPVID).
ProtoVlanSuported	Indicates whether the remote port supports port and protocol VLANs.
ProtoVlanEnabled	Indicates whether the port and protocol VLANs are enabled on the remote port.

Viewing LLDP VLAN Name properties

Use this procedure to view LLDP VLAN Name properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **Port dot1**.
5. Select the **Neighbor VLAN Name** tab.

The following table outlines the parameters of the **Neighbor VLAN Name** tab.

Table 78: Variable definitions

Vaiable	Value
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Specifies an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign

Vaiable	Value
	monotonically increasing index values to new entries, starting with one, after each reboot.
VlanId	Indicates the integer value used to identify the IEEE 802.1Q VLAN IDs with which the remote port is compatible.
VlanName	Indicates the VLAN name identified by the VLAN ID associated with the remote system.

Viewing LLDP Neighbor Protocol properties

Use this procedure to view LLDP Protocol properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **Port dot1**.
5. Select the **Neighbor Protocol** tab.

The following table outlines the parameters of the **Neighbor Protocol** tab.

Table 79: Variable definitions

Variable	Value
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Specifies an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
ProtocolIndex	Represents an arbitrary local integer value used by this agent to identify a particular protocol identity.
ProtocolId	Identifies the protocols associated with the remote port.

LLDP Port dot3 configuration using Enterprise Device Manager

Use the following procedures to configure LLDP Port dot3 and view IEEE 802.3 LLDP information.

Related topics:

Viewing LLDP auto-negotiation properties on page 358
Viewing LLDP PoE porperties on page 359
Viewing LLDP link aggregation properties on page 360
Viewing LLDP maximum frame size properties on page 361
Viewing LLDP neighbor auto-negotiation properties on page 361
Viewing LLDP neighbor PoE properties on page 362
Viewing LLDP neighbor link aggregation properties on page 363
Viewing LLDP neighbor maximum frame size properties on page 364

Viewing LLDP auto-negotiation properties

With the Local Port Auto-negotiation tab, you can view LLDP auto-negotiation properties for the local system.

To view the Local Port Auto-negotiation tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Local Port Auto-negotiation** tab.

The following table outlines the parameters of the **Port dot3 Local Port Auto-negotiation** tab.

Table 80: Variable definitions

Variable	Value
PortNum	Port number.
AutoNegSupported	Indicates whether the local port supports Auto-negotiation.

Variable	Value
AutoNegEnabled	Indicates whether Auto-negotiation is enabled on the local port.
AutoNegAdvertisedCap	This object contains the value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) associated with the local port on the system.
OperMauType	A value that indicates the operational MAU type of the given port on the local system.

Viewing LLDP PoE porperties

With the Local PoE tab, you can view LLDP PoE properties for the local system.

To open the Local PoE tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Local PoE** tab.

The following table outlines the parameters of the **Port dot3 Local PoE** tab.

Table 81: Variable definitions

Variable	Value
PortNum	Port number.
PowerPortClass	Identifies the port Class of the local port.
PowerMDISupported	Indicates whether MDI power is supported on the local port.
PowerMDIEnabled	Indicates whether MDI power is enabled on the local port.
PowerPairControlable	Derived from the value of the pethPsePortPowerPairsControlAbility object (defined in IETF RFC 3621), this value is used to indicate whether pair selection can be controlled on the local port.
PowerPairs	This object contains the value of the pethPsePortPowerPairs object (defined in IETF RFC 3621) for the local port: • signal • spare

Variable	Value
PowerClass	This object contains the value of the pethPsePortPowerClassifications object (defined in IETF RFC 3621) for the local port: • class0 • class1 • class2 • class3 • class4

Viewing LLDP link aggregation properties

With the Local Link Aggregate tab, you can view LLDP link aggregation properties for the local system.

To view the Local Link Aggregate tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Local Link Aggregate** tab.

The following table outlines the parameters of the **Port dot3 Local Link Aggregate** tab.

Table 82: Variable definitions

Variable	Value
PortNum	Port number.
LinkAggStatus	Specifies the link aggregation capabilities and the current aggregation status of the link.
LinkAggPortId	Contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component in link aggregation. If the port is not in a link aggregation state or does not support link aggregation, this value is set to zero.

Viewing LLDP maximum frame size properties

With the Local Max Frame tab, you can view LLDP maximum frame size properties for the local system.

To view the Local Max Frame tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Local Max Frame** tab.

The following table outlines the parameters of the **Port dot3 Local Max Frame** tab.

Table 83: Variable definitions

Variable	Value
PortNum	port number
MaxFrameSize	maximum frame size for the port

Viewing LLDP neighbor auto-negotiation properties

With the Neighbor Port Auto-Negotiation tab, you can view LLDP auto-negotiation properties for the remote system.

To view the Neighbor Port Auto-Negotiation tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Neighbor Port Auto-negotiation** tab.

The following table outlines the parameters of the **Port dot3 Neighbor Port Auto-negotiation** tab.

Table 84: Variable definitions

Variable	Value
TimeMark	The TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
AutoNegSupported	The truth value used to indicate whether the given port (associated with a remote system) supports Auto-negotiation.
AutoNegEnabled	Indicates whether Auto-negotiation is enabled on the remote port.
AutoNegAdvertisedCap	This object contains the value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) associated with the remote port.
OperMauType	A value that indicates the operational MAU type of the given port on the remote system.

Viewing LLDP neighbor PoE properties

With the Neighbor PoE tab, you can view LLDP PoE properties for the remote system.

To view the Neighbor PoE tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Neighbor PoE** tab.

The following table outlines the parameters of the **Port dot3 Neighbor PoE** tab.

Table 85: Variable definitions

Variable	Value
TimeMark	The TimeFilter for this entry.

