



ExtremeSwitching™

Configuring VLANs, Spanning Tree, and MultiLink Trunking on Ethernet Routing Switch 3500 Series

Release 5.3.6
NN47203-500
Issue 05.01
December 2017

© 2017, Extreme Networks, Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Extreme Networks shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Extreme Networks. End User agrees to indemnify and hold harmless Extreme Networks, Extreme Networks' 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

Extreme Networks is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Extreme Networks. Extreme Networks 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. Extreme Networks does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Extreme Networks provides a limited warranty on Extreme Networks hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Extreme Networks' standard warranty language, as well as information regarding support for this product while under warranty is available to Extreme Networks customers and other parties through the Extreme Networks Support website: <http://www.extremenetworks.com/support> under the link "Policies" or such successor site as designated by Extreme Networks. Please note that if You acquired the product(s) from an authorized Extreme Networks Channel Partner outside of the United States and Canada, the warranty is provided to You by said Extreme Networks Channel Partner and not by Extreme Networks.

"Hosted Service" means an Extreme Networks hosted service subscription that You acquire from either Extreme Networks or an authorized Extreme Networks Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Extreme Networks or Extreme Networks Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, <https://extremeportal.force.com> OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU

REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

Extreme Networks grants You a license within the scope of the license types described below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Extreme Networks or an Extreme Networks Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Extreme Networks in writing. Extreme Networks may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Extreme Networks through electronic means established by Extreme Networks specifically for this purpose.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part,

including any code and software unless expressly authorized by Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and/or use without the express written consent of Extreme Networks can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Extreme Networks Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Extreme Networks' website at: <http://www.extremenetworks.com/support/policies/software-licensing> or such successor site as designated by Extreme Networks. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Service Provider

THE FOLLOWING APPLIES TO EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS MUST BE AUTHORIZED IN WRITING BY EXTREME NETWORKS AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE EXTREME NETWORKS CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE EXTREME NETWORKS CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR

THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Extreme Networks product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Security Vulnerabilities

Information about Extreme Networks' security support policies can be found in the Global Technical Assistance Center Knowledgebase at <https://gtacknowledge.extremenetworks.com/>.

Downloading Documentation

For the most current versions of Documentation, see the Extreme Networks Support website: <http://documentation.extremenetworks.com>, or such successor site as designated by Extreme Networks.

Contact Extreme Networks Support

See the Extreme Networks Support website: <http://www.extremenetworks.com/support> for product or Hosted Service notices and articles, or to report a problem with your Extreme Networks product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Extreme Networks Support website: <http://www.extremenetworks.com/support/contact/> (or such successor site as designated by Extreme Networks), scroll to the bottom of the page, and select Contact Extreme Networks Support.

Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Extreme Networks are the registered or unregistered Marks of Extreme Networks, Inc., its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Extreme Networks or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(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 Extreme Networks or the applicable third party.

Extreme Networks is a registered trademark of Extreme Networks, Inc.

All non-Extreme Networks trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

For additional information on Extreme Networks trademarks, please see: <http://www.extremenetworks.com/company/legal/>

Contents

Chapter 1: Preface	12
Purpose.....	12
Training.....	12
Providing Feedback to Us.....	12
Getting Help.....	12
Extreme Networks Documentation.....	13
Subscribing to service notifications.....	14
Chapter 2: New in this document	15
Chapter 3: VLAN Fundamentals	16
CLI command modes.....	16
Virtual local area networks.....	17
VLAN support.....	18
IEEE 802.1Q VLAN workgroups.....	18
IEEE 802.1Q tagging.....	19
VLAN Tagging Enhancement.....	22
VLAN Configuration Control.....	22
VLANs spanning multiple switches.....	23
VLANs spanning multiple 802.1Q tagged switches.....	24
VLANs spanning multiple untagged switches.....	24
Shared servers.....	26
VLAN workgroup summary.....	27
VLAN configuration rules.....	29
MAC Flush.....	29
Voice VLAN Integration.....	30
Storm Control.....	30
MLT/DMLT/LAG Dynamic VLAN changes.....	31
Chapter 4: Spanning Tree Protocol Fundamentals	32
Spanning Tree Protocol.....	32
Port states.....	32
STP port mode.....	33
STP 802.1d compliance mode.....	33
Aging of dynamic entries in Forwarding Database.....	33
Port path cost.....	34
802.1t path cost calculation.....	34
Rapid Spanning Tree Protocol.....	34
Multiple Spanning Tree Protocol.....	35
Interoperability with legacy STP.....	35
Differences in port roles.....	35
Edge port.....	36

Path cost values.....	36
Rapid convergent.....	37
Negotiation process.....	37
Spanning Tree BPDU Filtering.....	38
Static STP Multicast Destination Configuration.....	39
Chapter 5: Multi-Link Trunking Fundamentals.....	41
About Multi-Link Trunking.....	41
MLT operation.....	41
MLT configuration examples.....	42
Client server configuration using Multi-Link Trunks.....	43
Before you configure trunks.....	44
Spanning tree considerations for Multi-Link Trunks.....	45
Additional tips about the Multi-Link Trunking feature.....	45
MLT enable or disable whole trunk.....	46
Distributed Multi-Link Trunk.....	46
Distributed LAG (802.3ad) LACP.....	47
SLPP Guard.....	47
Chapter 6: LACP And VLACP Fundamentals.....	49
IEEE 802.3ad Link Aggregation.....	49
Static LACP key to trunk ID binding.....	51
VLACP.....	51
Virtual LACP overview.....	52
VLACP features.....	53
Chapter 7: ADAC Fundamentals.....	55
ADAC operation.....	56
Auto-Detection of IP phones.....	56
Auto-Detection by MAC address.....	56
Auto-Detection by LLDP (IEEE 802.1AB).....	58
ADAC and 802.1AB interoperability.....	58
Auto-Configuration of IP phones.....	58
Chapter 8: VLAN configuration.....	60
Displaying VLANs by type.....	60
Displaying VLAN settings per port.....	61
Displaying verbose VLAN interface information.....	61
Displaying port membership.....	62
Setting or resetting a management VLAN.....	62
Deleting a management VLAN IP address.....	63
Displaying VLAN ID.....	63
Creating a VLAN.....	63
Deleting a VLAN.....	64
Configuring VLAN name.....	65
Disabling a voice VLAN.....	66
Displaying VLAN Configuration Control settings.....	66

Modifying VLAN Configuration Control settings.....	66
Enabling or disabling automatic PVID	67
Displaying automatic PVID status.....	68
Configuring VLAN settings per port.....	68
Configuring VLAN members.....	69
MAC address table configuration.....	69
Displaying the MAC address forwarding table	70
Configuring aging time for unseen MAC addresses.....	70
Flushing the MAC address table	71
Flushing a VLAN MAC address table	71
Flushing a FastEthernet interface MAC address table.....	72
Flushing a MAC address table for a trunk.....	72
Flushing a single address from the MAC address table.....	73
Chapter 9: STP configuration using CLI.....	74
Using spanning tree.....	74
Displaying spanning tree configuration information.....	74
Setting path cost calculation.....	75
Configuring STG parameters	75
Configuring STG operation mode.....	76
Configuring STP for ports.....	77
Configuring STP port mode	78
Enabling or disabling STP 802.1d compliance mode.....	78
Disabling STP for ports	78
Using Advanced Spanning Tree.....	79
Displaying RSTP configuration details.....	79
Displaying RSTP bridge statistics.....	79
Displaying RSTP status information.....	80
Displaying RSTP port configuration details.....	80
Displaying RSTP port role.....	80
Displaying RSTP port statistics	81
Displaying RSTP status per port.....	81
Configuring RSTP parameters.....	82
Displaying MSTP related information.....	83
Displaying MSTP status information.....	83
Displaying MSTP related statistics.....	83
Displaying MSTP Cist port information.....	83
Displaying MSTP Cist port role	84
Displaying MSTP Cist port statistics.....	84
Displaying MSTP bridge and VLAN information	85
Displaying MSTP bridge statistics	85
Displaying MSTP port information.....	86
Displaying MSTP port role.....	86
Displaying MSTP port statistics	87

Configuring MSTP parameters for Cist bridge	87
Configuring MSTP parameters for Common Spanning Tree using CLI.....	88
Configuring MSTP region parameters.....	89
Configuring MSTP MSTI bridge parameters	90
Configuring MSTP MSTI port parameters.....	90
Deleting an MSTP bridge.....	91
Enabling or disabling an MSTP bridge.....	92
Configuring STP BPDU filtering.....	92
Configuring STP Multicast Destination MAC address.....	93
Chapter 10: Multi-Link Trunking configuration using CLI.....	95
Configuring a Multi-Link Trunk.....	95
Deleting a MultiLink Trunk.....	96
Configuring MLT whole trunk.....	96
Displaying MLT configuration.....	97
Displaying MLT members.....	97
Displaying the MLT whole trunk status.....	98
Selecting an SLPP Guard Ethernet type.....	98
Variable definitions.....	99
Configuring SLPP Guard	99
Variable definitions.....	99
Using Distributed Multi-Link Trunking.....	100
Configuring DMLT.....	100
Displaying DMLT configuration.....	100
Chapter 11: Configuring ADAC for IP Phones using CLI.....	102
Configuring global ADAC settings.....	102
Disabling or clearing ADAC settings.....	103
Resetting ADAC settings to the default	104
Configuring ADAC MAC address range.....	104
Resetting MAC address ranges using CLI.....	105
Configuring ADAC device settings per port.....	105
Setting ADAC detection method.....	106
Disabling ADAC per port.....	107
Resetting ADAC port settings to default	107
Restoring ADAC detection method to default.....	108
Displaying ADAC settings per port.....	109
Displaying ADAC MAC range.....	110
Displaying ADAC detection method status.....	110
Chapter 12: Configuring LACP and VLACP using CLI.....	112
Configuring Link Aggregation Group using CLI.....	112
Configuring LACP system priority.....	112
Configuring LACP port mode.....	113
Resetting LACP port mode to default.....	113
Enabling or removing LACP aggregation for ports.....	114

Assigning a key value to a port.....	115
Assigning LACP priority for ports.....	116
Configuring LACP timeout.....	116
Displaying LACP information.....	117
Displaying LACP aggregator information.....	117
Displaying LACP port information.....	118
Displaying LACP port debug information.....	119
Displaying LACP port statistics information.....	120
Clearing LACP port statistics.....	121
Configuring Static LACP Key to Trunk ID binding.....	121
Configuring VLACP using CLI.....	123
Enabling or disabling VLACP globally.....	123
Configuring multicast MAC address for VLACP.....	123
Configuring VLACP on a port.....	124
Resetting VLACP MAC address value	126
Disabling VLACP on a port.....	126
Displaying VLACP status.....	127
Displaying VLACP configuration for a port.....	127
Chapter 13: Configuring VLANs using Enterprise Device Manager.....	129
VLAN management using EDM.....	129
Displaying VLAN information using EDM.....	129
Modifying an existing VLAN in STG mode using EDM.....	131
Modifying an existing VLAN in RSTP mode using EDM.....	133
Modifying an existing VLAN in MSTP mode using EDM.....	134
Creating a VLAN in STG mode using EDM.....	136
Creating a VLAN in RSTP mode using EDM.....	138
Creating a VLAN in MSTP mode using EDM.....	140
Deleting a VLAN using EDM.....	142
VLAN configuration for ports using EDM.....	142
Displaying VLAN membership port information using EDM.....	142
Configuring VLAN membership ports using EDM.....	143
Selecting VLAN configuration control using EDM.....	145
Port configuration for VLANs using EDM.....	146
Displaying port VLAN membership information using EDM.....	147
Configuring ports for VLAN membership using EDM.....	148
Configuring an IPv6 interface using EDM.....	150
Interfaces tab field descriptions.....	150
MAC address table management using EDM.....	151
Flushing the MAC address table using EDM.....	152
Flushing the MAC address table for an interface using EDM.....	152
Flushing the MAC address table for a VLAN using EDM.....	153
Flushing the MAC address table for a trunk using EDM.....	153
Flushing a single MAC address table entry using EDM.....	154

Link Aggregation Control Protocol.....	155
Displaying LAG information using EDM.....	155
Link Aggregation Group configuration using EDM.....	156
Configuring Static LACP Key to Trunk ID binding using EDM.....	166
Configuring MLT and VLACP global settings using EDM.....	167
Configuring MLT whole trunk using EDM.....	168
Enabling or disabling global VLACP using EDM.....	168
VLACP configuration for ports using EDM.....	169
Displaying the VLACP configuration for ports using EDM.....	169
Configuring VLACP for specific ports using EDM.....	171
Chapter 14: Configuring Spanning Tree Groups using Enterprise Device Manager.....	174
Changing the Spanning Tree mode using EDM.....	174
Resetting the switch using EDM.....	175
Rediscovering the switch using EDM.....	175
Configuring STP BPDU Filtering using EDM.....	175
Spanning Tree Group configuration using EDM.....	176
Configuring STG globally using EDM.....	176
Displaying STG configuration general information using EDM.....	177
Displaying STG status information using EDM.....	179
Displaying STG port information using EDM.....	181
Configuring STG for a single port using EDM.....	182
Rapid Spanning Tree Protocol.....	184
Rapid Spanning Tree Protocol.....	184
Displaying RSTP general information using EDM.....	185
Displaying RSTP ports information using EDM.....	187
Displaying RSTP status using EDM.....	189
Graphing RSTP port statistics using EDM.....	190
Multiple Spanning Tree Protocol.....	191
Multiple Spanning Tree Protocol	191
Displaying MSTP general information using EDM.....	191
Displaying CIST port information using EDM.....	194
Graphing CIST Port Statistics using EDM.....	196
Displaying MSTI Bridges using EDM.....	198
Inserting MSTI Bridges using EDM.....	199
Deleting MSTI Bridges using EDM.....	199
Displaying MSTI Port information using EDM.....	200
Graphing MSTI port statistics using EDM.....	201
Setting up bridging.....	202
Viewing Bridge base information using EDM.....	202
Viewing information about specific unicast MAC address using EDM.....	202
Displaying current MAC Address Table using EDM	203
Graphing port bridge statistics using EDM.....	204
Chapter 15: Configuring Multi-Link Trunking using Enterprise Device Manager.....	206

Multi-Link Trunk features.....	206
Configuring Multi-Link Trunks using EDM.....	206
Configuring Multi-Link Trunks using EDM.....	207
Displaying MLT utilization using EDM.....	208
Graphing Multi-Link Trunk statistics using EDM.....	208
Graphing Multi-Link Trunk Ethernet error statistics using EDM.....	210
Selecting an SLPP Guard Ethernet type using EDM.....	213
Configuring SLPP Guard using EDM.....	213
Chapter 16: Configuring ADAC for IP phones using Enterprise Device Manager.....	215
Configuring ADAC globally using EDM.....	215
ADAC port information management using EDM.....	217
Displaying port ADAC for information using EDM.....	217
Configuring ADAC for specific ports using EDM.....	219
ADAC MAC address range configuration using EDM.....	221
Displaying the MAC address range table using EDM.....	221
Creating MAC address ranges using EDM.....	222
Deleting MAC address ranges using EDM.....	222

Chapter 1: Preface

Purpose

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

Training

Ongoing product training is available. For more information or to register, you can access the Web site at www.extremenetworks.com/education/.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at internalinfodev@extremenetworks.com

Getting Help

Product purchased from Extreme Networks

If you purchased your product from Extreme Networks, use the following support contact information to get help.

If you require assistance, contact Extreme Networks using one of the following methods:

- [GTAC \(Global Technical Assistance Center\) for Immediate Support](#)
 - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
 - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- [GTAC Knowledge](#) – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- [The Hub](#) – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- [Support Portal](#) – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Product purchased from Avaya

If you purchased your product from Avaya, use the following support contact information to get help.

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

Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation

www.extremenetworks.com/documentation/

Table continues...

Archived Documentation (for previous versions and legacy products)
Release Notes

www.extremenetworks.com/support/documentation-archives/

www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing.

Subscribing to service notifications

Subscribe to receive an email notification for product and software release announcements, Vulnerability Notices, and Service Notifications.

About this task

You can modify your product selections at any time.

Procedure

1. In an Internet browser, go to <http://www.extremenetworks.com/support/service-notification-form/>.
2. Type your first and last name.
3. Type the name of your company.
4. Type your email address.
5. Type your job title.
6. Select the industry in which your company operates.
7. Confirm your geographic information is correct.
8. Select the products for which you would like to receive notifications.
9. Click **Submit**.

Chapter 2: New in this document

There are no new feature changes in this release.

Chapter 3: VLAN Fundamentals

CLI command modes

Command Line Interface (CLI) provides the following command modes:

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

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

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

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

Table 1: CLI command modes

Command mode and sample prompt	Entrance commands	Exit commands
User Executive Switch>	No entrance command, default mode	exit or logout
Privileged Executive Switch#	enable	exit or logout
Global Configuration Switch (config)#	From Privileged Executive mode, enter configure terminal	To return to Privileged Executive mode, enter end or

Table continues...

Command mode and sample prompt	Entrance commands	Exit commands
		exit To exit CLI completely, enter logout
Interface Configuration Switch (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 configure a loopback, enter interface loopback <loopback number>	To return to Global Configuration mode, enter exit To return to Privileged Executive mode, enter end To exit CLI completely, enter logout
Application Configuration Switch (config-app)#	From Global, or Interface Configuration mode, enter application	To return to Global Configuration mode, enter exit To return to Privileged Executive mode, enter end To exit CLI completely, enter logout

Virtual local area networks

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

In simple terms, a virtual local area network (VLAN) provides a mechanism to fine-tune broadcast domains. You can create port-based and IPv6 protocol-based virtual local area networks (VLANs):

- IEEE 802.1Q port-based VLANs

A port-based VLAN is a VLAN in which the switch ports are explicitly configured to be in the VLAN. When you create a port-based VLAN, you assign a Port VLAN Identifier (PVID) and

specify which ports belong to the VLAN. The PVID is used to coordinate VLANs across multiple switches.

- IPv6 protocol-based VLANs

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

- VLAN Configuration Control

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

For more information, see [VLAN Configuration Control](#) on page 22.

VLAN support

The switch supports 256 VLANs, either by-port, under the 802.1d bridging model, or IPv6 protocol-based VLANs.

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

When the switch is installed for the first time, all ports are assigned to the default VLAN (PVID = 1). The default management VLAN is VLAN 1.