Variable	Value
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PowerPortClass	Identifies the port Class of the remote port.
PowerMDISupported	Indicates whether MDI power is supported on the remote port.
PowerMDIEnabled	Indicates whether MDI power is enabled on the remote port.
PowerPairControlable	Derived from the value of the pethPsePortPowerPairsControlAbility object (defined in IETF RFC 3621), this value is used to indicate whether pair selection can be controlled on the remote port.
PowerPairs	This object contains the value of the pethPsePortPowerPairs object (defined in IETF RFC 3621) for the remote port. • signal • spare
PowerClass	This object contains the value of the pethPsePortPowerClassifications object (defined in IETF RFC 3621) for the remote port. • class0 • class1 • class2 • class3 • class4

Viewing LLDP neighbor link aggregation properties

With the Neighbor Link Aggregate tab, you can view LLDP link aggregation properties for the remote system.

To view the Neighbor Link Aggregate tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.

3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Neighbor Link Aggregate** tab.

The following table outlines the parameters of the **Port dot3 Neighbor Link Aggregate** tab.

Table 86: Variable definitions

Variable	Value
TimeMark	The TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
LinkAggStatus	Specifies the link aggregation capabilities and the current aggregation status of the remote link.
LinkAggPortId	Contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component in link aggregation. If the port is not in a link aggregation state or does not support link aggregation, this value is set to zero.

Viewing LLDP neighbor maximum frame size properties

With the Neighbor Max Frame tab, you can view LLDP maximum frame size properties for the remote system.

To view the Neighbor Max Frame tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Neighbor Max Frame** tab.

The following table outlines the parameters of the **Port dot3 Neighbor Max Frame** tab.

Table 87: Variable definitions

Variable	Value
TimeMark	The TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
MaxFrameSize	Maximum Frame Size for the remote port.

LLDP Port MED configuration using Enterprise Device Manager

Use the following procedures to configure LLDP Port MED and view MED LLDP information.

Related topics:

Viewing local policy properties on page 365
Viewing local location properties on page 366
Viewing coordinate-based location details on page 367
Viewing civic address location details on page 368
Viewing LLDP local PoE PSE properties on page 370
Viewing LLDP neighbor capabilities properties on page 370
Viewing LLDP neighbor policy properties on page 371
Viewing LLDP neighbor location properties on page 372
Viewing coordinate-based location details on page 373
Viewing civic address location details on page 374
Viewing LLDP neighbor PoE properties on page 374
Viewing LLDP neighbor PoE PSE properties on page 375
Viewing LLDP neighbor PoE PD properties on page 376
Viewing LLDP neighbor inventory properties on page 377

Viewing local policy properties

With the Local Policy tab, you can view LLDP policy properties for the local system.

To open the Local Policy tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Local Policy** tab.
6. Click **Insert**. The **Insert Local Policy** dialog box appears.
7. Enter the parameters according to the Variable definitions table.
8. Click **Insert**.

The following table outlines the parameters of the **Port MED Local Policy** tab.

Table 88: Variable definitions

Variable	Value
PortNum	Port number.
PolicyAppType	Voice or voice-signaling application type.
PolicyVlanID	An extension of the VLAN Identifier for the port, as defined in IEEE 802.1P-1998. A value of 1 through 4094 is used to define a valid PVID. A value of 0 is used if the device is using priority tagged frames, meaning that only the 802.1p priority level is significant and the default VID of the ingress port is being used instead. A value of 4095 is reserved for implementation use.
PolicyPriority	Indicates the value of the 802.1p priority which is associated with the local port.
PolicyDscp	This object contains the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the given port on the local system.
PolicyTagged	A value of true indicates that the application is using a tagged VLAN. A value of false indicates that for the specific application, the device is using an untagged VLAN or does not support a port based VLAN operation. In this case, both the VLAN ID and the Layer 2 priority fields are ignored, and only the DSCP value has relevance.

Viewing local location properties

With the Local Location tab, you can view LLDP location properties for the local system.

To open the Local Location tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Local Location** tab.

The following table outlines the parameters of the **Port MED Local Location** tab.

Table 89: Variable definitions

Variable	Value
PortNum	Port number.
LocationSubtype	The location subtype advertised by the remote device: • unknown • coordinateBased • civicAddress • elin
LocationInfo	The location information. The parsing of this information is dependent on the value LocationSubtype.

Viewing coordinate-based location details

You can select and view or configure details for coordinate-based locations listed on the Local Location tab.

To view or configure details for coordinate-based locations:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Local Location** tab.
6. Select a location with the LocationSubtype listed as coordinateBased.

   The Location Detail button is activated.

7. Click the **Location Detail** button to view or configure the local detailed location information. The **Insert Local Location** dialog box appears.
8. Enter the parameters according to the Variable definitions table.
9. Click **Ok**.

The following table outlines the parameters of the **Port MED Coordinate Based Location** dialog box.

Table 90: Variable definitions

Variable	Value
Latitude	Specifies the latitude in degrees, and its relation to the equator (North or South).
Longitude	Specifies the longitude in degrees, and its relation to the prime meridian (East or West).
Altitude	Specifies the altitude, and the units of measurement used (meters or floors).
Map Datum	Specifies the reference datum. The format can be one of the following: • WGS84: World Geodesic System 1984, Prime Meridian Name: Greenwich • NAD83/NAVD88 North American Datum 1983/ North American Vertical Datum of 1988 • NAD83/MLLW: North American Datum 1983/ Mean Lower Low Water •

Viewing civic address location details

Use this procedure to view and configure details for civic address locations.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Local Location** tab.
6. Select a location with the **LocationSubtype** listed as civicAddress
7. Click the **Location Detail** button.

8. Enter details and click **OK**.
9. Click **Close**.

The following table outlines the parameters of the **Port MED Civic Address Location** dialog box.

Table 91: Variable definitions

Variable	Value
Country Code	Country code (2 upper case letters)
State	National subdivisions (state, canton, region)
County	County, parish, gun (JP), district (IN)
City	City, township, shi (JP)
City District	City division, city district, ward
Block (Neighborhood, block)	Neighborhood, block
Street	Street
Leading street direction	Leading street direction
Trailing street suffix	Trailing street suffix
Street suffix	Street suffix
House number	House number
House number suffix	House number suffix
Landmark or vanity address	Landmark or vanity address
Additional Location info	Additional location information
Name (Residence and office occupant)	Residence and office occupant
Postal/Zip code	Postal/Zip code
Building (structure)	Building (structure)
Apartment (suite)	Unit number (apartment, suite)
Floor	Floor
Room number	Room number
Place type	Office
Postal community name	Postal community name
Post office box P.O.Box	Post office box
Additional Code	Additional code

Viewing LLDP local PoE PSE properties

With the Local PoE PSE tab, you can view LLDP PoE PSE properties for the local system.

To view the Local PoE PSE tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Local PoE PSE** tab.

The following table outlines the parameters of the **Port MED Local PoE PSE** tab.

Table 92: Variable definitions

Variable	Value
PortNum	Port number.
PSEPortPowerAvailable	This object contains the value of the power available (in units of 0.1 watts) from the PSE through this port.
PSEPortPDPriority	Indicates the PD power priority that is advertised on this PSE port: • unknown: priority is not configured or known by the PD • critical: the device advertises its power priority as critical, see RFC 3621 • high: the device advertises its power priority as high, see RFC 3621 • low: the device advertises its power priority as low, see RFC 3621

Viewing LLDP neighbor capabilities properties

With the Neighbor Capabilities tab, you can view LLDP capabilities properties for the remote system.

To view the Neighbor Capabilities tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor Capabilities** tab.

The following table outlines the parameters of the **Port MED Neighbor Capabilities** tab.

Table 93: Variable definitions

Variable	Value
TimeMark	The TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
CapSupported	Identifies the MED system capabilities supported on the remote system.
CapCurrent	Identifies the MED system capabilities that are enabled on the remote system.
DeviceClass	Remote MED device class.

Viewing LLDP neighbor policy properties

With the Neighbor Policy tab, you can view LLDP policy properties for the remote system.

To view the Neighbor Policy tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, click **Port MED**.
5. Select the **Neighbor Policy** tab.

The following table outlines the parameters of the **Port MED Neighbor Policy** tab.

Table 94: Variable definitions

Variable	Value
TimeMark	The TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PolicyAppType	Specifies the type of policy which has been applied.
PolicyVlanID	An extension of the VLAN Identifier for the port, as defined in IEEE 802.1P-1998. A value of 1 through 4094 is used to define a valid PVID. A value of 0 is used if the device is using priority tagged frames, meaning that only the 802.1p priority level is significant and that the default VID of the ingress port is being used instead. A value of 4095 is reserved for implementation use.
PolicyPriority	Indicates the value of the 802.1p priority which is associated with the remote system connected to the port.
PolicyDscp	This object contains the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the remote system connected to the port.
PolicyUnknown	A value of true indicates that the network policy for the specified application type is currently unknown. In this case, the VLAN ID, the Layer 2 priority, and the DSCP value fields are ignored. A value of false indicates that this network policy is defined.
PolicyTagged	A value of true indicates that the application is using a tagged VLAN. A value of false indicates that for the specific application, the device is using an untagged VLAN or does not support a port based VLAN operation. In this case, both the VLAN ID and the Layer 2 priority fields are ignored, and only the DSCP value has relevance.

Viewing LLDP neighbor location properties

With the Neighbor Location tab, you can view LLDP location properties for the remote system.

To view the Neighbor Location tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor Location** tab.

The following table outlines the parameters of the **Port MED Neighbor Location** tab.

Table 95: Variable definitions

Variable	Value
TimeMark	The TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
LocationSubtype	The location subtype advertised by the remote device: • unknown • coordinateBased • civicAddress • elin
LocationInfo	The location information advertised by the remote device. The parsing of this information is dependent on the location subtype.

Viewing coordinate-based location details

From the Neighbor Location tab, you can select coordinate-based locations and view details for the remote system.

To view coordinate-based location details:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.

4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor Location** tab.
6. Select a location with the **LocationSubtype** listed as coordinateBased

   The Location Details button is activated.
7. Click the **Location Details** button.

   The Coordinate Based Location window displays the selected location details.
8. Click **Close**.

Viewing civic address location details

From the Neighbor Location tab, you can select civic address locations and view details for the remote system.

To view civic address location details:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor Location** tab.
6. Select a location with the **LocationSubtype** listed as civicAddress

   The Location Details button is activated.
7. Click the **Location Details** button.

   The Civic Address Location window displays the selected location details.
8. Click **Close**.

Viewing LLDP neighbor PoE properties

With the Neighbor PoE tab, you can view LLDP PoE properties for the remote system.

To view the Neighbor PoE tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor PoE** tab.

The following table outlines the parameters of the **Port MED Neighbor PoE** tab.

Table 96: Variable definitions

Variable	Value
TimeMark	The TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PoEDeviceType	The type of PoE device.

Viewing LLDP neighbor PoE PSE properties

With the Neighbor PoE PSE tab, you can view LLDP PoE PSE properties for the remote system.

To view the Neighbor PoE PSE tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor PoE PSE** tab.

The following table outlines the parameters of the **Port MEDNeighbor PoE PSE** tab.

Table 97: Variable definitions

Variable	Value
TimeMark	The TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PSEPowerAvailable	Specifies the power available (in units of 0.1 watts) from the PSE connected remotely to this port.
PSEPowerSource	Defines the type of PSE Power Source advertised by the remote device. • primary: indicates that the device advertises its power source as primary. • backup: indicates that the device advertises its power source as backup.
PSEPowerPriority	Specifies the priority advertised by the PSE connected remotely to the port: • critical: indicates that the device advertises its power priority as critical, see RFC 3621. • high: indicates that the device advertises its power priority as high, see RFC 3621. • low: indicates that the device advertises its power priority as low, see RFC 3621.