You can configure VLANs through the CLI or EDM interfaces. The switch supports binary and ASCII configuration files. You can also configure VLANs using both SNMP and ASCII scripts.

IEEE 802.1Q tagging

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

The switch supports the Independent VLAN Learning (IVL) model. IVL allows duplicate MAC address to be present in different sets, but not in the same set or VLAN.

IEEE 802.1Q VLAN workgroups

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

Frames received in one VLAN can only be forwarded within that VLAN, and multicast frames and unknown unicast frames are flooded only to ports in the same VLAN. When you set up VLANs, you segment networks to increase network capacity and performance without changing the physical

network topology. With network segmentation, each switch port connects to a segment that is a single broadcast domain.

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

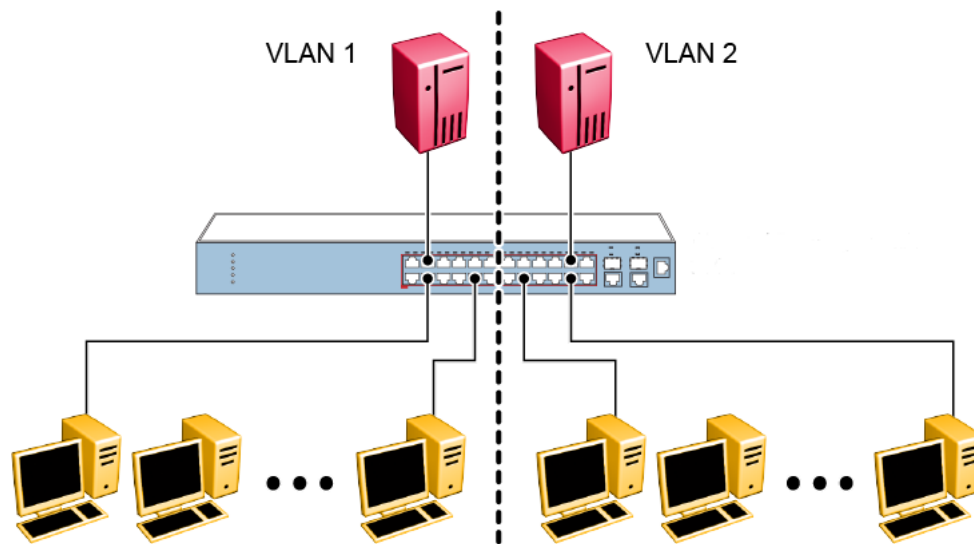


Figure 1: Port-based VLAN example

IEEE 802.1Q tagging

The switch operates in accordance with the IEEE 802.1Q tagging rules. Important terms used with the 802.1Q tagging feature are:

- VLAN identifier (VID)—the 12-bit portion of the VLAN tag in the frame header that identifies an explicit VLAN.
- Port VLAN identifier (PVID)—a classification mechanism that associates a port with a specific VLAN. For example, a port with a PVID of 3 (PVID =3) assigns all untagged frames received on this port to VLAN 3.
- Tagged frame—the 32-bit field (VLAN tag) in the frame header that identifies the frame as belonging to a specific VLAN. Untagged frames are marked (tagged) with this classification as they leave the switch through a port that is configured as a tagged port.
- Untagged frame—a frame that does not carry any VLAN tagging information in the frame header.
- VLAN port members—a set of ports that form a broadcast domain for a specific VLAN. A port can be a member of one or more VLANs.

- Untagged member—a port that is configured as an untagged member of a specific VLAN. When an untagged frame exits the switch through an untagged member port, the frame header remains unchanged. When a tagged frame exits the switch through an untagged member port, the tag is stripped and the tagged frame is changed to an untagged frame.
- Tagged member—a port that is configured as a member of a specific VLAN. When an untagged frame exits the switch through a tagged member port, the frame header is modified to include the 32-bit tag associated with the PVID. When a tagged frame exits the switch through a tagged member port, the frame header remains unchanged (original VID remains).
- User priority—a three-bit field in the header of a tagged frame. The field is interpreted as a binary number, and therefore has a value of 0 to 7. This field allows the tagged frame to carry the user priority across bridged LANs in which the individual LAN segments are sometimes unable to signal priority information.
- Port priority—the priority level assigned to untagged frames received on a port. This value becomes the user priority for the frame. Tagged packets get their user priority from the value contained in the 802.1Q frame header.
- Unregistered packet—a tagged frame that contains a VID where the receiving port is not a member of that VLAN.

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

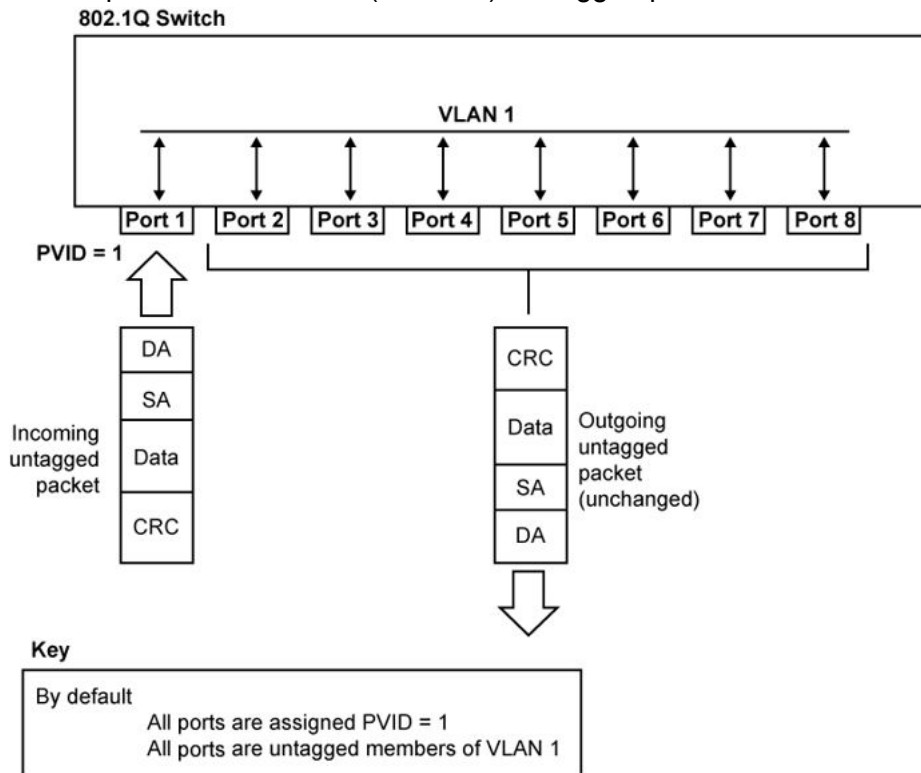


Figure 2: Default VLAN settings

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

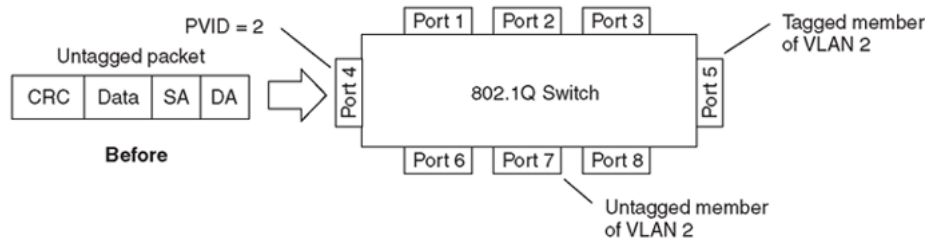


Figure 3: Port-based VLAN assignment

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

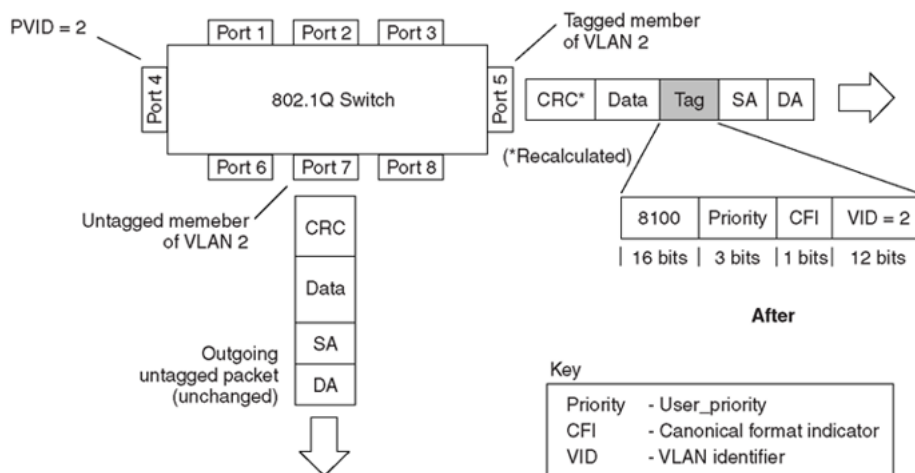


Figure 4: 802.1Q tag assignment (after port-based VLAN assignment)

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

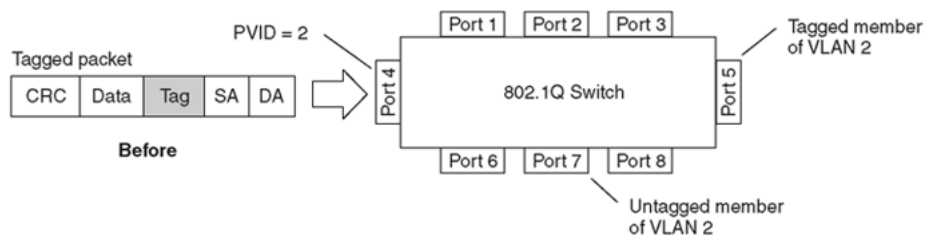


Figure 5: 802.1Q tag assignment

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

(untagged) as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.

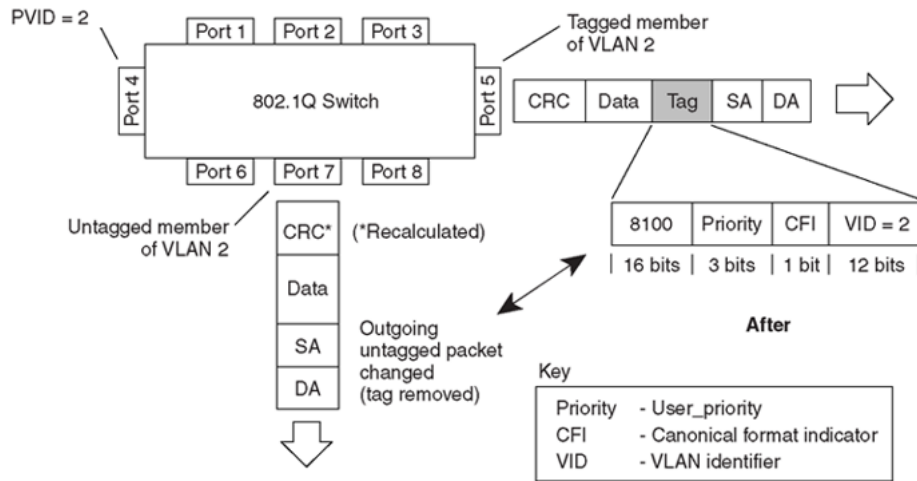


Figure 6: 802.1Q tagging (after 802.1Q tag assignment)

VLAN Tagging Enhancement

Rather than setting a port to untagged or tagged mode, you can also choose to enable or disable PVID tagging.

Following table summarizes the tagging options:

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

VLAN Configuration Control

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

VLAN Configuration Control offers four options for controlling VLAN modification:

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

adding it to the new VLAN. The PVID of the port will be changed to the new VID to which it was added.

! **Important:**

Strict is the factory default setting.

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

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

VLAN Configuration Control does not apply to protocol-based VLANs. A port regardless of its tagging mode can belong to one or more protocol-based VLANs, but in the same time it cannot belong to two or more protocol-based VLANs containing the same PID. The user is responsible to remove a port from any previous protocol-based VLAN membership. A protocol-based VLAN cannot be set as PVID for a port.

VLANs spanning multiple switches

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

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

VLANs spanning multiple 802.1Q tagged switches

The following figure shows VLANs spanning two switch devices (S1 and S2). The 802.1Q tagging is enabled on S1, port 2 and on S2, port 1 for VLAN 1 and VLAN 2. Both ports are tagged members of VLAN 1 and VLAN 2.

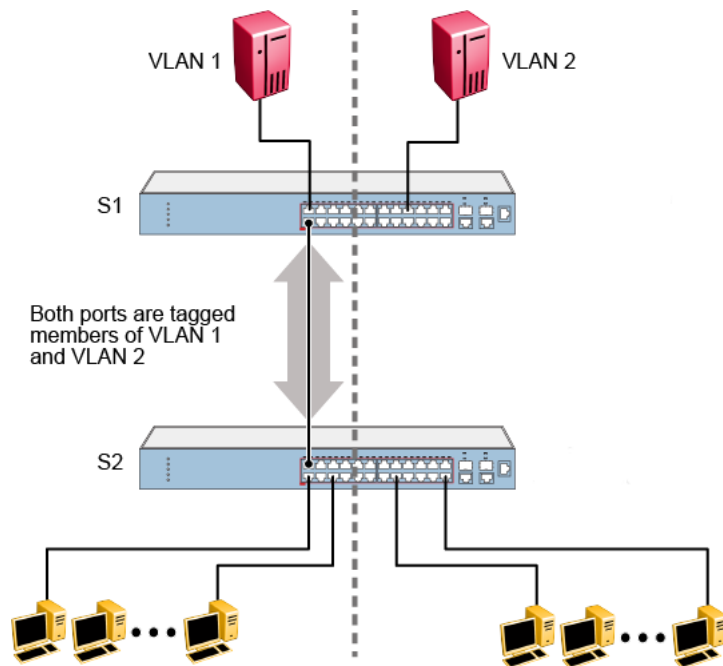


Figure 7: VLANs spanning multiple 802.1Q tagged switches

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

VLANs spanning multiple untagged switches

The figure below shows VLANs spanning multiple untagged switches. In this configuration, S2 does not support 802.1Q tagging and you must use a single switch port on each switch for each VLAN. For this configuration to work properly, you must set Spanning Tree participation to Disabled (the STP is not supported across multiple LANs).

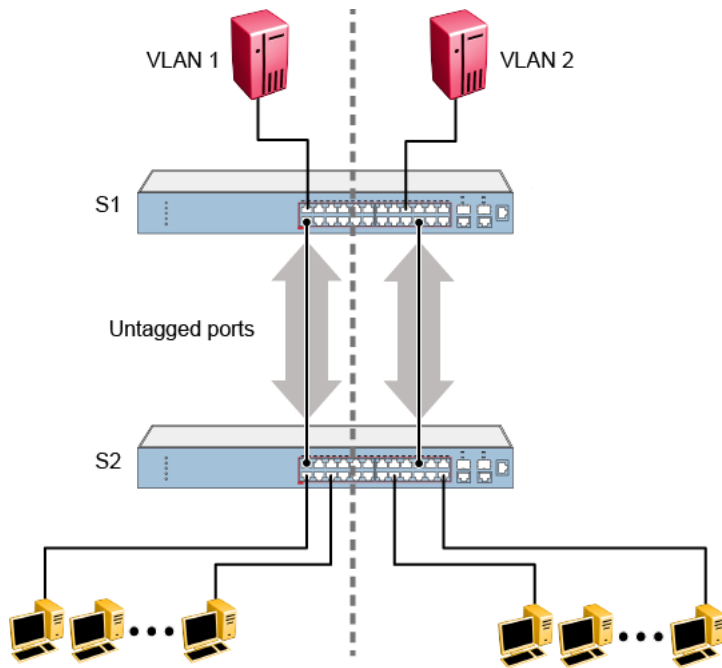


Figure 8: VLANs spanning multiple untagged switches

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

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

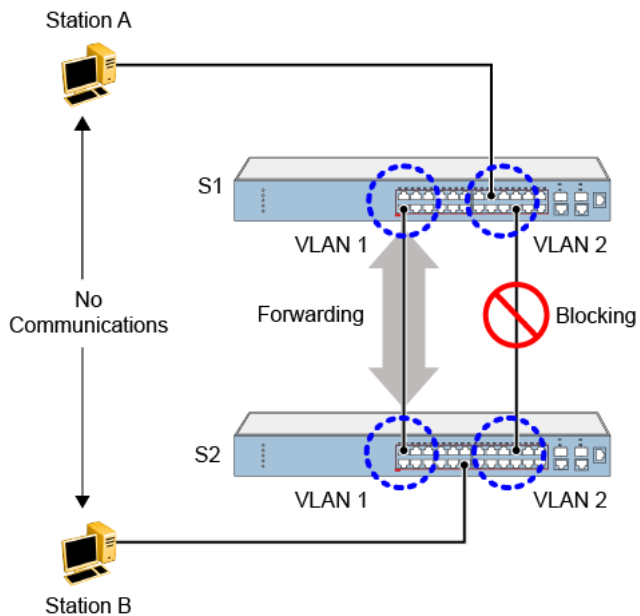


Figure 9: Possible problems with VLANs and Spanning Tree Protocol

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

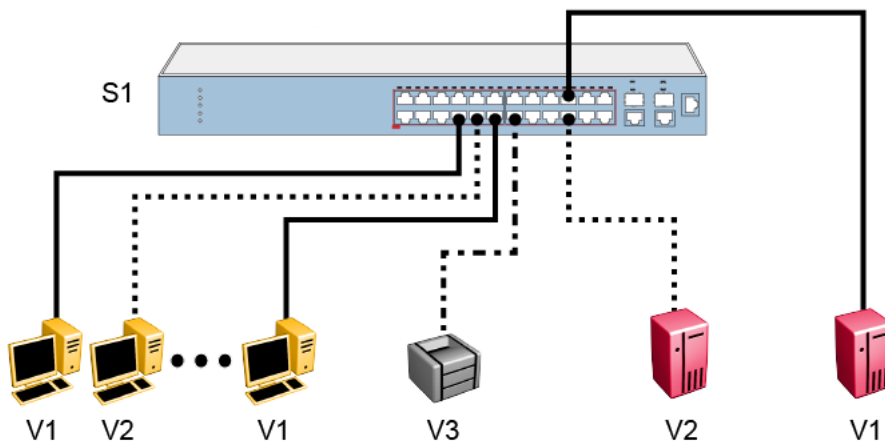
Communications failure occurs between VLAN 2 of S1 and VLAN 2 of S2, blocking communications between Stations A and B.