Viewing LLDP neighbor PoE PD properties

With the Neighbor PoE PD tab, you can view LLDP PoE PD properties for the remote system.

To view the Neighbor PoE PD tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.

4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor PoE PD** tab.

The following table outlines the parameters of the **Port MED Neighbor PoE PD** tab.

Table 98: Variable definitions

Variable	Value
TimeMark	The TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PDPowerReq	Specifies the value of the power required (in units of 0.1 watts) by a Powered Device (PD) connected remotely to the port.
PDPowerSource	Defines the type of Power Source advertised as being used by the remote device: • fromPSE: indicates that the device advertises its power source as received from a PSE. • local: indicates that the device advertises its power source as local. • localAndPSE: indicates that the device advertises its power source as using both local and PSE power.
PDPowerPriority	Defines the priority advertised as being required by the PD connected remotely to the port: • critical: indicates that the device advertises its power priority as critical, see RFC 3621. • high: indicates that the device advertises its power priority as high, see RFC 3621. • low: indicates that the device advertises its power priority as low, see RFC 3621.

Viewing LLDP neighbor inventory properties

With the Neighbor Inventory tab, you can view LLDP Inventory properties for the remote system.

To view the Neighbor Inventory tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor inventory** tab.

The following table outlines the parameters of the **Port MED Neighbor Inventory** tab.

Table 99: Variable definitions

Variable	Value
TimeMark	The TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
HardwareRev	The vendor-specific hardware revision string as advertised by the remote device.
FirmwareRev	The vendor-specific firmware revision string as advertised by the remote device.
SoftwareRev	The vendor-specific software revision string as advertised by the remote device.
SerialNum	The vendor-specific serial number as advertised by the remote device.
MfgName	The vendor-specific manufacturer name as advertised by the remote device.
ModelName	The vendor-specific model name as advertised by the remote device.
AssetID	The vendor-specific asset tracking identifier as advertised by the remote device.

LLDP MED policy management using Enterprises Device Manager

Use the information in this section to view, create, and edit LLDP MED policies for the switch.

Related topics:

Viewing LLDP MED policies on page 379
Creating LLDP MED policies on page 380
Editing LLDP MED policies on page 381
Deleting LLDP MED policies on page 383

Viewing LLDP MED policies

Use this procedure to view LLDP MED policy properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. In the work area, click the **Local Policy** tab.

Use the data in the following table to help you understand the LLDP MED local policy display.

Table 100: Variable definitions

Field	Description
PortNum	Indicates the port number
PolicyAppType	Shows the policy application type.
PolicyVlanID	Indicates the extension of the VLAN Identifier for the port, as defined in IEEE 802.1P-1998. A value of 1 through 4094 is used to define a valid PVID. A value of 0 is used if the device is using priority tagged frames, meaning that only the 802.1p priority level is significant and the default VID of the ingress port is being used instead. A value of 4095 is reserved for implementation use.

Field	Description
PolicyPriority	Indicates the value of the 802.1p priority which is associated with the local port.
PolicyDscp	Contains the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the given port on the local system.
PolicyTagged	Indicates whether the application is using a tagged VLAN, untagged VLAN, or does not support a port based VLAN operation.

Creating LLDP MED policies

Use this procedure to create a new LLDP MED policy for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. In the work area, click the **Local Policy** tab.
6. Click **Insert** .
7. To select a port to create a policy for, click the **PortNum** elipsis.
8. Click **Ok** .
9. In the **PolicyAppType** section, select one or both boxes.
10. To select a VLAN identifier for the selected port, click the **PolicyVlanID** elipsis.
11. Click **Ok** .
12. Double-click the **PolicyPriority** box.
13. Type a priority value.
14. Double-click the **PolicyDscp** box.
15. Type a DSCP value.
16. To use a tagged VLAN, click the **PolicyTagged** box.

    OR

    To use an untagged VLAN, clear the **PolicyTagged** box.
17. Click **Insert** .

Use the data in the following table to create a new LLDP MED policy for the local system.

Table 101: Variable definitions

Field	Description
PortNum	Specifies the port on which to configure LLDP MED policies.
PolicyAppType	Specifies the policy application type. • voice—selects the voice network policy • voiceSignaling—selects the voice signaling network policy
PolicyVlanID	Specifies the VLAN identifier for the selected port or ports. Values range from 1–4094. If you select priority tagged frames, the system recognizes only the 802.1p priority level and uses a value of 0 for the VLAN ID of the ingress port.
PolicyPriority	Specifies the value of the 802.1p priority that applies to the selected switch port or ports. Values range from 0–7.
PolicyDscp	Specifies the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the selected switch port or ports. Values range from 0–63.
PolicyTagged	Specifies the type of VLAN tagging to apply on the selected switch port or ports. • when selected—uses a tagged VLAN • when cleared—uses an untagged VLAN or does not support port-based VLANs. If you select untagged, the system ignores the VLAN ID and priority values, and recognizes only the DSCP value.

Editing LLDP MED policies

Use this procedure to edit a previously configured LLDP MED policy for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.

3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. To select a policy to edit, click the PortNum.
6. In the policy row, double-click the cell in the**PolicyVlanID** column.
7. Select a VLAN from the list.
8. Click **Ok** .
9. In the policy row, double-click the cell in the**PolicyPriority** column.
10. Edit the policy priority value.
11. In the policy row, double-click the cell in the**PolicyDscp** column.
12. Edit the policy DSCP value.
13. In the policy row, double-click the cell in the**PolicyTagged** column.
14. Select a value from the list.
15. On the toolbar, click **Apply** .

Use the data in the following table to edit a previously configured LLDP MED policy for the local system.

Table 102: Variable definitions

Field	Description
PortNum	Indicates the port on which to configure LLDP MED policies. This is a read-only cell.
PolicyAppType	Indicates the policy application type. This is a read-only cell. • voice— voice network policy • voiceSignaling— voice signaling network policy
PolicyVlanID	Specifies the VLAN identifier for the selected port or ports. Values range from 1–4094. If you select priority tagged frames, the system recognizes only the 802.1p priority level and uses a value of 0 for the VLAN ID of the ingress port.
PolicyPriority	Specifies the value of the 802.1p priority that applies to the selected switch port or ports. Values range from 0–7.
PolicyDscp	Specifies the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the selected switch port or ports. Values range from 0–63.

Field	Description
PolicyTagged	Specifies the type of VLAN tagging to apply on the selected switch port or ports. • true—uses a tagged VLAN • false—uses an untagged VLAN or does not support port-based VLANs. If you select untagged, the system ignores the VLAN ID and priority values, and recognizes only the DSCP value.

Deleting LLDP MED policies

Use this procedure to delete a LLDP MED policy.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. In the work area, click the **Local Policy** tab.
6. To select a policy to delete, click the PortNum.
7. On the toolbar, click **Delete** .

Configuring LLDP Timers using EDM

Use the following procedure to configure LLDP Timers.

Note:

LLDP timers apply to the entire device and can not be configured by port.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.

5. In the LLDP work area, click the **Globals** tab.
6. In the Globals section, configure timers as required.
7. On the toolbar, click **Apply**.
8. On the toolbar, you can click **Refresh** to verify the configuration.

Variable definitions

The following table describes the variables associated with configuring LLDP timers.

Variable	Value
lldpMessageTxInterval	Indicates interval, in seconds, at which LLDP frames are transmitted on behalf of this LLDP agent. DEFAULT: 30s
lldpMessageTxHoldMultiplier	Indicates the time-to-live value expressed as a multiple of the object. The actual time-to-live value used in LLDP frames, transmitted on behalf of this LLDP agent, is expressed by the following formula: TTL = min(65535, (lldpMessageTxInterval *lldpMessageTxHoldMultiplier). DEFAULT: 4s
lldpReinitDelay	Indicates the delay (in seconds) from when the LLDP Port AdminStatus of a particular port is disabled until reinitialization begins. DEFAULT: 2s
lldpTxDelay	Indicates the delay (in seconds) between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB. The recommended value for the lldpTxDelay is set by the following formula: 1 <= lldpTxDelay <= (0.25 * lldpMessageTxInterval) DEFAULT: 2s
lldpNotificationInterval	Controls the transmission of LLDP notifications. DEFAULT: 5s

Enabling or disabling Avaya TLV transmit flags

Use this procedure to enable or disable the transmission of optional proprietary Avaya TLVs from switch ports to Avaya IP phones.

Procedure steps

1. From the navigation pane, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics work area, click **802.1AB** .
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Port Config** tab.
6. To select a port, click the **PortNum**.
7. In the port row, double-click the cell in the **TLVsTxEnable** column.
8. Select a checkbox to enable a TLV.

   OR

   Clear a checkbox to disable a TLV.
9. Click **Ok**.
10. On the toolbar, click **Apply**.

Variable definitions

Variable	Value
poeConservationLevel	Enables or disables the TLV for requesting a specific power conservation level for an Avaya IP phone connected to the switch port. ❗ **Important:** Only Ethernet ports on switches that support PoE can request a specific power conservation level for an Avaya IP phone.
callServer	Enables or disables the TLV for advertising call server IPv4 addresses to an Avaya IP phone connected to the switch port.

Variable	Value
fileServer	Enables or disables the TLV for advertising file server IPv4 addresses to an Avaya IP phone connected to the switch port.
framingTlv	Enables or disables the frame tagging TLV for exchanging Layer 2 priority tagging information between the switch and an Avaya IP phone.

Configuring the PoE conservation level request TLV

Use this procedure to request a specific power conservation level for an Avaya IP phone connected to a switch port.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**
4. In the 802.1AB tree, click **Avaya**
5. In the Avaya work area, click the **Local Port** tab.
6. Click **PortNum** to select a port.
7. In the port row, configure as required.
8. On the toolbar, click **Apply**.

Variable definitions

The following table describes the variables associated with configuring the PoE conservation level request TLV.

Variable	Value
PoeConsLevelRequest	Specifies the power conservation level to request for a vendor specific PD. RANGE: 0–255 DEFAULT: 0 With the default value of 0, the switch does not request a power conservation level for an Avaya IP phone connected to the port.

Configuring the 802.1Q framing TLV

Use this procedure to configure the frame tagging mode for exchanging Layer 2 priority tagging information between the switch and an Avaya IP phone.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the Avaya work area, click the **Local Port** tab.
6. Click **PortNum** to select a port.
7. In the port row, configure as required.
8. On the toolbar, click **Apply**.

Variable definitions

The following table describes the variables associated with configuring 802.1Q framing TLV.

Variable	Value
Dot1QFramingRequest	Specifies the frame tagging mode. Values include: • tagged—frames are tagged based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. • non-tagged—frames are not tagged with 802.1Q priority. • auto—an attempt is made to tag frames based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. If there is no LLDPMED Network Policy information available, an attempt is made to tag frames based on server configuration. If that fails, traffic is transmitted untagged. DEFAULT: Auto

Configuring the switch call server IP address TLV

Use this procedure to define the local call server IP addresses that switch ports can advertise to Avaya IP phones.

You can define IP addresses for a maximum of 8 local call servers.

Important:

The switch does not support the advertisement of IPv6 addresses to Avaya IP phones.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the Avaya work area, click the **Local Call Servers** tab.
6. Click **CallServerNum** to select a port.
7. In the port row, configure as required.
8. On the toolbar, click **Apply**.

Variable definitions

The following table describes the variables associated with the Local Call Servers tab.

Variable	Value
CallServerNum	Displays the call server number.
CallServerAddressType	Displays the call server IP address type.
CallServerAddress	Defines the local call server IP address to advertise.