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

Shared servers

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

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



Key

—	VLAN 1 (PVID=1)
.....	VLAN 2 (PVID=2)
- - - - -	VLAN 3 (PVID=3)

Figure 10: Multiple VLANs sharing resources

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

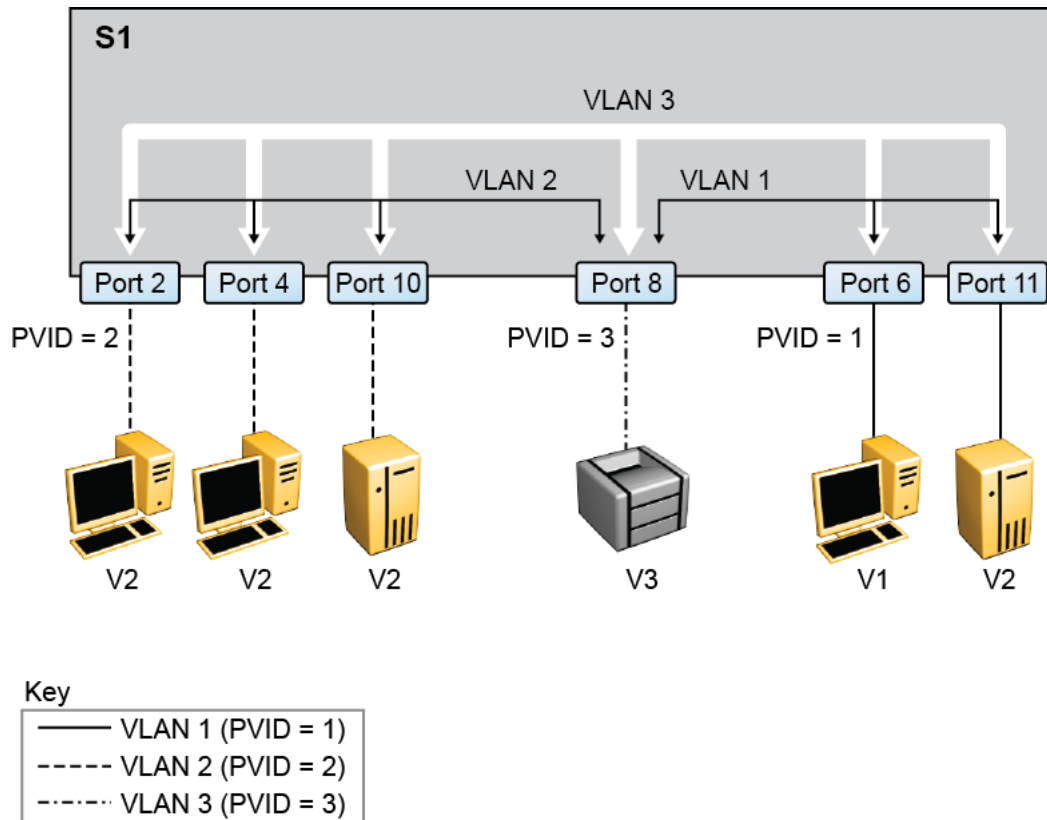


Figure 11: VLAN broadcast domains within the switch

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

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

VLAN workgroup summary

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

As shown in the figure below, S1 is configured with multiple VLANs:

- Ports 1, 6, 11, and 12 are in VLAN 1.

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

Because S4 does not support 802.1Q tagging, a single switch port on each switch must be used for each VLAN (see [VLANs spanning multiple untagged switches](#) on page 24).

The connection to S2 requires only one link between the switches because S1 and S2 are both switches that support 802.1Q tagging (see [VLANs spanning multiple 802.1Q tagged switches](#) on page 24).

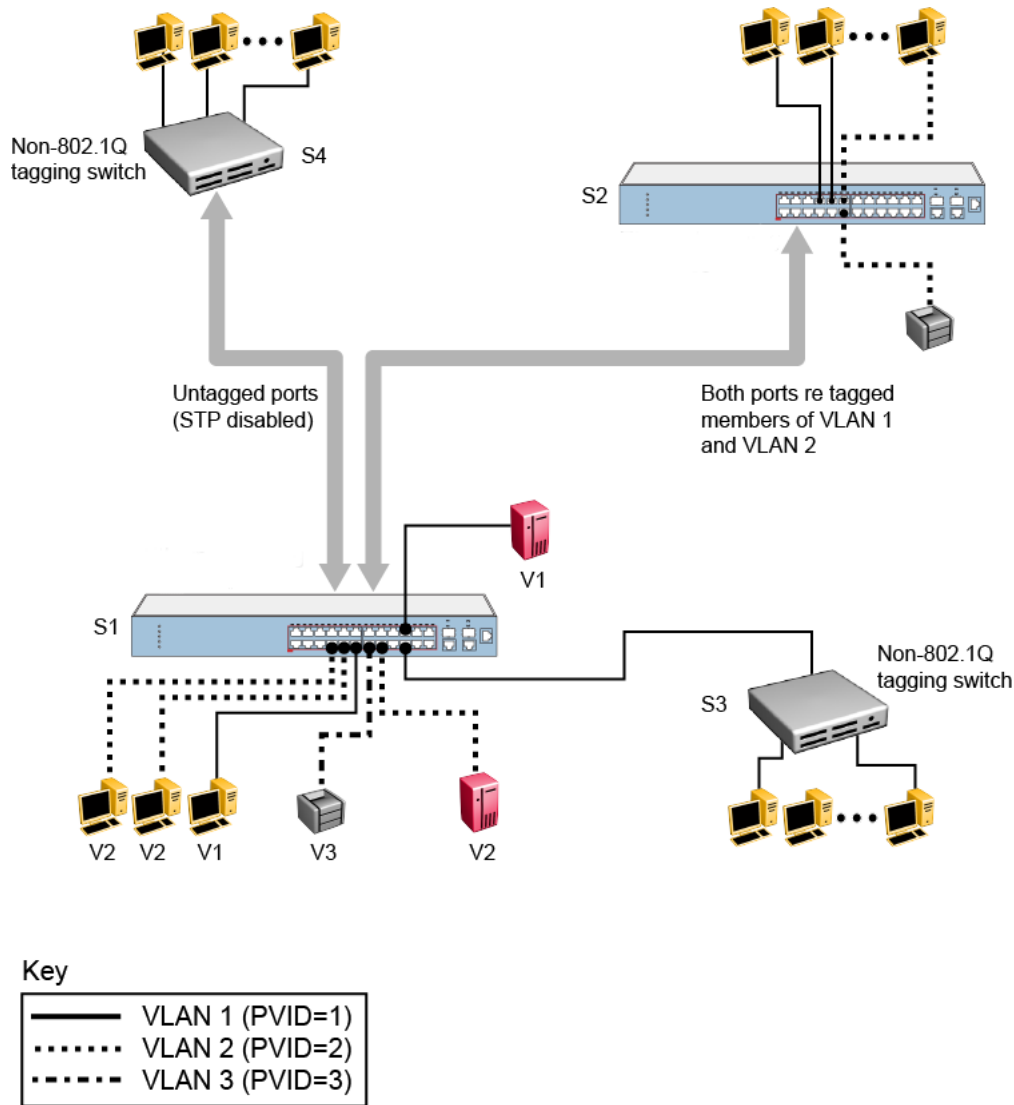


Figure 12: VLAN configuration spanning multiple switches

VLAN configuration rules

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

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

MAC Flush

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

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

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

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

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

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

- AGELOCK
- SECRET
- STATIC

Higher priority tasks can delay MAC Address clearing.

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 LLDP 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:

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

You can configure up to 6 Voice VLANs.

Storm Control

This feature provides granular control of Broadcast, Multicast and Unicast traffic rates on a per-port basis. Broadcast, Multicast and Unicast traffic rates can be individually or collectively controlled on a switch or switch stack by setting the following: low-watermark and high watermark values in packets per second (pps), polling interval value, action type, and SNMP traps. When a high watermark is exceeded, an action of None, Drop or Shutdown can be applied to the traffic type.

A defined action is reversed, or ceases, when the traffic rate in pps falls below the low-watermark setting. When an action of 'drop' is used, traffic is dropped when traffic exceeds the high-watermark and will not resume forwarding until the traffic rate falls below the low-watermark. When the action of 'shutdown' is used, the switch port is administratively shutdown when traffic exceeds the high-

watermark and requires administrator intervention to re-enable the switch port to resume traffic forwarding.

The Storm Control feature includes logging of watermark crossings and sending of traps for the low and high watermark crossings. Traps for high watermark exceeded may be sent repeatedly at a user specified interval.

Storm Control feature uses the rising and falling threshold levels to block and restore the forwarding of Broadcast, Multicast or Unicast packets.

Storm Control feature is disabled by default.

MLT/DMLT/LAG Dynamic VLAN changes

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

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

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

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

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

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

Chapter 4: Spanning Tree Protocol Fundamentals

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

Spanning Tree Protocol

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

Port states

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

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

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

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

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

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

- Blocking
- Listening
- Learning
- Forwarding

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

STP port mode

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

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

STP 802.1d compliance mode

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

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

Aging of dynamic entries in Forwarding Database

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

If the network topology did not change, the aging timeout value is specified by the `dot1dTpAgingTime` MIB variable. This can be configured through the user interface console. The

range of applicable values specified in the IEEE standard is 10 to 1000000 seconds, whereas Extreme Networks recommends a default value 300 seconds.

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

Port path cost

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

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

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

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

802.1t path cost calculation

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

Rapid Spanning Tree Protocol

The Spanning Tree implementation is based on IEEE 802.1d, which is slow to respond to a topology change in the network (such as a dysfunctional link in a network). The Rapid Spanning Tree Protocol (RSTP or IEEE 802.1w) reduces the recovery time after a network breakdown. In certain configurations the RSPT recovery time is less than 1 second. It also maintains a backward compatibility with the IEEE 802.1d, which was the Spanning Tree implementation prior to RSTP. The

backward compatibility can be maintained by configuring a port to be in STP compatible mode. A port operating in the STP compatible mode transmits and receives only STP BPDUs and drops any RSTP BPDUs.

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

Multiple Spanning Tree Protocol

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

The switch uses RSTP and MSTP to achieve the following:

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

Interoperability with legacy STP

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

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

Differences in port roles

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

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

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

Edge port

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

Path cost values

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

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

Table continues...

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

Rapid convergent

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

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

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

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

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

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

Switch A is the Root.

Negotiation process

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

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

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

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

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

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

PC 3 cannot communicate with either PC 1 or PC 2 until the negotiation process between switch B and switch C is complete.

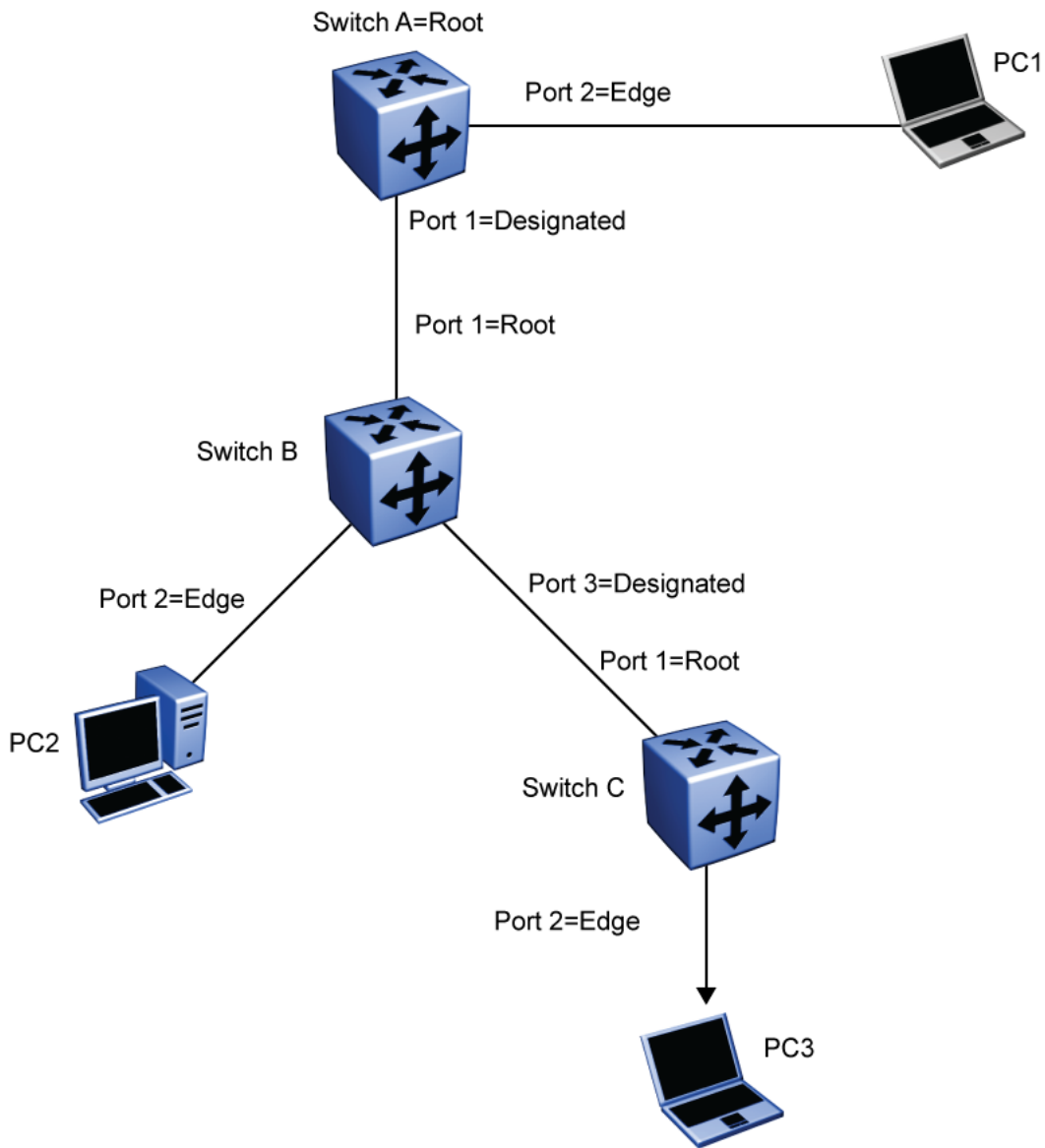


Figure 13: Negotiation process

Spanning Tree BPDU Filtering

The Spanning Tree Protocol detects and eliminates logical loops in a bridged or switched network. Any bridge that participates in the spanning tree exchanges information with other bridges using configuration messages known as Bridge Protocol Data Units (BPDU). Based on the BPDU

information exchange, the bridge with the lowest bridge ID becomes the root. This process is called the root selection process.

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

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

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

*** Note:**

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

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

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

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

Static STP Multicast Destination Configuration

Static STP Multicast Destination Configuration feature provides low cost resilient access with automatic failover to CPE or small sites located at the edge of a SPB MAN fabric. With this feature, you can create a configurable parameter to modify the STP Default Spanning Tree Group (802.1d STP) destination multicast MAC address to any custom MAC address. The switch can leverage SPB to STP interoperability workaround with this feature.

STP loops or rings are created external to a SPB MAN, with the rings terminating on two separate SPB BEB switches. The nonstandard STP multicast MAC lets the BPDUs to pass through an SPB ISID from one SPB BEB switch to another, which terminate at the opposite ends of the network loop or ring. This provides an automatic re-convergence in case of link failure.

This feature supports changing the STP MAC only in conjunction with configuration of multiple Spanning Tree Groups.

 **Note:**

The new configured MAC address must begin with 01.

Chapter 5: Multi-Link Trunking Fundamentals

About Multi-Link Trunking

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

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

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

Trunking can be described in the following terms:

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

The two basic switching requirements of MLTs are:

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

MLT operation

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

MLT configuration examples

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

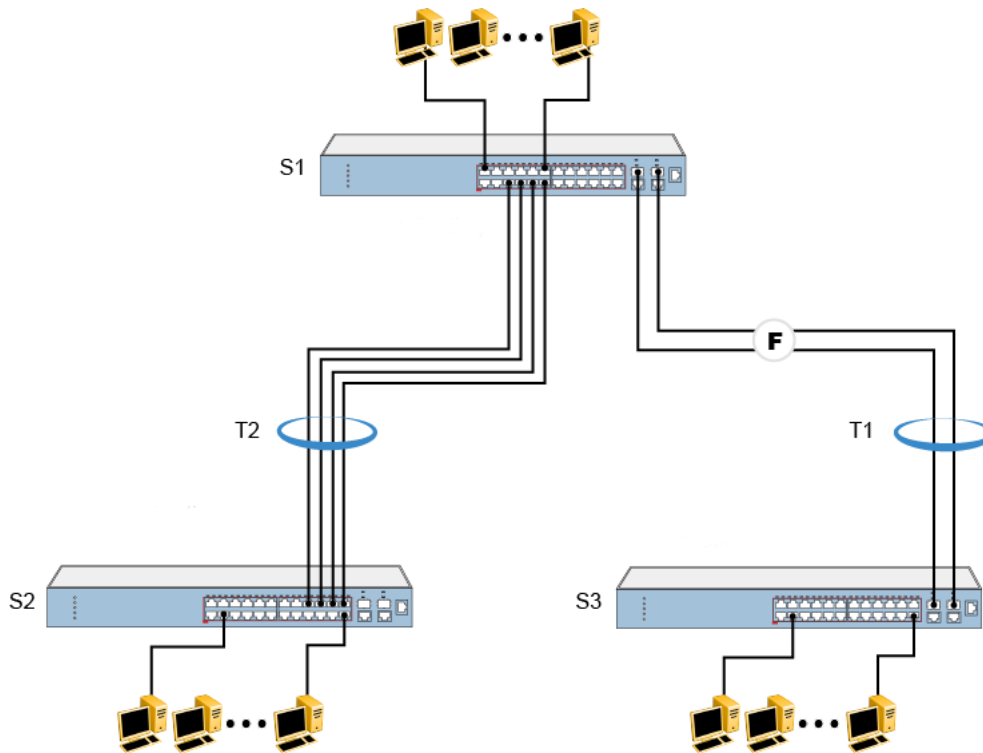


Figure 14: Switch-to-switch trunk configuration example

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

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

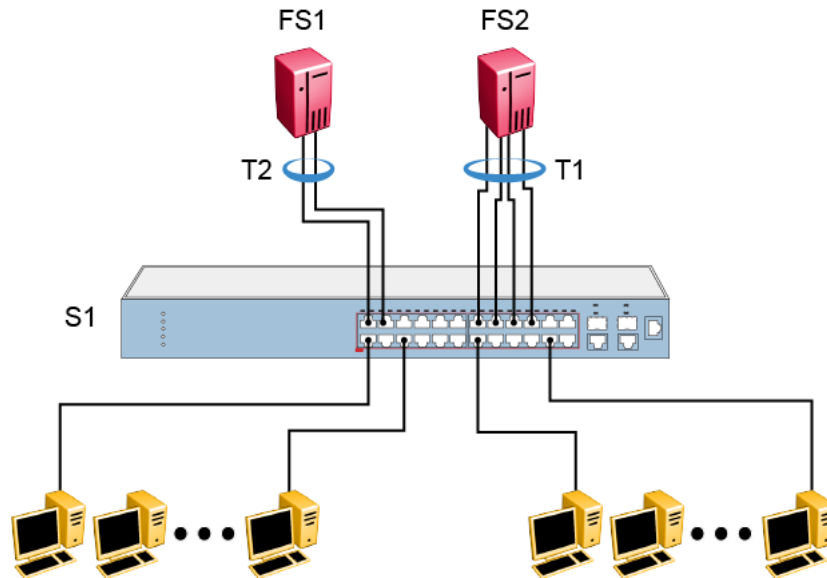


Figure 15: Switch-to-server trunk configuration example

Client server configuration using Multi-Link Trunks

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

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

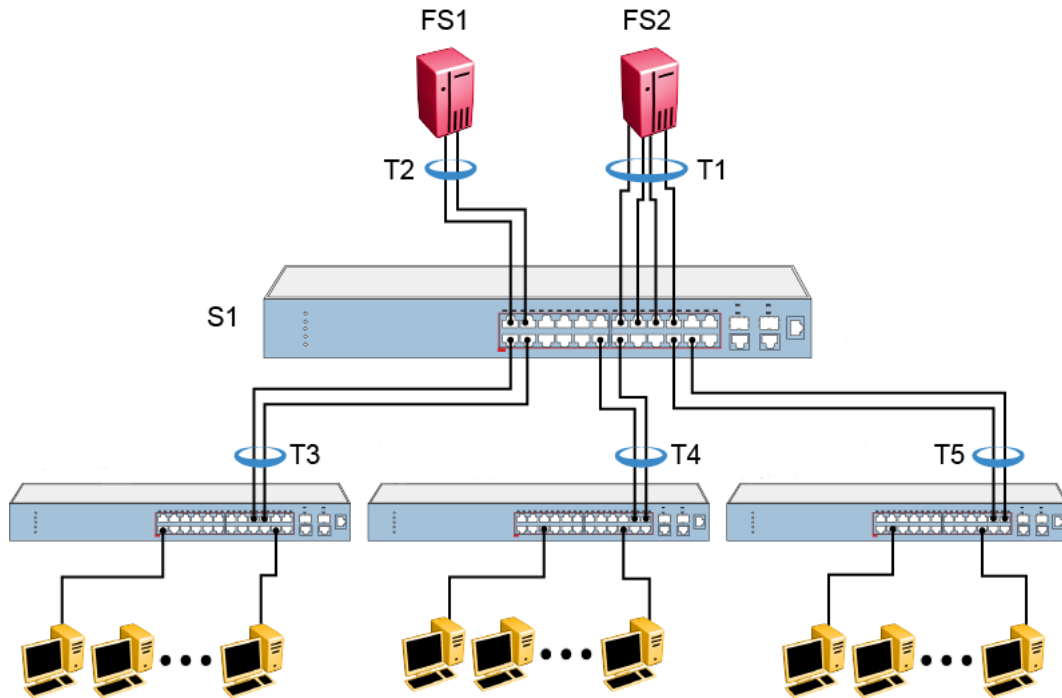


Figure 16: Client/server configuration example

For detailed information about configuring trunks, see [Configuring a MultiLink Trunk using CLI](#) on page 95 and [Configuring Multi-Link Trunking using Enterprise Device Manager](#) on page 206.

Before you configure trunks

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

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

1. Read the configuration rules provided in the next section, [Spanning tree considerations for Multi-Link Trunks](#) on page 45.
2. Determine which switch ports (up to four) are to become trunk members (the specific ports making up the trunk). A minimum of two ports are required for each trunk.

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

Trunk member ports must have the same VLAN and VLACP configuration. LACP should not be enabled on the selected trunk ports.

3. All network cabling should be complete and stable before configuring any trunks, to avoid configuration errors.
4. Consider how the existing spanning tree reacts to the new trunk configuration (see [Spanning tree considerations for Multi-Link Trunks](#) on page 45).

5. Consider how existing VLANs are affected by the addition of a trunk.

Spanning tree considerations for Multi-Link Trunks

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

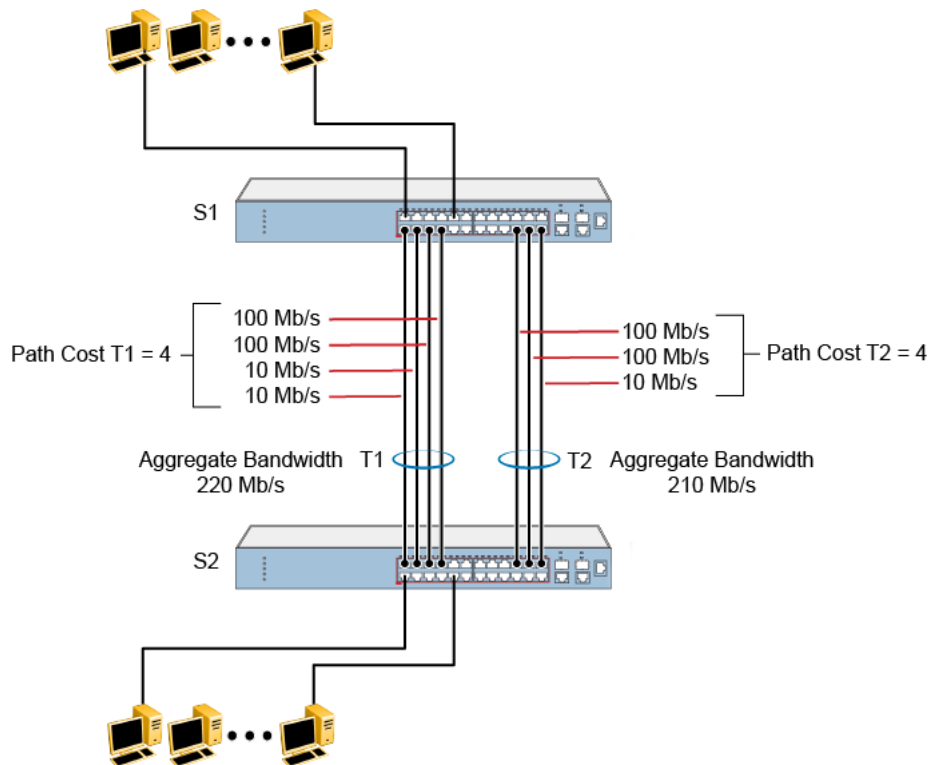


Figure 17: Path Cost arbitration example

Additional tips about the Multi-Link Trunking feature

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

The trunk is viewed by management stations as a single spanning tree port. The spanning tree port is represented by the trunk member with the lowest port number. For example, if ports 13, 14, 15,

and 16 are trunk members of trunk T1, the management station views trunk T1 as spanning tree port 13.

! Important:

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

MLT enable or disable whole trunk

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

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

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

! Important:

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

Distributed Multi-Link Trunk

Distributed Multi-Link Trunking (DMLT) supports up to six link aggregation trunk groups with a maximum of four members per group using either a basic or advanced load balancing algorithm. Link members can be ports from a local unit or from any other unit in a switch stack. For DMLT procedures, see [Using Distributed MultiLink Trunking using CLI](#) on page 100.

Distributed LAG (802.3ad) LACP

Distributed Link Aggregation Group (D-LAG) supports up to six link aggregation trunk groups with a maximum of four active members per group using the Link Aggregation Control Protocol (LACP) over point-to-point links in each group. Link members can be ports from a local unit or from any other unit in a switch stack.

For Distributed LAG procedures, see [Configuring Link Aggregation Group using CLI](#) on page 112.

SLPP Guard

Because SMLT networks, by design, disable STP, RSTP, or MSTP for participating ports, you need a method to prevent loops that involve these ports.

When you use a switch that does not support Simple Loop Protection Protocol (SLPP) in combination with other switches that support SLPP and Switch Clustering (SMLT)—for example, ERS 5000 Series or ERS 8300—the SLPP Guard feature provides additional network loop protection.

A switch that does not support SLPP, does not generate SLPP packets on ports that have SLPP Guard enabled. But when you enable SLPP Guard on switch ports, the switch 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. After the predetermined interval expires, SLPP Guard reenables the port. As an option, you can configure SLPP Guard to administratively disable the port indefinitely.

Example

In the following example, switch A and B are SMLT switches. Switch C is the Edge Switch. Assume all the ports are in VLAN 20 and SLPP Guard are enabled. Switch A sends SLPP PDU packets to ports 1, 5, and 10.

Because SLPP Guard is enabled on port 5 of switch C, when a SLPP PDU packet is received from port 5 of switch A, port 5 of switch C is shut down. Switch C can correctly detect the SLPP packets only when the SLPP Guard EtherType that is configured on switch C is the same as the SLPP PDU EtherType configured on the SMLT core (A and B switches).

* Note:

When SLPP Guard is active on the Edge Switch, the misconfigured link is disabled by the Edge Switch. You cannot enable SLPP Guard on ports that are members of MLTs, DMLTs, LACPs, or LAGs.

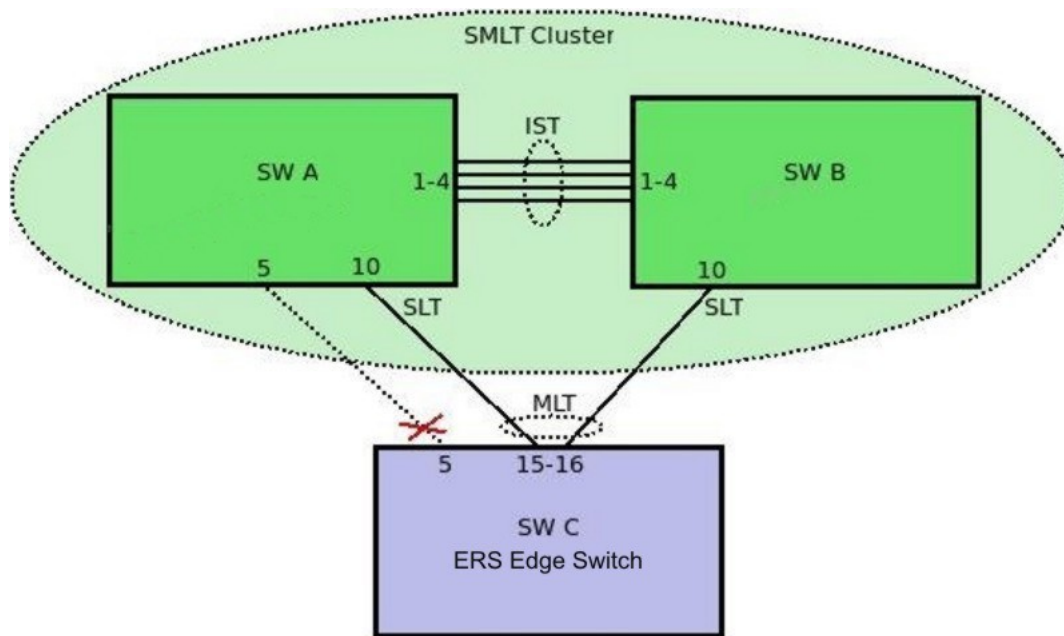


Figure 18: SLPP guard enabled on misconfigured link

For information about configuring SLPP Guard using CLI, see [Configuring SLPP Guard](#) on page 99. For information about configuring SLPP Guard using EDM, see [Configuring SLPP Guard using EDM](#) on page 213.

Chapter 6: LACP And VLACP Fundamentals

IEEE 802.3ad Link Aggregation

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

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

- Dynamic LAG
- MLT

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

The switch supports both Link Aggregation groups and Multilink trunks. By default, Link Aggregation is set to disabled on all ports. A Link Aggregation group or trunk group can be created or deleted automatically using LACP.

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

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

The failover process is as follows:

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

! Important:

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

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

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

802.3 Link Aggregation is available through the CLI. The CLI supports the following commands:

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

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

To specify the LACP mode:

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

To assign an administrative key value to a port:

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

To specify the port priority:

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

To set port time-out:

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

To set LACP system priority:

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

CLI Show commands for LACP:

- `show lacp aggr`
- `show lacp port [<portlist>]`
- `show lacp port aggr <1-65535>`
- `show lacp debug member [portlist]`

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

For more information about the syntax and parameters of the CLI commands, see [Configuring Link Aggregation Group using CLI](#) on page 112.

Static LACP key to trunk ID binding

Static LACP key to trunk ID binding provides you with more control over the association between LACP ports and trunk groups than dynamic binding. For backwards compatibility, both static LACP key to trunk ID binding and dynamic binding are available. However, when the static method is set, it overrides the dynamic method.

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

Note:

Extreme Networks recommends you to use the Static LACP key to trunk ID binding because it can prevent undesired configurations. For example, if you configure two LACP trunks, the MLT IDs are assigned to each trunk in the order of their creation. If the device is rebooted, the LACP and VLACP fundamentals order that each LAG receives a trunk might invert and the LACP aggregator might receive a different trunk than what was intended. The Static LACP key to trunk ID binding feature association between LAGs and MLT IDs can prevent this problem.

Static LACP key to trunk ID binding is enabled by default. When configured, the Static LACP key - MLT ID binding overrides the dynamic association. If no binding settings are configured, the dynamic association applies.

Important:

With Static LACP key to trunk ID binding, you must keep track of the used trunk IDs. Binding multiple keys to different trunks may easily lead to the use of all available MLT IDs. If all MLT IDs are used, you cannot configure a new LACP trunk, even if all the other required conditions for trunk formation are accomplished.

VLACP

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

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

Virtual LACP overview

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

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

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

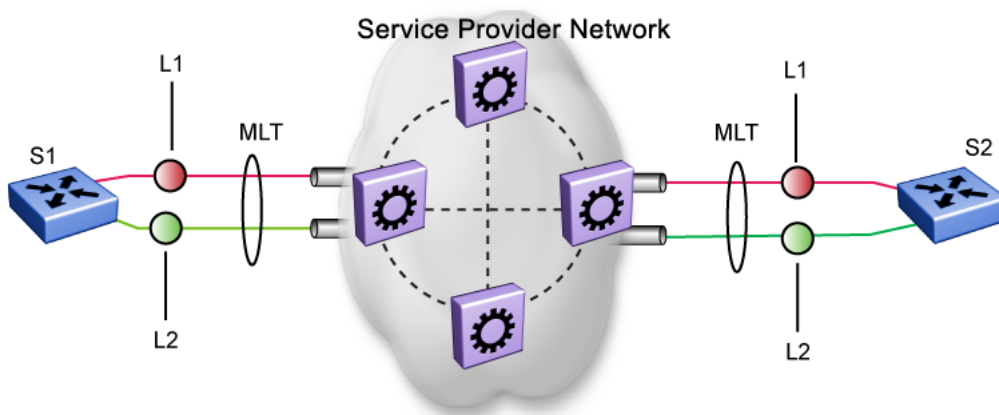


Figure 19: MLT extended through the service provider network

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

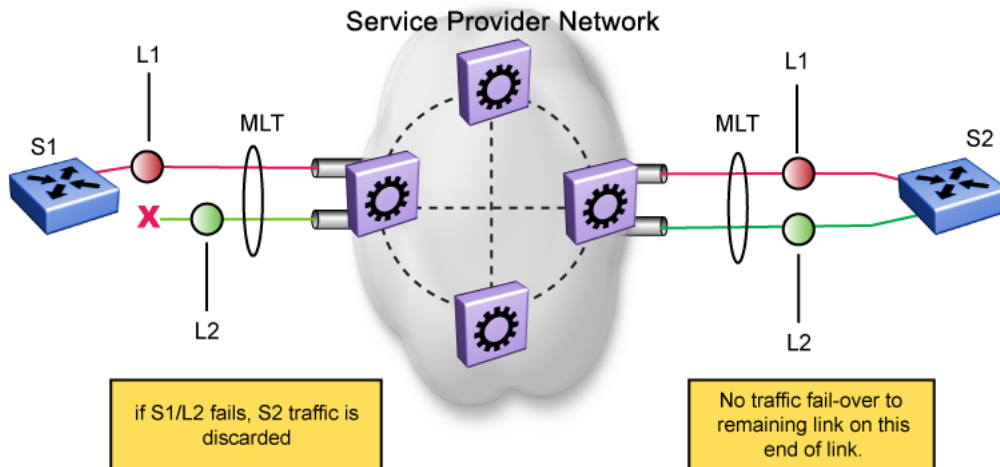


Figure 20: Link-down failure

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

Virtual LACP (VLACP) is an extension of LACP, which can provide an end-to-end failure detection mechanism. With VLACP, far-end failures can be detected allowing an MLT to fail over properly when end-to-end connectivity is not guaranteed for certain links in an aggregation group.

VLACP features

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

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

Troubleshooting

Error logs are created for the following failures and errors:

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

Chapter 7: ADAC Fundamentals

Auto-Detection and Auto-Configuration (ADAC) is supported on IP phones. With ADAC, you can automatically configure the switch to support and prioritize IP Phone traffic.

When ADAC is enabled and a 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 IP phone and the switch.

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

 **Note:**

Because the switches have limited QoS resources, the ADAC implementation differs from the other Ethernet Routing Switch platforms. It is necessary to free up some QoS resources in order for ADAC to apply the configuration on ports. For more information, see *Configuring Quality of Service on Ethernet Routing Switch 3500 Series*.

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

- **Untagged-Frames-Basic:**

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

- **Untagged-Frames-Advanced:**

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

- **Tagged Frames:**

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

ADAC operation

The following sections provide detailed explanations of ADAC operation.

Auto-Detection of IP phones

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

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

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

The detection mechanism can be selected either before enabling auto-detection on the port, or if ADAC is globally disabled

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

Auto-detection by MAC address is based on using predefined MAC addresses to determine that the specified port is connected to a IP phone. For more information and the list of defined MAC address ranges, see [Auto-Detection by MAC address](#) on page 56.