Configuring the switch file server IP address TLV

Use this procedure to define the local file server IP addresses that switch ports can advertise to Avaya IP phones.

You can define IP addresses for a maximum of 4 local call servers.

Note:

If your Avaya IP Handset uses SIP, 802.1AB (LLDP) TLVs do not provide all information for the IP Phone. You must specify a file server IP address TLV so the IP phone can download the SIP configuration information, because the IP Phone retrieves information related to the SIP domain, port number and transport protocol from the file server.

Important:

The switch does not support the advertisement of IPv6 addresses to Avaya IP phones.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the Avaya work area, click the **Local File Servers** tab.
6. Click **FileServerNum** to select a port.
7. In the port row, configure as required.
8. On the toolbar, click **Apply**.
9. On the toolbar, you can click **Refresh** to verify the configuration.

Variable definitions

The following table describes the variables associated with the Local File Servers tab

Variable	Value
FileServerNum	Displays the file server number.
FileServerAddressType	Displays the file server IP address type.
FileServerAddress	Defines file server IP address to advertise.

Viewing Avaya IP phone power level TLV information

Use this procedure to display power level information received on switch ports from an Avaya IP phone.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the Avaya work area, click the **Neighbor Devices** tab.

Variable definitions

The following table describes the variables associated with the neighbor devices tab.

Variable	Value
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
CurrentConsLevel	Displays the PoE conservation level configured on the Avaya IP phone connected to the switch port.
TypicalPower	Displays the average power level used by the Avaya IP phone connected to the switch port.
MaxPower	Displays the maximum power level for the Avaya IP phone connected to the switch port.

Viewing remote call server IP address TLV information

Use this procedure to display call server IP address information received on switch ports from an Avaya IP phone.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor Call Servers** tab.

Variable definitions

Variable	Value
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
PortCallServerAddressType	Displays the call server IP address type used by the Avaya IP phone connected to the switch port.
PortCallServerAddress	Displays the call server IP address used by the Avaya IP phone connected to the switch port.

Viewing remote file server IP address TLV information

Use this procedure to display file server IP address information received on switch ports from an Avaya IP phone.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor File Servers** tab.

Variable definitions

Variable	Value
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
PortFileServerAddressType	Displays the file server IP address type used by the Avaya IP phone connected to the switch port.
PortFileServerAddress	Displays the file server IP address used by the Avaya IP phone connected to the switch port.

Viewing PoE conservation level support TLV information

Use this procedure to display PoE conservation level information received on switch ports from an Avaya IP phone.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor PoE** tab.

Variable definitions

Variable	Value
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
PoeConsLevelValue	Displays the PoE conservation level supported by the Avaya IP phone connected to the switch port.

Viewing remote 802.1Q Framing TLV information

Use this procedure to display Layer 2 frame tagging mode information received on switch ports from connected Avaya IP phones.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor Dot1Q** tab.

Variable definitions

Variable	Value
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.

Variable	Value
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
Dot1QFraming	Displays the Layer 2 frame tagging mode for the Avaya IP phone connected to the switch port. Values include: • tagged—frames are tagged based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. • non-tagged—frames are not tagged with 802.1Q priority. • auto—an attempt is made to tag frames based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. If there is no LLDP-MED Network Policy information available, an attempt is made to tag frames based on server configuration. If that fails, traffic is transmitted untagged. • The default tagging mode is auto.

Viewing remote IP TLV information

Use this procedure to display IP address configuration information received on switch ports from connected Avaya IP phones.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor IP Phone** tab.

Variable definitions

Variable	Value
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
PortPhoneAddressType	Displays the IP address type for the Avaya IP phone connected to the switch port.
PortPhoneAddress	Displays the IP address for the Avaya IP phone connected to the switch port.
PortPhoneAddressMask	Displays the IP address subnet mask for the Avaya IP phone connected to the switch port.
PortPhoneGatewayAddress	Displays gateway IP address for the Avaya IP phone connected to the switch port.

Appendix A: LACP over SMLT configuration example

This appendix shows you how to configure LACP over SMLT.

LACP over SMLT configuration example

The following configuration example shows you how to configure LACP over SMLT.

The configuration is a triangle SMLT in which A and B are SMLT aggregation switches and C is the edge switch. The MAC address for switch A is 00:aa:aa:aa:aa:00; for switch B, 00:bb:bb:bb:bb:00: and C, 00:cc:cc:cc:cc:00.

Prerequisites

- Ports 3 and 4 of switches A and B are SMLT ports.
- LACP is enabled on ports 1–4 of edge switch C, ports 3 and 4 of switch A, and ports 3 and 4 of switch B, .
- The switches are all in Global Configuration mode.

Switch A configuration

Use the following procedure to configure switch A.

Procedure steps

1. Prevent loops by configuring the switch in advance mode:

   ```
   lacp port-mode advance
   ```

2. Select switch A base MAC (00:aa:aa:aa:aa:00) as the system MAC and configure the LAC system MAC for SMLT:

```
lacp smlt sys-id 00:aa:aa:aa:aa:00
```

3. Place switch A in interface mode:

   ```
   interface fastethernet 3,4
   ```

4. Assign key 2 to ports 3 and 4

   ```
   lacp key 2
   ```

5. Enable LACP on ports 3 and 4:

   ```
   lacp mode active
   ```

6. Return switch A to Global Configuration mode:

   ```
   exit
   ```

7. Bind MLT 30 to key 2. This command tells MLT application to reserve MLT 30 for LACP key 2. Otherwise MLT will dynamically allocate an unused MLT # for LACP. Populate SMLT ID to the reserved trunk to make it SMLT enabled.

   ```
   lacp key 2 mlt 30 smlt 2
   ```

8. Enable MLT1 with ports 1 and 2.

   ```
   mlt 1 en mem 1-2
   ```

9. Set MLT 1 as the IST trunk.

   ```
   int mlt 1
   ```

10. Set the IST VLAN ID as 10 and the IST peer IP address as 10.30.20.101.

    ```
    ist enable peer-ip 10.30.20.101 vlan 10
    ```

11. Return switch A to the Global Configuration mode:

    ```
    exit
    ```

Switch B configuration

Use the following procedure to configure switch B.

Procedure steps

1. Prevent loops by configuring the switch in advance mode:

   ```
   lacp port-mode advance
   ```

2. Select switch A base MAC (00:aa:aa:aa:aa:00) as the system MAC and configure the LAC system MAC for SMLT:

```
lacp smlt sys-id 00:aa:aa:aa:aa:00
```

3. Place switch A in interface mode:

   ```
   interface fastethernet 5
   ```

4. Assign key 2 to ports 3 and 4:

   ```
   lacp key 2
   ```

5. Enable LACP on ports 3 and 4:

   ```
   lacp mode active
   ```

6. Return switch B to the Global Configuration mode:

   ```
   exit
   ```

7. Bind MLT 30 to key 2. This command instructs the MLT application to reserve MLT 30 for LACP key 2. Otherwise MLT will dynamically allocate an unused MLT number for LACP. Populate SMLT ID to the reserved trunk to make it SMLT-enabled.

   ```
   lacp key 2 mlt 30 smlt 2
   ```

8. Enable MLT1 with ports 1 and 2.

   ```
   mlt 1 en mem 1-2
   ```

9. Set MLT 1 as the IST trunk.

   ```
   int mlt 1
   ```

10. Set the IST VLAN ID as 10 and the IST peer IP address as 10.30.20.101.

    ```
    ist enable peer-ip 10.30.20.100 vlan 10
    ```

11. Return switch B to the Global Configuration mode:

    ```
    exit
    ```

Switch C configuration

Use the following procedure to configure switch C.

Procedure steps

1. Prevent loops by configuring the switch in advance mode:

   ```
   lacp port-mode advance
   ```

2. Place switch C in interface mode:

```
interface fastethernet 1-4
```

3. Enable LACP on ports 1–4:

```
lacp mode active
```

```
e
```

4. Disable STP participation on ports 1–4 in all STGs:

```
spanning-tree port 1–4 stp <1–8> learning disable
```

5. Return switch C to the Global Configuration mode:

```
exit
```

Index

A

ActorAdminKey field 314
ActorLagID field 314
ActorOperKey field 314
ActorSystemID field 314
ADAC 128–130, 132, 134, 136, 215
  and stacking 134
  configuring using CLI 215
  initial user settings 128
  operating modes 129
  Tagged-Frames operating mode 132
  Untagged-Frames-Advanced operating mode 130
  Untagged-Frames-Basic Operating Mode 130
  User Restrictions 136
ADAC and EAP 135
adac command (global) 215
adac command (per port) 217
Add VLAN Membership field 42, 56
AdminEdgePort field 288
AdminEdgeStatus field 295
AdminP2P field 295
AdminPathCost field 284
AdminPointToPoint field 288
AggregateOrIndividual field 314

B

BPDU Filtering 41
BrgAddress field 292
Bridge Forward Delay field 47, 53, 61
Bridge Forward Delay Time field 42, 50, 56
Bridge Hello Time field 42, 47, 50, 53
Bridge Hold Time field 61
Bridge Max. Age Time field 42, 50, 56
Bridge Maximum Age Time field 47, 53, 61
Bridge parameter 333, 334
  Base tab 333
    BridgeAddress field 333
    NumPorts field 333
    Type 333
  Forwarding tab 334
    Address field 334
    Port field 334
    Status field 334
Bridge Priority (in Hex) field 42, 50
Bridge Priority field 47, 53, 56, 61
Bridge Tx Hold Count 56
Bridge Tx Hold Count field 50
BridgeForwardDelay field 286, 292
BridgeHelloTime field 286
BridgeInstance field 301
BridgeMaxAge field 286, 292
BridgePriority field 292

C

CIST Root field 61
clear mac-address-table 156
clear mac-address-table address 157
clear mac-address-table interface FastEthernet 157
clear mac-address-table interface mlt 157
clear mac-address-table interface vlan 157
CollectorMaxDelay field 314
CompatibilityMode field 313
ConfigDigest field 292
ConfigIdSel field 292
configuration 190
  SLT 190
configuring SMLT 187
  config mlt ist, create ip vlan-id 187
Create STP Group field 42, 56
CurrentPortRole field 295, 301

D

default adac command 216
default adac command (per port) 217
default adac port enable command 220
default mac-address-table aging-time 156
Default Path Cost Type 56
Default Path Cost Type field 50, 53, 61
DefaultVLANId field 270
Delete STP Group field 42, 56
Delete VLAN Membership field 42, 56
Designated Root field 47, 53
DesignatedBridge field 284, 288, 295, 301
DesignatedCost field 284, 288, 295, 301
DesignatedPort field 284, 288, 295, 301
DesignatedRoot field 284, 286, 288, 295, 301
DHCP 30
Display Spanning Tree Switch Settings option 42, 50, 56
Display Spanning Tree VLAN Membership option 42
Dynamic Host Configuration Protocol (DHCP) 30

E

EAP and ADAC 135
Edge field 52, 59
EffectivePortState field 290, 295, 301
Enable Stp field 284
Enabled field 298

F

FastStart field 284
FilterTaggedFrames field 270
ForcePortState field 295, 301
ForceProtocolVersion field 292
Forward Delay field 47, 53, 61
ForwardDelay field 286, 292
Forwarding tab 334
ForwardTransitions field 284, 288, 297, 302

H

Hello Time field 47, 53
HelloTime field 295
HelloTime time 286
HoldTime field 292
Hop Count field 61

I

Index field 314
Instance field 298
InstanceDownCount field 298
InstanceUpCount field 298
Inter-switch trunk (IST) 96
  about 96
InvalidBPDUsRcvd field 302
InvalidConfigBpduRxCount field 297
InvalidMstBpduRxCount field 297
InvalidRstBpduRxCount field 297
InvalidTcnBpduRxCount field 297
IP directed broadcasting 158
  configuring with CLI 158
IST 96
  about 96
  aggregation switch processes 96
  single point of failure 96