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 58.

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

Auto-Detection by MAC address

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

Following table shows a list of the default MAC address ranges.

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

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

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

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

The maximum number of ranges that ADAC supports is 128.

Auto-Detection by LLDP (IEEE 802.1AB)

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

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

ADAC and 802.1AB interoperability

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

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

Auto-Configuration of IP phones

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

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

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

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

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

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

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

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

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

Chapter 8: VLAN configuration

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

Displaying VLANs by type

Use this procedure to display all port-based or protocol-based VLANs.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show vlan [type {port | protocol | voice-vlan}]
```

 **Note:**

Enter `show vlan` to display all VLANs.

Variable definitions

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

Variable	Value
type	Enter the type of VLAN. Values include: <ul style="list-style-type: none">• port — show all port-based VLANs• protocol — show all protocol-based VLANs• voice-vlan — show all voice VLANs

Displaying VLAN settings per port

Use this 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

1. Enter Privileged EXEC mode:

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

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

Variable definitions

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

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

Displaying verbose VLAN interface information

Procedure

1. Enter Privileged EXEC mode:

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

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

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

Example

```
Switch #show vlan interface verbose
      Filter Filter
      Untag. Unreg.
Port  Frames  Frames  PVID  VLAN  VLAN Name          PRI  Tagging    Port Name
-----
1      No       Yes     1     1     VLAN #1            0    UntagAll   Port 1
-----
2      No       Yes     2     2     VLAN #2            0    UntagAll   Port 2
-----
```

Displaying port membership

Procedure

1. Enter Privileged EXEC mode:
`enable`
2. At the command prompt, enter the following command:
`show vlan interface vids [<portlist>]`

Variable definitions

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

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

Setting or resetting a management VLAN

Procedure

1. Enter Global Configuration mode:
`enable`
`configure terminal`
2. At the command prompt, enter the following command:
`[default] vlan mgmt <1-4094>`

Variable definitions

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

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

Deleting a management VLAN IP address

Important:

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

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

```
default ip address
```

Displaying VLAN ID

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show vlan id <1-4094>
```

Variable definitions

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

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

Creating a VLAN

Use this procedure to create port-based or IPv6 protocol-based VLANs.

Important:

This procedure fails if the VLAN already exists.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
vlan create {<2-4094> | <vid_list>} [name <WORD>] [ type { port |
protocol-ipv6Ether2 | voice-vlan}] | [voice-vlan] [msti <1-7> |
cist]
```

Example

```
vlan create 2-10,80 type port
vlan create 15 type voice-vlan
```

Variable definitions

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

Variable	Value
<1-4094> <vid_list>	Enter the ID of the VLAN you want to create or enter as a list or range of VLAN IDs to create multiple VLANs simultaneously. A VLAN ID can range from 1 to 4094..
name <WORD>	Enter the new name you want for the VLAN.
type	Enter the type of VLAN. Values include: <ul style="list-style-type: none"> • port — port-based VLAN • protocol-ipv6Ether2 — IPv6 protocol-based VLAN • voice-vlan — voice VLAN
msti <1-7> cist	This parameter is available only in MSTP mode. It associates the VLAN with either an MSTI instance or the CIST.

Deleting a VLAN

Use this procedure to delete a VLAN.

Procedure

1. Enter Global Configuration mode:

```
enable
```



```
configure terminal
```

- At the command prompt, enter one of the following commands:

- `vlan delete <vid_list>`

OR

- `no vlan <vid_list>`

Variable definitions

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

Variable	Value
<code><vid_list></code>	Enter the ID of the VLAN or enter as a list or range of VLAN IDs to delete.

Configuring VLAN name

Use this procedure to configure or change the name of a VLAN.

Procedure

- Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- At the command prompt, enter the following command:

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

Variable definitions

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

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

Disabling a voice VLAN

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

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

Displaying VLAN Configuration Control settings

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show vlan configcontrol
```

Modifying VLAN Configuration Control settings

This procedure applies the selected option to all VLANs on the switch.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
vlan configcontrol {[automatic] | [autopvid] | [flexible] |
[strict]}
```

Variable definitions

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

Variable	Value
automatic	Specifies AutoPVID and automatic change to membership of port-based VLANs
autopvid	Specifies automatic change to PVID
flexible	Specifies no restricts or automatic changes
strict	Specifies AutoPVID and restrictions imposed on adding port to VLAN and changing tagging

Enabling or disabling automatic PVID

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

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Variable definitions

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

Variable	Value
[no]	Disables automatic PVID.

Displaying automatic PVID status

Procedure

1. Log on to CLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
show auto-pvid
```

Configuring VLAN settings per port

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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


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

Variable definitions

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

Variable	Value
<portlist>	Enter the port numbers you want to configure for a VLAN.
tagging {enable disable tagAll untagAll tagPvidOnly untagPvidOnly}	Specifies the mode for PVID and non-PVID tagging.
pvid <1-4094>	Associates the port with a specific VLAN.
filter-untagged-frame {enable disable}	Enables or disables the port to filter received untagged packets.
filter-unregistered-frames {enable disable}	Enables or disables the port to filter received unregistered packets.
priority <0-7>	Sets the port as a priority for the switch to consider as it forwards received packets.
name <WORD>	Enter the name you want for this port.

Table continues...

Variable	Value
	 Important: This option is available only if a single port is specified in the <portlist>

Configuring VLAN members

Use this procedure to add a port or delete a port from a specific VLAN.

Procedure

1. Enter Global Configuration mode:


```
enable
configure terminal
```

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

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

Variable definitions

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

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

MAC address table configuration

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

! Important:

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

Displaying the MAC address forwarding table

You can filter the MAC Address table by port number. The MAC address table can store up to 16000 addresses.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

Variable definitions

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

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

Configuring aging time for unseen MAC addresses

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

```
[default] mac-address-table aging-time <10-1000000>
```

Variable definitions

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

Variable	Value
<10- 1000000>	Specifies the aging time in seconds that you want for MAC addresses before they expire.
default	Sets the aging time for MAC addresses to the default value, 300 seconds.

Flushing the MAC address table

Use this procedure to clear all addresses in the MAC address table.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

Variable definitions

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

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

Flushing a VLAN MAC address table

Use this procedure to clear the MAC addresses for a specific VLAN.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

Variable definitions

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

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

Flushing a FastEthernet interface MAC address table

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

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

Variable definitions

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

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

Flushing a MAC address table for a trunk

Use this procedure to clear the MAC addresses for the specified trunk. This procedure flushes only addresses that are learned on the trunk.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
clear mac-address-table interface mlt <1-6>
```


Variable definitions

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

Variable	Value
<1-6>	Specifies the trunk for which you want to flush the MAC addresses.

Flushing a single address from the MAC address table

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

Variable definitions

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

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

Chapter 9: STP configuration using CLI

This chapter describes how to configure the Spanning Tree Protocol using the Command Line Interface (CLI).

Using spanning tree

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

For detailed information about spanning tree parameters, Spanning Tree Groups, and configuration guidelines, see [Spanning Tree Protocol Fundamentals](#) on page 32.

Displaying spanning tree configuration information

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

Variable definitions

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

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

Setting path cost calculation

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```
2. At the command prompt, enter the following command:

```
spanning-tree cost-calc-mode [dot1d|dot1t]
```

Configuring STG parameters

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```
2. At the command prompt, enter the following command:

```
spanning-tree [cost-calc-mode][forward-time <4-30>] [hello-time <1-10>] [max-age <6-40>][mode][multicast-address <H.H.H>][port-mode] [priority {0*0000 | 0*1000 | 0*2000 | 0*3000 | ... | 0*E000 | 0*F000}]
```
3. To reset to default, use the following command:

```
default spanning-tree [cost-calc-mode][forward-time] [hello-time] [max-age][multicast-address][mode][port-mode] [priority]
```

Variable definitions

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

Variable	Value
cost-calc-mode	Specifies pathcost type.
forward-time <4-30>	Specifies the forward time of the STG in seconds. RANGE: 4-30 seconds DEFAULT: 15 seconds
hello-time <1-10>	Specifies the hello time of the STG in seconds. RANGE: 1-10 seconds DEFAULT: 2 seconds

Table continues...

Variable	Value
max-age <6–40>	Specifies the max-age of the STG in seconds. RANGE: 6–40 seconds DEFAULT: 20 seconds
multicast-address<H.H.H>	Specifies spanning-tree multicast MAC address to default.
mode	Specifies the operation mode as one of the following protocols: <ul style="list-style-type: none"> • mstp — multiple spanning tree protocol • rstp —rapid spanning tree protocol • stpg — spanning tree group protocol
port-mode	Specifies the port mode.
priority {0*0000 0*1000 0*2000 0*3000 ... 0*E000 0*F000}	Sets the spanning tree priority (in Hex); if 802.1T compliant, this value must be a multiple of 0x10000.
default	Sets the STP parameters to their default values.

Configuring STG operation mode

Warning:

To prevent the stack from losing its configuration, multiple power cycling (hard resets) is not recommended after alternately changing spanning-tree operation mode.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Variable definitions

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

Variable	Value
mode {mstp rstp stpg}	Specifies the operation mode as one of the following protocols: <ul style="list-style-type: none"> • mstp — multiple spanning tree protocol • rstp —rapid spanning tree protocol • stpg — spanning tree group protocol

Configuring STP for ports

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port> or interface vlan <1-4094>
```

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

```
[default] spanning-tree [port <portlist>] [learning {disable|normal|fast}] [cost <1-65535>] [priority <0-255>]
```

Variable definitions

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

Variable	Value
port <portlist>	<p>Enables spanning tree for the specified port or ports; enter the port or ports you want enabled for spanning tree.</p> <p>! Important:</p> <p>If you omit this parameter, the system uses the port number you specified after you issued the interface command.</p>
learning {disable normal fast}	<p>Specifies the STP learning mode:</p> <ul style="list-style-type: none"> • disable — disable spanning tree on the port • normal — normal learning mode • fast — FastLearn mode <p>If [default] is used with the learning parameter, the learning mode is set to the default mode of normal mode.</p>
cost <1-65535>	<p>Enter the path cost of the spanning tree.</p> <p>RANGE: 1 to 65535</p> <p>DEFAULT: The default value for path cost depends on the type of port.</p>
priority <0-255>	<p>Enter the priority value of the spanning tree.</p> <p>RANGE: 0 to 255</p> <p>DEFAULT: 0x8000.</p> <p>If [default] is used with the priority parameter, the priority is set to the default value of 0x8000.</p>

Configuring STP port mode

Use this procedure to configure Spanning Tree port mode to enable a port to maintain STP membership when the port is moved from one VLAN to another.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:

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

Variable definitions

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

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

Enabling or disabling STP 802.1d compliance mode

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

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:

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

Disabling STP for ports

Use this procedure to disable STP for ports in a specific STG.

Procedure

1. Enter Interface Configuration mode:

```
enable
```

```
configure terminal
```


```
interface Ethernet <port> or interface vlan <1-4094>
```

- At the command prompt, enter the following command:

```
no spanning-tree [port <portlist>]
```

Variable definitions

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

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

Using Advanced Spanning Tree

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

Displaying RSTP configuration details

Procedure

- Enter Privileged EXEC mode:

```
enable
```

- At the command prompt, enter the following command:

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

Displaying RSTP bridge statistics

Procedure

- Enter Privileged EXEC mode:

```
enable
```

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

```
show spanning-tree rstp statistics
```

Displaying RSTP status information

Procedure

1. Enter Privileged EXEC mode:
2. At the command prompt, enter the following command:

```
enable
```

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

Displaying RSTP port configuration details

Procedure

1. Enter Privileged EXEC mode:
2. At the command prompt, enter the following command:

```
enable
```

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

Variable definitions

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

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

Displaying RSTP port role

Procedure

1. Enter Privileged EXEC mode:
2. At the command prompt, enter the following command:

```
enable
```

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


Variable definitions

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

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

Displaying RSTP port statistics

Procedure

1. Enter Privileged EXEC mode:

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

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

Variable definitions

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

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

Displaying RSTP status per port

Procedure

1. Enter Privileged EXEC mode:

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

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

Variable definitions

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

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

Configuring RSTP parameters

Use this procedure to set the RSTP parameters, which include forward delay, hello time, maximum age time, default pathcost version, bridge priority, transmit hold count, and version for the bridge.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Variable definitions

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

Variable	Value
port <portlist>	Filters on the list of ports.
cost <1 — 200000000>	Sets the RSTP pathcost on the single or multiple ports. DEFAULT: 200000.
edge-port {false true}	Indicates whether the single or multiple ports should be assumed to be edge port. This parameter sets the Admin value of edge port status. DEFAULT: false
learning {disable enable}	Enables or disables RSTP on the single or multiple ports. DEFAULT: enable
p2p {auto force-false force-true}	Indicates whether the single or multiple port should be treated as a point-to-point link or not. This command sets the Admin value of P2P status. DEFAULT: force-true
priority {00 10 ... F0}	Sets the RSTP port priority on the single or multiple port. DEFAULT: 80

Table continues...

Variable	Value
protocol-migration <i>{false true}</i>	Forces the single or multiple ports to transmit RSTP BPDUs when set true, while operating in RSTP mode. DEFAULT: false

Displaying MSTP related information

Use this procedure to display the MSTP related bridge-level, VLAN, and region information.

Procedure

1. Enter Privileged EXEC mode:
`enable`
2. At the command prompt, enter the following command:
`show spanning-tree mstp config`

Displaying MSTP status information

Procedure

1. Enter Privileged EXEC mode:
`enable`
2. At the command prompt, enter the following command:
`show spanning-tree mstp status`

Displaying MSTP related statistics

Procedure

1. Enter Privileged EXEC mode:
`enable`
2. At the command prompt, enter the following command:
`show spanning-tree mstp statistics`

Displaying MSTP Cist port information

Use this procedure to display the MSTP Cist Port information maintained by every port of the Common Spanning Tree.

Procedure

1. Enter Privileged EXEC mode:
enable
2. At the command prompt, enter the following command:
show spanning-tree mstp port config [<portlist>]

! Important:

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

Variable definitions

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

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

Displaying MSTP Cist port role**Procedure**

1. Enter Privileged EXEC mode:
enable
2. At the command prompt, enter the following command:
show spanning-tree mstp port role [<portlist>]

Variable definitions

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

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

Displaying MSTP Cist port statistics**Procedure**

1. Enter Privileged EXEC mode:

```
enable
```

- At the command prompt, enter the following command:

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

Variable definitions

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

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

Displaying MSTP bridge and VLAN information

Procedure

- Enter Privileged EXEC mode:

```
enable
```

- At the command prompt, enter the following command:

```
show spanning-tree mstp msti config <1 -7>
```

Variable definitions

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

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

Displaying MSTP bridge statistics

Procedure

- Enter Privileged EXEC mode:

```
enable
```

- At the command prompt, enter the following command:

```
show spanning-tree mstp msti statistics <1 -7>
```

Variable definitions

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

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

Displaying MSTP port information

Procedure

1. Enter Privileged EXEC mode:
enable
2. At the command prompt, enter the following command:
show spanning-tree mstp msti port config <1-7> [<portlist>]

Variable definitions

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

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

Displaying MSTP port role

Procedure

1. Enter Privileged EXEC mode:
enable
2. At the command prompt, enter the following command:
show spanning-tree mstp msti port role <1-7> [<portlist>]

Variable definitions

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

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

Displaying MSTP port statistics

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

Variable definitions

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

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

Configuring MSTP parameters for Cist bridge

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

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

Variable definitions

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

Variable	Value
max-hop <600-4000>	Sets the MSTP maximum hop count. DEFAULT: 2000
forward-time <4-30>	Sets the MSTP forward delay for the Cist Bridge in seconds.

Table continues...

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

Configuring MSTP parameters for Common Spanning Tree using CLI

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port> or interface vlan <1-4094>
```

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

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

Variable definitions

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

Variable	Value
port <portlist>	Specifies a list or range of port numbers.
cost <1 — 2000000000>	Sets the MSTP pathcost on the single or multiple port. DEFAULT: 200000
hello-time <1–10>	Sets the MSTP hello time on the single or multiple port for the Common Spanning Tree. DEFAULT: 2
edge-port {false true}	Indicates whether the single or multiple port should be assumed to be edge port or not. This parameter sets the Admin value of edge port status. DEFAULT: false
learning {disable enable}	Enables or disables MSTP on the single or multiple port. DEFAULT: enable
p2p {auto force-false force-true}	Indicates whether the single or multiple port should be treated as a point-to-point link or not. This command sets the Admin value of P2P Status. DEFAULT: force-true
priority {00 10 ... F0}	Sets the MSTP port priority on the single or multiple port. DEFAULT: 80
protocol-migration {false true}	Forces the single or multiple port to transmit MSTP BPDUs when set true, while operating in MSTP mode. DEFAULT: false

Configuring MSTP region parameters

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Variable definitions

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

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

Configuring MSTP MSTI bridge parameters

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Variable definitions

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

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

Configuring MSTP MSTI port parameters

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
```

```
interface Ethernet <port> or interface vlan <1-4094>
```

- At the command prompt, enter the following command:

```
spanning-tree mstp msti <1 - 7> [port <portlist>] [cost <1
-2000000000>][learning {disable | enable}][priority {00 | 10 | ...|
F0}]
```

Variable definitions

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

Variable	Value
<1-7>	Filter on MSTP instance.
port <portlist>	Enter a list or range of port numbers.
cost <1 — 2000000000>	Set the MSTP port pathcost on the single or multiple port for the bridge instance. DEFAULT: 200000
learning {disable enable}	Enable or disable MSTP on the single or multiple port for the bridge instance. DEFAULT: enable
priority {00 10 ... F0}	Set the MSTP port priority on the single or multiple port for the bridge instance. DEFAULT: 80

Deleting an MSTP bridge

Procedure

- Enter Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface Ethernet <port> or interface vlan <1-4094>
```

- At the command prompt, enter the following command:

```
no spanning-tree mstp msti <1-7>
```

Variable definitions

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

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

Enabling or disabling an MSTP bridge

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port> or interface vlan <1-4094>
```

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

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

Variable definitions

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

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

Configuring STP BPDU filtering

This procedure can be used in all STP modes (STPG, RSTP, and MSTP).