L

LACP 117, 203, 313
  configuring with Device Manager 313
  configuring with the CLI 203
  port mode 117
Learning field 52, 59
Link aggregation 115

M

MAC address forwarding database table 155
  configuring with CLI 155
mac-address-table aging-time command 156
MacAddress field 314
Max. Hop Count 56
MaxAge field 286, 292
MaxHopCount field 292
Maximum Age Time field 47, 53, 61
MLT 65, 67
  configuration rules 67
MLT and STP 70
MLT load-balancing 68
MSTP 171
  configuring using CLI 171
MSTP mode 56
  Display Spanning Tree Switch Settings option 56
  Spanning Tree Port Configuration option 56
MstpDownCount field 292
MstpUpCount field 292
Mutlilink trunks 65

N

NewRootBridgeCount field 292
NewRootCount field 298
NewRootIdCount field 286
NoOfInstancesSupported field 292

O

OperEdgePort field 288
OperEdgeStatus field 295
OperP2P field 295
OperPointToPoint field 288
OperVersion field 290, 295
options 56
  Display Spanning Tree Switch Settings 56
  Spanning Tree Group Configuration 56
  Spanning Tree Port Configuration 56

P

Participating field 288

Participation field 45
PartnerLagID field 314
PartnerOperKey field 314
PartnerSystemID field 314
PartnerSystemPriority field 314
Path Cost field 45, 52, 59
PathCost field 284, 288, 295, 301
PathCostDefault 286
PathCostDefaultType field 292
Port field 45, 52, 59, 288, 290, 295, 301
Priority field 45, 52, 59, 284, 286, 288, 295, 298, 301
ProtocolMigration field 288, 295
ProtocolMigrationCount field 297

R

ReceivedBPDUs field 302
Region Name field 61
Regional Root field 61
Regional Root Path Cost 61
RegionalPathCost field 295
RegionalRoot field 292, 295, 298
RegionalRootCost field 292
RegionConfigChangeCount field 292
RegionName field 292
RegionVersion field 292
Role field 52, 59, 290
Root field 292
Root Path Cost field 47, 53, 61
Root Port field 47, 53, 61
RootCost field 286, 292, 298
RootPort field 286, 292, 298
RSTP 168
    configuring using CLI 168
RSTP mode 50
    Display Spanning Tree Switch Settings 50
    Spanning Tree Group Configuration 50
    Spanning Tree Port Configuration 50
RstpDownCount field 286
RstpUpCount field 286
RxConfigBpduCount field 297
RxMstBpduCount field 297
RxRstBpduCount field 297
RxTcnBpduCount field 297

S

SelectedPortRole field 295
show adac command 221
show adac interface command 221
show mac-address-table command 155
SLT 98
    about 98
SMLT 74–76, 80, 94, 96, 97, 185
    advantages 75
    configuring with the CLI 185
    square configuration 80
    stack configuration 94
    triangle configuration 76
    advantages 75
    end station configuration example 97
    IST 96
    STP convergence resolution 75
    traffic flow examples 97
SMLT configuration steps 102
Spanning Tree Configuration Menu screen 50
Spanning Tree Configuration Menu screen in MSTP
        mode 56
Spanning Tree Group Configuration option 42, 50
Spanning Tree Group Configuration screen 42
Spanning Tree Group Configuration screen in MSTP
        mode 56
Spanning Tree Group Configuration screen in RSTP
        mode 50
Spanning Tree Port Configuration option 42, 50, 56
Spanning Tree Port Configuration screen 45
Spanning Tree Port Configuration screen in MSTP mode
       59
Spanning Tree Port Configuration screen in RSTP mode
       52
Spanning Tree Switch Settings screen 47
Spanning Tree Switch Settings screen in MSTP mode 61
Spanning Tree Switch Settings screen in RSTP mode 53
Spanning Tree VLAN Membership screen 49, 63
Split Multi-Link Trunking (SMLT) 74
State field 45, 52, 59, 284, 288, 295, 301
STG 33
StgId field 284
STGs 160
    configuring using CLI 160
STP and MLT 70
STP BPDU Filtering 159
    Configuring with CLI 159
STP Group 49
STP Group field 45, 47, 59, 61, 63
STP Group State field 42, 56
STP mode 159
    settings using CLI 159
STP mode field 56
STP Mode field 42, 45, 47, 50, 53
STP Multicast Address field 42
STPG mode 42

Display Spanning Tree Switch Settings option 42
Display Spanning Tree VLAN Membership option 42
Spanning Tree Group Configuration option 42
Spanning Tree Port Configuration option 42

T

Tagged BPDU on tagged port field 42
TimeSinceTopologyChange field 286, 292, 298
TLVs 139, 140
IEEE 802.1 organizationally-specific 140
IEEE 802.3 organizationally-specific 140
Management 139
Organizationally-specific for MED devices 140
TopChanges field 286, 292, 298
TransmittedBPDUs field 302
Transparent tab 334
troubleshooting 56
spanning tree groups 56
VLANs 56
Troubleshooting ISTs 200
Trunk field 45, 52, 59
Tx Hold Count field 53, 61
TxConfigBpduCount field 297
TxHoldCount field 292
TXHoldCount field 286
TxMstBpduCount field 297
TxRstBpduCount field 297
TxTcnBpduCount field 297

U

Unit field 45, 52

V

VCC 153
configuring with CLI 153
Version field 286
VID used for tagged BPDU field 42
VLACP 119, 209, 317
configuring with Device Manager 317
configuring with the CLI 209
VLAN Configuration Control 153
configuring with CLI 153
VLAN Membership field 49, 63
VlanIds 334
VlanIds field 270
VLANs 145
configuring with CLI 145