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port> or interface vlan <1-4094>
```

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

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

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

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

4. To disable, use the following command:

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

- To display the status of parameters, use the following command:

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

Variable definitions

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

Variable	Value
port <portlist>	Specifies the ports affected by the command.
enable	Enables STP BPDU Filtering on the specified ports. DEFAULT: Disabled
no	Disables STP BPDU Filtering on the specified ports.
default	Returns STP BPDU Filtering to the default value on the specified ports. DEFAULT: disabled
timeout <10–65535 0>	When BPDU filtering is enabled, this indicates the time (in seconds) during which the port remains disabled after it receives a BPDU. The port timer is disabled if this value is set to 0. DEFAULT: 120 seconds

Configuring STP Multicast Destination MAC address

Procedure

- Enter Global Configuration mode:


```
enable
```

```
configure terminal
```
- Enter the following command to configure the Multicast MAC address:


```
spanning-tree multicast-address <H.H.H>
```
- To display the new Multicast MAC address, use the following command:


```
show spanning-tree config
```

Example

The following shows an example outputs for the **spanning-tree multicast-address 01:02:03:04:05:06** command.

```
Switch(config)#spanning-tree multicast-address 01:02:03:04:05:06
Switch(config)#show spanning-tree config
```

STP configuration using CLI

```
Bridge Priority (hex):      8000
Designated Root:          10D3000C8544E900
Root Port:                 1
Root Path Cost:           37
Hello Time:                2 seconds
Maximum Age Time:         20 seconds
Forward Delay:            15 seconds
Bridge Hello Time:        2 seconds
Bridge Maximum Age Time:  20 seconds
Bridge Forward Delay:     15 seconds
Tagged BPDU on tagged port: No
VID used for Tagged BPDU: 4001
STP Group State:          Active
STP Multicast Address:    01:02:03:04:05:06
Switch#
```

Variable definitions

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

Variable	Value
<H.H.H>	Multicast MAC Address (i.e. H.H.H or XX:XX:XX:XX:XX:XX or XX.XX.XX.XX.XX.XX or XX-XX-XX-XX-XX-XX)

Chapter 10: Multi-Link Trunking configuration using CLI

This chapter describes how to configure multi-link trunking, link aggregation group, VLACP, distributed multi-link trunking, and distributed link aggregation group using CLI.

Configuring a Multi-Link Trunk

Important:

An MLT must be disabled when you are adding ports.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Variable definitions

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

Variable	Value
id	Specifies the trunk ID. RANGE: 1 to 6
name <trunkname>	Specifies a text name for the trunk. Enter up to 16 alphanumeric characters.
enable disable	Enables or disables the trunk.

Table continues...

Variable	Value
member <portlist>	Enter the ports that you want as members of the trunk.
learning <disable fast normal>	Sets STP learning mode.
loadbalance <advance basic>	Specifies MLT load balancing mode. Advance mode uses IP based load balancing. Basic mode uses MAC based load balancing.
bpdu {all-ports single-port}	Sets BPDU send/received mode.

Deleting a MultiLink Trunk

Procedure

1. Enter Global Configuration mode:


```
enable
configure terminal
```
2. At the command prompt, enter the following command to delete a specific MLT:


```
no mlt [<id>]
```
3. To delete all configured MLTs, enter the following command:


```
no mlt
```

Variable definitions

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

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

Configuring MLT whole trunk

Use this procedure to configure the shutdown of all ports in the MLT. This procedure enables or disables the MLT whole trunk feature.

Procedure

1. Enter Global Configuration mode:


```
enable
```



```
configure terminal
```

- At the command prompt, enter the following command:

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

Variable definitions

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

Variable	Value
no	Disables the MLT whole trunk feature.

Displaying MLT configuration

Use the following procedure to display MLT configuration and utilization.

Procedure

- Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- At the command prompt, enter the following command:

```
show mlt [spanning-tree <1-6>] | [utilization <1-6>]
```

Variable definitions

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

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

Displaying MLT members

Procedure

- Enter Privileged EXEC mode:

```
enable
```

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

```
show mlt all-members
```

Displaying the MLT whole trunk status

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

Example

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

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

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

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

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

Selecting an SLPP Guard Ethernet type

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Enter the following command to select an SLPP Guard ethernet type:

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

3. Enter the following command to configure the default value:

```
default slpp-guard ethertype
```

Variable definitions

The following table describes the parameters for the `slpp-guard ethertype` command.

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

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Enter the following command to configure SLPP Guard for switch ports:

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

Variable definitions

The following table describes the parameters for the `slpp-guard` command.

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

Table continues...

Variable	Value
	until it is manually re-enabled. The default timeout value is 60 seconds.

Using Distributed Multi-Link Trunking

Use the procedures in this section to configure Distributed Multi-Link Trunking (DMLT) using CLI.

Configuring DMLT

Use this procedure to configure Distributed Multi-Link Trunking (DMLT).

Procedure

1. Enter Global Configuration mode:


```
enable
configure terminal
```
2. At the command prompt, enter the following command:


```
mlt [<1-6> spanning-tree]
```

Variable definitions

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

Variable	Value
<1-6>	Specifies the MLT ID
spanning tree	Sets MTL spanning-tree settings

Displaying DMLT configuration

Use this procedure to display Distributed Multi-Link Trunking (DMLT) configuration and utilization.

Procedure

1. Enter Global Configuration mode:


```
enable
configure terminal
```
2. At the command prompt, enter the following command:


```
show mlt [utilization <1-6>] [spanning-tree <1-6>]
```

Variable definitions

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

Variable	Value
utilization <1-6>	Displays the utilization of the specified enabled MLT(s) in percentages.
spanning tree <1-6>	Displays Multi-Link trunk spanning tree settings.

Chapter 11: Configuring ADAC for IP Phones using CLI

Configuring global ADAC settings

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. At the command prompt, enter the following command to enable global settings for ADAC:

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

Variable definitions

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

Variable	Value
enable	Enables ADAC on the device.
op-mode { <i>untagged-frames-basic</i> <i>untagged-frames-advanced</i> <i>tagged-frames</i> }	Sets the ADAC operation mode to one of the following: <ul style="list-style-type: none">• <i>untagged-frames-basic</i>: IP Phones send untagged frames, and the Voice VLAN is not created• <i>untagged-frames-advanced</i>: IP Phones send untagged frames, and the Voice VLAN is created• <i>tagged-frames</i>: IP Phones send tagged frames, and the Voice VLAN is created
voice-vlan <1-4094>	Sets the Voice VLAN ID. The assigned VLAN ID must previously be created as a voice-vlan..
uplink-port < <i>portlist</i> >	Configures a maximum of 8 ports as uplink ports.

Table continues...

Variable	Value
call-server-port <portlist>	Configures a maximum of 8 ports as Call Server ports.
mac-range-table {low-end}{0123.4567.89ab}{high-end}{0123.4567.89ff}	<p>Adds new supported MAC address range.</p> <p>! Important: MAC address must be entered in Hexadecimal format.</p> <p>! Important: Specify the low-end parameter first to set the high-end parameter (H.H.H/xx.xx.xx.xx.xx.xx) for mac-range-table.</p>

Disabling or clearing ADAC settings

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Variable definitions

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

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

Resetting ADAC settings to the default

Use this procedure to restore default ADAC settings on the device.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Variable definitions

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

Variable	Value
enable	Restores the default state of ADAC
op-mode	Restores the default ADAC operation mode
voice-vlan	Restores the default Voice-VLAN ID
uplink-port	Restores the default Uplink port
call-server-port	Restores the default Call Server port
mac-range-table	Restores the MAC address ranges supported by default

Configuring ADAC MAC address range

Use this procedure to add or delete a specified range to the table of MAC addresses recognized as IP Phones by the Auto-Detection process.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Variable definitions

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

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

Resetting MAC address ranges using CLI

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

Procedure

1. Enter Global Configuration mode:


```
enable
configure terminal
```
2. At the command prompt, enter the following command:


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

Configuring ADAC device settings per port

Use this procedure to set ADAC settings for the device on a specific port.

Procedure

1. Enter Interface Configuration mode:


```
enable
configure terminal
interface Ethernet <port> or interface vlan <1-4094>
```
2. At the command prompt, enter the following command:

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

Variable definitions

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

Variable	Value
enable	Enables auto-detection on ports
port <portlist>	Specifies the port number for which settings are to be changed
tagged-frames-pvid {<1-4094> no-change}	Sets Tagged-Frames PVID on the port or ports listed. Use <i>no-change</i> to keep the current setting
tagged-frames-tagging{tagAll tagPvidOnly untagPvidOnly no-change}	Sets Tagged-Frames Tagging to: <ul style="list-style-type: none"> • tagAll • tagPvidOnly • untagPvidOnly Use <i>no-change</i> to keep the current setting.
detection{[mac][lldp]}	Enables detection mechanisms on ports; either mac or lldp.

Setting ADAC detection method

Use this procedure to set the detection method, by MAC address or using LLDP (IEEE 802.1AB) for a device on a port.

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port> or interface vlan <1-4094>
```

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

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

Variable definitions

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

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

Disabling ADAC per port

Use this procedure to disable ADAC settings for the device on a specific port.

Procedure

1. Enter Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface Ethernet <port> or interface vlan <1-4094>
```

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

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

Variable definitions

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

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

Resetting ADAC port settings to default

Use this procedure to restore the per port ADAC settings to defaults for the specified ports.

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port> or interface vlan <1-4094>
```

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

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

Variable definitions

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

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

Restoring ADAC detection method to default

Use this procedure to restore the ADAC auto-detection method by either MAC address or LLDP for a device on a port.

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port> or interface vlan <1-4094>
```

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

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

Variable definitions

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

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

Displaying ADAC settings per port

Use this procedure to display ADAC settings for the device on a specific port.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Variable definitions

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

Variable	Value
Type	Specifies how ADAC classifies this port: <ul style="list-style-type: none"> • T: Telephony port • CS: Call Server port • U: Uplink port or part of the same trunk as the current set uplink port
Auto-Detection	Controls whether the interface should auto-detect; if there is any IP Phone connected to it (and implicitly apply auto-configuration for it)

Table continues...

Variable	Value
Oper State	Indicates whether ADAC is enabled or disabled on that port
Auto-Configuration	Specifies if the auto-configuration is applied on a port or not
Tagged-Frames PVID	Specifies the PVID value that Auto-Configuration apply for ports having Auto-Detection enabled and running in Tagged-Frames operational mode. A value of 0 indicates that Auto-Configuration cannot change the PVID for the respective port. If the VLAN with the ID equal with this PVID does not exist when Auto-Configuration is applied to a port, then Auto-Configuration won't change the port's PVID (it will ignore the current value of this parameter, and treat it as if its value is currently 0);
Tagged-FramesTagging	Specifies the tagging value that Auto-Configuration apply for ports having Auto-Detection enabled and running in Tagged-Frames operational mode.

Displaying ADAC MAC range

Use this procedure to display the range of MAC addresses used by ADAC to identify an IP Phone with the MAC detection mechanism.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:

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

Displaying ADAC detection method status

Use this procedure to display the status of detection mechanism for the device on a specific port.

Procedure

1. Enter Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface Ethernet <port> or interface vlan <1-4094>
```

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

```
show adac detection interface
```

Chapter 12: Configuring LACP and VLACP using CLI

Configuring Link Aggregation Group using CLI

Use the procedures in this section to configure 802.3ad Link Aggregation (D-LAG) using CLI.

Related links

- [Configuring LACP system priority](#) on page 112
- [Configuring LACP port mode](#) on page 113
- [Resetting LACP port mode to default](#) on page 113
- [Enabling or removing LACP aggregation for ports](#) on page 114
- [Assigning a key value to a port](#) on page 115
- [Assigning LACP priority for ports](#) on page 116
- [Configuring LACP timeout](#) on page 116
- [Displaying LACP information](#) on page 117
- [Displaying LACP aggregator information](#) on page 117
- [Displaying LACP port information](#) on page 118
- [Displaying LACP port debug information](#) on page 119
- [Displaying LACP port statistics information](#) on page 120
- [Clearing LACP port statistics](#) on page 121

Configuring LACP system priority

Use this procedure to set a system priority for LACP.

Procedure

1. Enter Global Configuration mode:

```
enable  
configure terminal
```
2. At the command prompt, enter the following command:

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


Related links

[Configuring Link Aggregation Group using CLI](#) on page 112

[Variable definitions](#) on page 113

Variable definitions

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

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

Related links

[Configuring LACP system priority](#) on page 112

Configuring LACP port mode

Use this procedure to set the mode for an LACP port.

Procedure

1. Enter Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface Ethernet <port> or interface vlan <1-4094>
```

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

```
lACP mode [port <portlist>] {off|passive}active}
```

Related links

[Configuring Link Aggregation Group using CLI](#) on page 112

Resetting LACP port mode to default

Use this procedure to place an LACP port in the default mode.

Procedure

1. Enter Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface Ethernet <port> or interface vlan <1-4094>
```

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

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

Related links

[Configuring Link Aggregation Group using CLI](#) on page 112

[Variable definitions](#) on page 114

Variable definitions

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

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

Related links

[Resetting LACP port mode to default](#) on page 113

Enabling or removing LACP aggregation for ports

Use this procedure to enable or remove LACP aggregation on the specified port(s).

Procedure

1. Enter Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface Ethernet <port> or interface vlan <1-4094>
```

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

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

Related links

[Configuring Link Aggregation Group using CLI](#) on page 112

[Variable definitions](#) on page 114

Variable definitions

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

Variable	Value
port <portlist>	Specifies the port(s) you want to enable LACP aggregation.

Table continues...

Variable	Value
no	Removes LACP aggregation for the specified port(s)
default	Disables LACP aggregation by default.

Related links

[Enabling or removing LACP aggregation for ports](#) on page 114

Assigning a key value to a port

Use this procedure to assign a key value for the specified port(s).

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port> or interface vlan <1-4094>
```

2. At the command prompt, enter the following command to assign a key value :

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

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

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

Related links

[Configuring Link Aggregation Group using CLI](#) on page 112

[Variable definitions](#) on page 115

Variable definitions

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

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

Related links

[Assigning a key value to a port](#) on page 115

Assigning LACP priority for ports

Use this procedure to set an LACP priority for the specified port(s).

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port> or interface vlan <1-4094>
```

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

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

Related links

[Configuring Link Aggregation Group using CLI](#) on page 112

[Variable definitions](#) on page 116

Variable definitions

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

Variable	Value
port <portlist>	Specifies the ports for which you want to set LACP priority.
<0-65535>	Specifies a priority number for the port. RANGE: 0 to 65535 DEFAULT: 32768
default	Sets the LACP priority for the specified port(s) to the default value of 32768.

Related links

[Assigning LACP priority for ports](#) on page 116

Configuring LACP timeout

Use this procedure to set an LACP timeout for the specified port(s).

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
```

```
interface Ethernet <port> or interface vlan <1-4094>
```

- At the command prompt, enter the following command:

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

Related links

[Configuring Link Aggregation Group using CLI](#) on page 112

[Variable definitions](#) on page 117

Variable definitions

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

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

Related links

[Configuring LACP timeout](#) on page 116

Displaying LACP information

Use this procedure to display LACP information for the entire system.

Procedure

- Enter Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface Ethernet <port> or interface vlan <1-4094>
```

- At the command prompt, enter the following command:

```
show lacp system
```

Related links

[Configuring Link Aggregation Group using CLI](#) on page 112

Displaying LACP aggregator information

Use this procedure to display LACP aggregator information.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:

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

Related links

- [Configuring Link Aggregation Group using CLI](#) on page 112
- [Variable definitions](#) on page 118

Variable definitions

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

Variable	Value
<1-65535>	Specifies the aggregator ID

Related links

- [Displaying LACP aggregator information](#) on page 117

Displaying LACP port information

Use this procedure to display LACP port information..

Procedure

1. Enter Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface Ethernet <port> or interface vlan <1-4094>
```
2. At the command prompt, enter the following command:

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

Important:

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

Related links

- [Configuring Link Aggregation Group using CLI](#) on page 112
- [Variable definitions](#) on page 119

Variable definitions

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

Variable	Value
aggr	Selects port that are members of aggregator
port <portlist>	Specifies the ports for which you want information.

Related links

[Displaying LACP port information](#) on page 118

Displaying LACP port debug information

Use this procedure to display LACP port debug information.

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port> or interface vlan <1-4094>
```

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

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

The command can display the following terms:

LACP Receiving State:

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

Selection State:

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

Related links

[Configuring Link Aggregation Group using CLI](#) on page 112

[Variable definitions](#) on page 120

Variable definitions

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

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

Related links

[Displaying LACP port debug information](#) on page 119

Displaying LACP port statistics information

Use this procedure to display LACP port statistics information.

Procedure

1. Enter Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface Ethernet <port> or interface vlan <1-4094>
```

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

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

Related links

[Configuring Link Aggregation Group using CLI](#) on page 112

[Variable definitions](#) on page 120

Variable definitions

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

Variable	Value
aggr	Selects port that are members of aggregator
port <portlist>	Specifies the port(s) for which you want statistics.

Related links

[Displaying LACP port statistics information](#) on page 120

Clearing LACP port statistics

Use this procedure to clear port statistics.

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port> or interface vlan <1-4094>
```

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

```
lacp clear-stats [port <portlist>]
```

Related links

[Configuring Link Aggregation Group using CLI](#) on page 112

[Variable definitions](#) on page 121

Variable definitions

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

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

Related links

[Clearing LACP port statistics](#) on page 121

Configuring Static LACP Key to Trunk ID binding

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

* Note:

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

Binding an LACP key to a specific trunk ID

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

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- At the command prompt, enter the following command:

```
lacp key <1-4095> mlt-id <1-6>
```

Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#lacp key 11 mlt-id 1
```

Variable definitions

Name	Description
<1-4095>	The LACP key to use.
<1-6>	The MLT ID.

Deleting an LACP key binding to a trunk ID

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

Procedure

- Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- At the command prompt, enter the following command:

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

Note:

The MLT ID for the defaulted LACP key becomes 0.

Variable definitions

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

Displaying LACP key bindings to trunk IDs

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

Procedure

- Enter Privileged EXEC mode:

```
enable
```

- Use the following command to display all LACP key bindings:

```
show lacp key
```

- Use the following command to display a specific LACP binding:

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

Variable definitions

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

Configuring VLACP using CLI

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

* Note:

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

Enabling or disabling VLACP globally

Use this procedure to enable or disable VLACP globally for the device using this procedure.

Procedure

- Enter Global Configuration mode:


```
enable
```

```
configure terminal
```
- At the command prompt, enter the following command:


```
[no] vlacp enable
```

Variable definitions

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

Variable	Value
no	Disables VLACP globally for the device.

Configuring multicast MAC address for VLACP

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

Procedure

- Enter Global Configuration mode:

```
enable
configure terminal
```

- At the command prompt, enter the following command:

```
vlacp macaddress <macaddress>
```

Variable definitions

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

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

Configuring VLACP on a port

Use this procedure to configure VLACP parameters on a port.

Procedure

- Enter Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port> or interface vlan <1-4094>
```

- At the command prompt, enter the following command:

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

Variable definitions

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

Variable	Value
<i><port></i>	Specifies the port number.
enable disable	Enables or disables VLACP.
timeout <i><long/short></i>	Specifies whether the timeout control value for the port is a long or short timeout. <ul style="list-style-type: none"> long sets the port timeout value to: (timeout-scale value) x (slow-periodic-time value). short sets the port's timeout to: (timeout-scale value) x (fast-periodic-time value).

Table continues...

Variable	Value
	<p>For example, if the timeout is set to short while the timeout-scale value is 3 and the fast-periodic-time value is 400 ms, the timer expires after 1200 ms.</p> <p>DEFAULT: long</p>
fast-periodic-time <integer>	<p>Specifies the number of milliseconds between periodic VLACPDU transmissions using short timeouts.</p> <p>RANGE: 400 to 20000 ms</p> <p>DEFAULT: 500 ms</p>
slow-periodic-time <integer>	<p>Specifies the number of milliseconds between periodic VLACPDU transmissions using long timeouts.</p> <p>RANGE: 10000 to 30000 ms</p> <p>DEFAULT: 30000 ms</p>
timeout-scale <integer>	<p>Sets a timeout scale for the port, where timeout = (periodic time) x (timeout scale).</p> <p>RANGE: 1 to 10</p> <p>DEFAULT: 3</p> <p>* Note:</p> <p>With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. However, if the timeout-scale is set to 1, the port timeout value does not take into account the normal travel time of the VLACPDU. The port expects to receive a VLACPDU at the same moment the partner port sends it. Therefore, the delayed VLACPDU results in the link being blocked, and then enabled again after the packet arrives. To prevent this scenario from happening, set the timeout-scale to a value larger than 1.</p>
funcmac-addr <macaddress>	<p>Specifies the address of the far-end switch or stack configured to be the partner of this switch or stack. If none is configured, any VLACP-enabled switch communicating with the local switch through VLACP PDUs is considered to be the partner switch.</p> <p>* Note:</p> <p>VLACP has only one multicast MAC address, configured using the <code>vlacp macaddress</code> command, which is the Layer 2 destination address used for the VLACPDUs. The port-</p>

Table continues...

Variable	Value
	<p>specific funcmac-addr parameter does not specify a multicast MAC address, but instead specifies the MAC address of the switch or stack to which this port is sending VLACPDUs. You are not always required to configure funcmac-addr. If not configured, the first VLACP-enabled switch that receives the PDUs from a unit assumes that it is the intended recipient and processes the PDUs accordingly.</p> <p>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.</p>
ethertype <hex>	<p>Sets the VLACP protocol identification for this port. Defines the ethertype value of the VLACP frame.</p> <p>RANGE: 8101–81FF</p> <p>DEFAULT: 8103</p>

Resetting VLACP MAC address value

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

Procedure

1. Enter Global Configuration mode:


```
enable
configure terminal
```
2. At the command prompt, enter the following command:


```
no vlacp macaddress
```

Disabling VLACP on a port

Use this procedure to disable VLACP on the port.

Procedure

1. Enter Global Configuration mode:


```
enable
```

```
configure terminal
```

- At the command prompt, enter the following command:

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

Variable definitions

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

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

Displaying VLACP status

Use this procedure to display the status of VLACP on the switch.

Procedure

- Enter Privileged EXEC mode:

```
enable
```

- At the command prompt, enter the following command:

```
show vlacp
```

Displaying VLACP configuration for a port

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

Procedure

- Enter Privileged EXEC mode:

```
enable
```

- At the command prompt, enter the following command:

```
show vlacp interface <port>
```

Among other properties, the `show vlacp interface` command displays a column called `HAVE PARTNER`, with possible values of `yes` or `no`.

If `HAVE PARTNER` is `yes` when `ADMIN ENABLED` and `OPER ENABLED` are `true`, then that port has received VLACPDUs from a port and those PDUs were recognized as valid according to the interface settings.

If `HAVE PARTNER` is `no`, when `ADMIN ENABLED` and `OPER ENABLED` are `true`, then that port did not receive any VLACPDUs yet.

If `HAVE PARTNER` is `no`, when `ADMIN ENABLED` is `true` and `OPER ENABLED` is `FALSE`, then the partner for that port is down (that port received at least one correct VLACPDUs, but did not receive additional VLACPDUs within the configured timeout period). In this case, VLACP blocks the port.

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

Variable definitions

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

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

Chapter 13: Configuring VLANs using Enterprise Device Manager

This chapter describes how to use Enterprise Device Manager (EDM) to manage VLANs on your switch. You can use EDM to create, edit, and delete VLANs on your switch or stack.

VLANs

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

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

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

Related links

[VLAN management using EDM](#) on page 129

[VLAN configuration for ports using EDM](#) on page 142

[Selecting VLAN configuration control using EDM](#) on page 145

[Port configuration for VLANs using EDM](#) on page 146

[Configuring an IPv6 interface using EDM](#) on page 150

[MAC address table management using EDM](#) on page 151

[Link Aggregation Control Protocol](#) on page 155

[Configuring MLT and VLACP global settings using EDM](#) on page 167

[VLACP configuration for ports using EDM](#) on page 169

VLAN management using EDM

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

Displaying VLAN information using EDM

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

Procedure

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

VLAN display field descriptions

The following table describes the fields in the VLAN display.



Name	Description
Id	Indicates the VLAN ID for the VLAN.
Name	Indicates the name of the VLAN.
Ifindex	Indicates the interface index. This is a read-only value.
Type	Indicates the type of VLAN. Values include: <ul style="list-style-type: none"> • byPort: VLAN by port • byProtocolId: VLAN by protocol ID
VoiceEnabled	Indicates whether VLAN is a voice VLAN (true) or not (false).
PortMembers	Indicates the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only field.
StgId	Indicates the Spanning Tree Group to which the selected port(s) belongs. <p> Important:</p> This column is available only when the switch is operating in STG mode. The switch does not support multiple STGs when operating in the STPG mode.
ProtocolId	Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is byProtocolId; otherwise the protocol ID value is none (0). Values include: <ul style="list-style-type: none"> • 0

Table continues...

Name	Description
	<ul style="list-style-type: none"> ipV6
UserDefinedPid	Indicates the user defined protocol identifier for a protocol-based VLAN.
MstpInstance	<p>Indicates the MSTP instance associated with the VLAN. Values include:</p> <ul style="list-style-type: none"> none cist msti 1–7 <p> Important: This column is available only when the switch is operating in the MSTP mode.</p>
MacAddress	Indicates the MAC address associated with the VLAN.
Routing	Indicates whether routing is enabled (true) or disabled (false) for the VLAN.

Modifying an existing VLAN in STG mode using EDM

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

Procedure

- In the navigation tree, double-click **VLAN**.
- Double-click **VLANs**.
- In the work area, click the **Basic** tab.
- To select a VLAN to edit, click the **VLAN ID**.
- In the VLAN row, double-click the cell in the **Name** column.
- Type a character string to assign a unique name to the VLAN.
- In the VLAN row, double-click the cell in the **VoiceEnabled** column.
- Select a value from the list — true to specify the VLAN as a voice VLAN, or false to indicate the VLAN is not a voice VLAN.
- In the VLAN row, double-click the cell in the **PortMembers** column.
- Select ports to add to the VLAN.
OR
Deselect ports to remove them from the VLAN.
- Click **Ok**.

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

VLAN in STG mode field descriptions

The following table describes the fields on the VLAN in STG mode tab.


Name	Description
Id	Indicates the VLAN ID for the VLAN. This is a read-only value.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
Ifindex	Indicates the interface index. This is a read-only value.
Type	Indicates the type of VLAN. Values include: <ul style="list-style-type: none"> • byPort: VLAN by port • byProtocolId: VLAN by protocol ID This is a read-only value.
VoiceEnabled	Specifies whether VLAN is a voice VLAN (true) or not (false).
PortMembers	Specifies the ports that are members of the VLAN.
StgId	Indicates the Spanning Tree Group to which the selected port or ports belong. This is a read-only value. <p> Important:</p> This column is available only when the Spanning Tree administration operating mode is STG. The switch does not support multiple STGs when operating in the STG mode.
ProtocolId	Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is byProtocolId; otherwise the protocol ID value is none (0). Values include: <ul style="list-style-type: none"> • 0 • ipV6 This is a read-only value.
UserDefinedPid	Indicates the user defined protocol identifier for a protocol-based VLAN. This is a read-only value.

Table continues...

Name	Description
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Indicates whether routing is enabled (true) or disabled (false) for the VLAN.

Modifying an existing VLAN in RSTP mode using EDM

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

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. To select a VLAN to edit, click the VLAN ID.
5. In the VLAN row, double-click the cell in the **Name** column.
6. Type a character string to assign a unique name to the VLAN.
7. In the VLAN row, double-click the cell in the **VoiceEnabled** column.
8. Select a value from the list — true to specify the VLAN as a voice VLAN, or false to indicate the VLAN is not a voice VLAN.
9. In the VLAN row, double-click the cell in the **PortMembers** column.
10. Select ports to add to the VLAN.
OR
Deselect ports to remove them from the VLAN.
11. Click **Ok**.
12. In the VLAN row, double-click the cell in the **Routing** column.
13. Select a value from the list — true to enable routing for the VLAN, or false to disable routing for the VLAN.
14. On the toolbar, click **Apply**.

VLAN in RSTP mode field descriptions

The following table describes the fields for VLAN in RSTP mode..

Name	Description
Id	Indicates the VLAN ID for the VLAN. This is a read-only value.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
Ifindex	Indicates the interface index. This is a read-only value.
Type	Indicates the type of VLAN. Values include: <ul style="list-style-type: none"> • byPort: VLAN by port • byProtocolId: VLAN by protocol ID This is a read-only value.
VoiceEnabled	Specifies whether VLAN is a voice VLAN (true) or not (false).
PortMembers	Specifies the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.
ProtocolId	Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is byProtocolId; otherwise the protocol ID value is none (0). Values include: <ul style="list-style-type: none"> • 0 • ipv6 This is a read-only value.
UserDefinedPid	Indicates the user defined protocol identifier for a protocol-based VLAN. This is a read-only value.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Indicates whether routing is enabled (true) or disabled (false) for the VLAN.

Modifying an existing VLAN in MSTP mode using EDM

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

Procedure

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


3. In the work area, click the **Basic** tab.
4. To select a VLAN to edit, click the VLAN ID.
5. In the VLAN row, double-click the cell in the **Name** column.
6. Type a character string to assign a unique name to the VLAN.
7. In the VLAN row, double-click the cell in the **VoiceEnabled** column.
8. Select a value from the list — true to specify the VLAN as a voice VLAN, or false to indicate the VLAN is not a voice VLAN.
9. In the VLAN row, double-click the cell in the **PortMembers** column.
10. Select ports to add to the VLAN.
OR
Deselect ports to remove them from the VLAN.
11. Click **Ok**.
12. In the VLAN row, double-click the cell in the **MstpInstance** column, if the switch is in MSTP mode.
13. Select a value from the list.
14. In the VLAN row, double-click the cell in the **Routing** column.
15. Select a value from the list — true to enable routing for the VLAN, or false to disable routing for the VLAN.
16. On the toolbar, click **Apply**.

VLAN in MSTP mode field descriptions

The following table describes the fields for VLAN in MSTP mode.

Name	Description
Id	Indicates the VLAN ID for the VLAN. This is a read-only value.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
Ifindex	Indicates the interface index. This is a read-only value.
Type	Indicates the type of VLAN. Values include: <ul style="list-style-type: none"> • byPort: VLAN by port • byProtocolId: VLAN by protocol ID This is a read-only value.
VoiceEnabled	Specifies whether VLAN is a voice VLAN (true) or not (false).

Table continues...

Name	Description
PortMembers	Specifies the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.
MstpInstance	Indicates the MSTP instance associated with the VLAN. Values include: <ul style="list-style-type: none"> • none • cist • msti 1–7  Important: This column is available only when the Spanning Tree administration operating mode is MSTP.
ProtocolId	Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is byProtocolId; otherwise the protocol ID value is none (0). Values include: <ul style="list-style-type: none"> • 0 • ipv6 This is a read-only value.
UserDefinedPid	Indicates the user defined protocol identifier for a protocol-based VLAN. This is a read-only value.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Indicates whether routing is enabled (true) or disabled (false) for the VLAN.

Creating a VLAN in STG mode using EDM

Use this procedure to create a new VLAN when the switch is in STG mode.

Before you begin

Select STG for the Spanning Tree administration mode.

Procedure

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


4. Click **Insert**.
5. In the **VLAN ID** field, type a value.
OR
Accept the default ID for the VLAN.
6. In the **Name** field, type a value.
OR
Accept the default name for the VLAN.
7. In the **Type** field, select **byPort** or **byProtocolId**.
8. To configure the VLAN as a voice VLAN, check the **VoiceEnabled** checkbox.
9. Click **Insert**.
10. In the VLAN row, double-click the cell in the **PortMembers** column.
11. Select ports to add to the VLAN.
OR
Deselect ports to remove them from the VLAN.
12. Click **Ok**.
13. In the VLAN row, double-click the cell in the **Routing** column.
14. Select a value from the list — **true** to enable routing for the VLAN, or **false** to disable routing for the VLAN.
15. On the toolbar, click **Apply**.

VLAN in STG mode field descriptions

The following table describes the fields to create VLANs in STG mode.

Name	Description
Id	Specifies the VLAN ID for the VLAN.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
Ifindex	Indicates the interface index. This is a read-only value.
Type	Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is by ProtocolID. The only supported value is ipv6.
VoiceEnabled	Specifies whether VLAN is a voice VLAN (true) or not (false).
PortMembers	Specifies the ports that are members of the VLAN.

Table continues...

Name	Description
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.
StgId	Indicates the Spanning Tree Group to which the selected port or ports belong. This is a read-only value.  Important: This column is available only when the Spanning Tree administration operating mode is STG. The switch does not support multiple STGs when operating in the STPG mode.
ProtocolId	Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is byProtocolId; otherwise the protocol ID value is none (0). Values include: <ul style="list-style-type: none"> • 0 • ipV6
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Indicates whether routing is enabled (true) or disabled (false) for the VLAN.

Creating a VLAN in RSTP mode using EDM

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

Before you begin

Select RSTP for the Spanning Tree administration mode.

Procedure

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

OR

- Accept the default ID for the VLAN.
6. In the **Name** field, type a value.
OR
Accept the default name for the VLAN.
 7. In the **Type** field, select **byPort** or **byProtocolId**.
 8. To configure the VLAN as a voice VLAN, check the **VoiceEnabled** checkbox.
 9. Click **Insert**.
 10. In the VLAN row, double-click the cell in the **PortMembers** column.
 11. Select ports to add to the VLAN.
OR
Deselect ports to remove them from the VLAN.
 12. Click **Ok**.
 13. In the VLAN row, double-click the cell in the **Routing** column.
 14. Select a value from the list — **true** to enable routing for the VLAN, or **false** to disable routing for the VLAN.
 15. On the toolbar, click **Apply**.

VLAN in RSTP mode field descriptions

The following table describes the fields to create a VLAN in RSTP mode.

Name	Description
Id	Specifies the VLAN ID for the VLAN.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
Ifindex	Indicates the interface index. This is a read-only value.
Type	Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is by ProtocolID. The only supported value is ipv6.
VoiceEnabled	Specifies whether VLAN is a voice VLAN (true) or not (false).
PortMembers	Specifies the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.

Table continues...

Name	Description
ProtocolId	Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is byProtocolId; otherwise the protocol ID value is none (0). Values include: <ul style="list-style-type: none"> • 0 • ipv6
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Indicates whether routing is enabled (true) or disabled (false) for the VLAN.

Creating a VLAN in MSTP mode using EDM

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

Before you begin

Select MSTP for the Spanning Tree administration mode.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **VLANs**.
3. In the work area, click the **Basic** tab.
4. Click **Insert**.
5. In the **Id** dialog box, type a value.
OR
Accept the default ID for the VLAN.
6. In the **Name** dialog box, type a value.
OR
Accept the default name for the VLAN.
7. In the **Type** field, select **byPort** or **byProtocolId**.
8. To configure the VLAN as a voice VLAN, check the **VoiceEnabled** checkbox.
9. Click the **MstpInstance** box arrow.
10. Select a value from the list.
11. Click **Insert**.

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

VLAN in MSTP mode field descriptions

The following table describes the fields to create a VLAN in MSTP mode.


Name	Description
Id	Indicates the ID for the VLAN.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
Ifindex	Indicates the interface index. This is a read-only value.
Type	Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is byProtocolId. The only supported value is ipv6.
VoiceEnabled	Specifies whether VLAN is a voice VLAN (true) or not (false).
PortMembers	Specifies the ports that are members of the VLAN.
ActiveMembers	Indicates the ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. This is a read-only value.
MstpInstance	<p>The MSTP instance associated with the VLAN. Values include:</p> <ul style="list-style-type: none"> • none • cist • msti 1–7 <p> Important:</p> <p>This column is available only when the Spanning Tree administration operating mode is MSTP.</p>

Table continues...

Name	Description
ProtocolId	Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is byProtocolId; otherwise the protocol ID value is none (0). Values include: <ul style="list-style-type: none"> • 0 • ipv6
UserDefinedPid	Indicates the user defined protocol identifier for a protocol based VLAN.
MacAddress	Indicates the MAC address associated with the VLAN. This is a read-only value.
Routing	Indicates whether routing is enabled (true) or disabled (false) for the VLAN.

Deleting a VLAN using EDM

Use this procedure to delete a VLAN.

Procedure

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

VLAN configuration for ports using EDM

Use the information in this section to view and configure VLAN membership for specific ports.

Displaying VLAN membership port information using EDM

Use this procedure to display the VLAN membership information for switch ports.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **VLANs**.
3. Click the **Ports** tab.

VLAN port membership field descriptions

The following table describes the fields to help you understand the VLAN port membership.

Name	Description
Index	Indicates the switch position in the stack and the port number. This is read-only value.
VlanIds	Indicates the VLAN IDs of which this port is a member. This is a read-only value.
DiscardUntaggedFrames	<p>Indicates how untagged frames received on this port are processed.</p> <ul style="list-style-type: none"> • true: untagged frames are discarded by the forwarding process • false: untagged frames are assigned to the VLAN specified by the VLAN ID. <p>This column applies to trunk ports only.</p>
FilterUnregisteredFrames	<p>Indicates how unregistered frames received on this port are processed:</p> <ul style="list-style-type: none"> • true: unregistered frames are discarded by the forwarding process • false: unregistered frames are assigned to the VLAN specified by the VLAN ID. <p>This column applies to access ports only.</p>
DefaultVlanId	Indicates the VLAN ID assigned to untagged and unregistered frames received on a port.
PortPriority	<p>Indicates the port priority for the switch to consider as it forwards received packets.</p> <p>RANGE: 0 to 7</p>
Tagging	<p>Indicates the type of VLAN port. Possible values are:</p> <ul style="list-style-type: none"> • untagAll (access) • tagAll (trunk) • untagPvidOnly • tagPvidOnly <p>If the port is a trunk port, the port is often a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN.</p>

Configuring VLAN membership ports using EDM

Use this procedure to configure VLAN membership for one or more switch ports.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **VLANs**.
3. Click the **Ports** tab.
4. To select a port to edit, click the port row.
5. In the port row, double-click the cell in the **DiscardUntaggedFrames** column.
6. Select a value from the list — **true** to discard untagged frames for the port, or **false** to accept untagged frames for the port.
7. In the port row, double-click the cell in the **FilterUnregisteredFrames** column.
8. Select a value from the list — **true** to discard unregistered frames for the port, or **false** to process unregistered frames normally for the port.
9. In the port row, double-click the cell in the **DefaultVlanId** column.
10. Type a value for the default VLAN ID.
11. In the port row, double-click the cell in the **PortPriority** column.
12. Select a value from the list.
13. In the port row, double-click the cell in the **Tagging** column.
14. Select a value from the list.
15. Repeat steps 5 through 15 to configure VLAN memberships for additional ports.
16. On the toolbar, click **Apply**.

VLAN Membership ports field descriptions

The following table describes the fields to configure VLAN membership ports.

Name	Description
Index	Indicates the switch position in the stack and the port number. This is read-only value.
VlanIds	Indicates the VLAN IDs of which this port is a member. This is a read-only value.
DiscardUntaggedFrames	Indicates how untagged frames received on this port are processed. <ul style="list-style-type: none"> • true: untagged frames are discarded by the forwarding process • false: untagged frames are assigned to the VLAN specified by the VLAN ID. This column applies to trunk ports only.

Table continues...

Name	Description
FilterUnregisteredFrames	<p>Indicates how unregistered frames received on this port are processed:</p> <ul style="list-style-type: none"> • true: unregistered frames are discarded by the forwarding process • false: unregistered frames are assigned to the VLAN specified by the VLAN ID. <p>This column applies to access ports only.</p>
DefaultVlanId	Indicates the VLAN ID assigned to untagged and unregistered frames received on a port.
PortPriority	<p>Indicates the port priority for the switch to consider as it forwards received packets.</p> <p>RANGE: 0 to 7</p>
Tagging	<p>Indicates the type of VLAN port. Possible values are:</p> <ul style="list-style-type: none"> • untagAll (access) • tagAll (trunk) • untagPvidOnly • tagPvidOnly <p>If the port is a trunk port, the port is often a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN.</p>

Selecting VLAN configuration control using EDM

Use this procedure to select configuration control for a VLAN.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **VLANs**.
3. In the work area, click the **Settings** tab.
4. In the **ManagementVlanID** dialog box, type a value.
5. In the **VlanConfigControl** section, click a radio button.
6. On the toolbar, click **Apply**.

VLAN configuration control field descriptions

The following table describes the fields used to set VLAN configuration control.

Name	Description
ManagementVlanID	Specifies the identifier of the management VLAN. RANGE: 1 to 4094.
VlanConfigControl	<p>VlanConfigControl presents four selections:</p> <ul style="list-style-type: none"> • automatic: This selection automatically adds an untagged port to a new VLAN and automatically removes it from any previous VLAN membership. The PVID of the port is automatically changed to the new VID of the VLAN it joins. Since the port is first added to the new VLAN and then removed from any previous membership, the Spanning Tree Group participation of the port is not disabled as long as the VLANs involved are in the same Spanning Tree Group • autopvid: When an untagged port is added to a new VLAN, the port is added to the new VLAN and the PVID is assigned to the new VID without removing it from any previous VLAN memberships. Using this option, an untagged port can have membership in multiple VLANs. • flexible: This selection functions in a similar manner to disabling AutoPVID functionality. When this option is used, an untagged port can belong to an unlimited number of VLANs. Any new additions of an untagged port to a new VLAN do not change the PVID of that port. • strict: The factory default, this selection restricts the addition of an untagged port to a VLAN if it is already a member of another VLAN. To add an untagged port to a new VLAN, the switch administrator must remove the port from all other VLANs of which it is a member before adding it to a new VLAN. The PVID of the port is changed to the new VID to which it was added.

Port configuration for VLANs using EDM

Use the information in this section to view and configure specific ports for VLAN membership.

Displaying port VLAN membership information using EDM

Use this procedure to display the VLAN membership information for switch ports.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. Click the **VLAN** tab.

Port VLAN membership information field descriptions

The following table describes the fields used to display VLAN membership information.

Name	Description
Index	Indicates the switch position in the stack and the port number. This is read-only value.
Vlanids	Indicates the VLAN IDs of which this port is a member. This is a read-only value.
DiscardUntaggedFrames	Indicates how untagged frames received on this port are processed. <ul style="list-style-type: none"> • true: untagged frames are discarded by the forwarding process • false: untagged frames are assigned to the VLAN specified by the VLAN ID. This column applies to trunk ports only.
FilterUnregisteredFrames	Indicates how unregistered frames received on this port are processed: <ul style="list-style-type: none"> • true: unregistered frames are discarded by the forwarding process • false: unregistered frames are assigned to the VLAN specified by the VLAN ID. This column applies to access ports only.
DefaultVlanId	Indicates the VLAN ID assigned to untagged and unregistered frames received on a port.
PortPriority	Indicates the port priority for the switch to consider as it forwards received packets. RANGE: 0 to 7

Table continues...

Name	Description
Tagging	<p>Indicates the type of VLAN port. Possible values are:</p> <ul style="list-style-type: none"> • untagAll (access) • tagAll (trunk) • untagPvidOnly • tagPvidOnly <p>If the port is a trunk port, the port is often a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN.</p>

Configuring ports for VLAN membership using EDM

Use this procedure to configure one or more switch ports for VLAN membership.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. Click the **VLAN** tab.
5. To select a port to edit, click the port row.
6. In the port row, double-click the cell in the **DiscardUntaggedFrames** column.
7. Select a value from the list — **true** to discard untagged frames for the port, or **false** to accept untagged frames for the port.
8. In the port row, double-click the cell in the **FilterUnregisteredFrames** column.
9. Select a value from the list — **true** to discard unregistered frames for the port, or **false** to process unregistered frames normally for the port.
10. In the port row, double-click the cell in the **DefaultVlanId** column.
11. Type a value for the default VLAN ID.
12. In the port row, double-click the cell in the **PortPriority** column.
13. Select a value from the list.
14. In the port row, double-click the cell in the **Tagging** column.
15. Select a value from the list.
16. Repeat steps 5 through 15 to configure VLAN memberships for additional ports.
17. On the toolbar, click **Apply**.

Configure ports for VLAN membership field descriptions

The following table describes the fields to configure ports for VLAN membership

Name	Description
Index	Indicates the switch position in the stack and the port number. This is read-only value.
VlanIds	Indicates the VLAN IDs of which this port is a member. This is a read-only value.
DiscardUntaggedFrames	<p>Indicates how untagged frames received on this port are processed.</p> <ul style="list-style-type: none"> • true: untagged frames are discarded by the forwarding process • false: untagged frames are assigned to the VLAN specified by the VLAN ID. <p>This column applies to trunk ports only.</p>
FilterUnregisteredFrames	<p>Indicates how unregistered frames received on this port are processed:</p> <ul style="list-style-type: none"> • true: unregistered frames are discarded by the forwarding process • false: unregistered frames are assigned to the VLAN specified by the VLAN ID. <p>This column applies to access ports only.</p>
DefaultVlanId	Indicates the VLAN ID assigned to untagged and unregistered frames received on a port.
PortPriority	<p>Indicates the port priority for the switch to consider as it forwards received packets.</p> <p>RANGE: 0 to 7</p>
Tagging	<p>Indicates the type of VLAN port. Possible values are:</p> <ul style="list-style-type: none"> • untagAll (access) • tagAll (trunk) • untagPvidOnly • tagPvidOnly <p>If the port is a trunk port, the port is often a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN.</p>

Configuring an IPv6 interface using EDM

Use this procedure to configure an IPv6 interface

Procedure

1. In the navigation tree, double-click **VLAN**.
2. In the **VLAN** tree, click **VLAN**.
3. In the VLAN work area, click the **Basic** tab.
4. Click **IPv6**.
5. Click **Insert**.
6. In the **Identifier** box, type the identifier portion of the address or leave the field blank to use the default MAC-based identifier that is created automatically. This is the IPv6 link-local address.
7. In the **Descr** box, type a description for this IPv6 interface (255 characters maximum length).
8. In the **ReasmMaxSize(MTU)** box, type a value in the MTU field to set the maximum size of an IPv6 packet, in bytes. The range is 1280 to 9600 and the default is 1500.
9. Click the **AdminStatus** box to create and enable the IPv6 interface at the same time.
10. In the **ReachableTime** box, you can type the reachable time. The range is 0 to 3600000 milliseconds.
11. In the **RetransmitTime** box, you can type the retransmit time. The range is 0 to 3600000 milliseconds.
12. Click **Insert**.

Interfaces tab field descriptions

The following table describes the fields on the Interfaces tab.

Name	Description
IfIndex	Specifies the Ifindex of the VLAN.
Identifier	Indicates the IPv6 address interface identifier, which is a binary string of up to 8 octets in network byte order.
IdentifierLength	Specifies the length of the interface identifier in bits.
Descr	Specifies a text string containing information about the interface. The network management system also sets this string.

Table continues...

Name	Description
VlanId	Identifies the VLAN associated with the entry. This value corresponds to the lower 12 bits in the IEEE 802.1Q VLAN tag.
Type	Specifies Unicast, the only supported type.
ReasmMaxSize(MTU)	Specifies the MTU for this IPv6 interface. The range is from 1280 to 9600, and the default value is 1500.
PhysAddress	Specifies the media-dependent physical address. For Ethernet, this is a MAC address.
AdminStatus	Specifies whether the administration status of the interface is enabled (true) or disabled (false). The default is enabled (true).
OperStatus	Specifies whether the operation status of the interface is up or down.
ReachableTime	Specifies the time that a neighbor is considered reachable after receiving a reachability confirmation. Values range from 0 to 30000 milliseconds. This is an optional field.
RetransmitTime	Specifies the RetransmitTime, which is the time between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. Values range from 0 to 3600000 milliseconds. This is an optional field.
MulticastAdminStatus	Specifies the multicast status as either True or False.

MAC address table management using EDM

This section describes how to manage the MAC address table by clearing entries.

Important:

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

Related links

- [Configuring VLANs using Enterprise Device Manager](#) on page 129
- [Flushing the MAC address table using EDM](#) on page 152
- [Flushing the MAC address table for an interface using EDM](#) on page 152
- [Flushing the MAC address table for a VLAN using EDM](#) on page 153
- [Flushing the MAC address table for a trunk using EDM](#) on page 153
- [Flushing a single MAC address table entry using EDM](#) on page 154

Flushing the MAC address table using EDM

Use this procedure to flush the MAC address table to clear all addresses in the MAC address table.

Procedure

1. In the navigation tree, double-click **Edit** to open the Edit navigation tree.
2. Double-click **Bridge** to open the Bridge work area.
3. Select the **Mac Flush** tab.
4. To clear all MAC address table entries, select the **FlushMacAddrTableAll** check box.
5. On the toolbar, click **Apply**.

Variable definitions

Table 2: MAC Flush tab parameters

Variable	Value
FlushMacAddrTableAll	Flushes all MAC addresses from MAC address table.
FlushMacAddrTableByPortlist	Flushes the MAC addresses for the 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 address from the MAC address table.

Flushing the MAC address table for an interface using EDM

Use this procedure to flush the MAC address table for an interface to clear the MAC address table for specified interface ports.

Procedure

1. In the navigation tree, double-click **Edit**.
2. Double-click **Bridge** to open the Bridge work area.
3. Select the **Mac Flush** tab.
4. Click the **FlushMacAddrTableByPortList** elipsis (...).
5. Select interface ports for which to clear MAC address table entries.
6. Click **Ok**.
7. On the toolbar, click **Apply**.

Related links

[MAC address table management using EDM](#) on page 151

Flushing the MAC address table for a VLAN using EDM

Use this procedure to flush the MAC address table for a VLAN to clear all MAC addresses for a specific VLAN.

Procedure

1. In the navigation tree, double-click **Edit** to open the Edit navigation tree.
2. Double-click **Bridge** to open the Bridge work area.
3. Select the **Mac Flush** tab.
4. Type a VLAN ID for which to clear the MAC address table in the **FlushMacAddrTableByVlan** box.
5. On the toolbar, click **Apply**.

Related links

[MAC address table management using EDM](#) on page 151

[MAC Flush tab field descriptions](#) on page 153

MAC Flush tab field descriptions

The following table describes the fields on the MAC Flush tab.

Name	Description
FlushMacAddrTableByVlan	Specifies the VLAN ID. RANGE: 1 to 4094

Related links

[Flushing the MAC address table for a VLAN using EDM](#) on page 153

Flushing the MAC address table for a trunk using EDM

Use this procedure to flush the MAC address table for a trunk to clear all MAC addresses for members of a multi-link trunk.

Procedure

1. In the navigation tree, double-click **Edit** to open the Edit navigation tree.
2. Double-click **Bridge** to open the Bridge work area.
3. Select the **Mac Flush** tab.

4. Type a trunk number for which to clear the MAC address table in the **FlushMacAddrTableByTrunk** box.
5. On the toolbar, click **Apply**.

Related links

- [MAC address table management using EDM](#) on page 151
- [MAC Flush field descriptions](#) on page 154

MAC Flush field descriptions

The following table describes the fields on the MAC Flush tab.

Name	Description
FlushMacAddrTableByTrunk	Specifies the multi-link trunk. RANGE: 1 to 6

Related links

- [Flushing the MAC address table for a trunk using EDM](#) on page 153

Flushing a single MAC address table entry using EDM

Use this procedure to flush a single MAC address table entry to clear one MAC address from the MAC address table.

Procedure

1. In the navigation tree, double-click **Edit** to open the Edit navigation tree.
2. Double-click **Bridge** to open the Bridge work area.
3. Select the **Mac Flush** tab.
4. Type a MAC address in the **FlushMacAddrTableByAddress** box.
5. On the toolbar, click **Apply**.

Related links

- [MAC address table management using EDM](#) on page 151
- [MAC Flush field descriptions](#) on page 154

MAC Flush field descriptions

The following table describes the fields on the MAC Flush tab.

Name	Description
FlushMacAddrTableByAddress	Specifies a MAC address. DEFAULT: 00:00:00:00:00:00.

Related links

[Flushing a single MAC address table entry using EDM](#) on page 154

Link Aggregation Control Protocol

With Link Aggregation (LA), you can create and manage a trunk group. You can control and configure a trunk group automatically through the use of the Link Aggregation Control Protocol (LACP). Use the procedures in this section to view and configure Link Aggregation Groups (LAG) and LACP.

Displaying LAG information using EDM

Use this procedure to view Link Aggregation Group (LAG) configuration information.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **MLT/LACP**.
3. Select the **LACP** tab.

LACP field descriptions

The following table describes the fields on the LACP tab.

Name	Description
Index	Specifies the unique identifier allocated to this Aggregator by the local System. This attribute identifies an Aggregator instance among the subordinate managed objects of the containing object. This value is read-only.
MacAddress	Specifies the MAC address used by this bridge when it must be referred to in a unique fashion.
AggregateOrIndividual	Specifies the read-only Boolean value indicating whether the Aggregation Port is able to Aggregate ('TRUE') or is only able to operate as an Individual link ('FALSE').
ActorLagId	Specifies the combined information of ActorSystemPriority, ActorSystemID, and ActorOperKey in "ActorSystemPriority-ActorSystemID-ActorOperKey" format.

Table continues...

Name	Description
ActorSystemPriority	Specifies the 2-octet read-write value used to define the priority value associated with the Actor's System ID.
ActorSystemID	Specifies the 6-octet read-only MAC address value that defines the value of the System ID for the System that contains this Aggregation Port.
ActorOperKey	Specifies the current operational value of the Key for the Aggregation Port. This is a 16-bit read-only value.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation Port. This is a 16-bit read-write value.
PartnerLagId	Specifies the combined information of PartnerSystemPriority, PartnerSystemID, and PartnerOperKey in "PartnerSystemPriority-PartnerSystemID-PartnerOperKey" format.
PartnerSystemPriority	Specifies the 2-octet read-only value that indicates the priority value associated with the Partner's System ID.
PartnerSystemID	Specifies the 6-octet read-only MAC address value consisting of the unique identifier for the current protocol Partner of this Aggregator. A value of zero indicates that there is no known Partner. If the aggregation is manually configured, this System ID value will be a value assigned by the local System.
PartnerOperKey	Specifies the current operational value of the Key for the Aggregator's current protocol Partner. This is a 16-bit read-only value.
CollectorMaxDelay	Specifies the value of this 16-bit read-write attribute defines the maximum delay, in tens of microseconds, that can be imposed by the Frame Collector between receiving a frame from an Aggregator Parser, and either delivering the frame to its MAC Client or discarding the frame.

Link Aggregation Group configuration using EDM

Use the procedures in this section to display or modify LAG member configuration.

Displaying LACP for LAG members using EDM

Use this procedure to display the existing LACP configuration for LAG members.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **LACP Ports** tab.

LACP Ports field descriptions

The following table describes the fields on the LACP Ports tab.

Name	Description
Index	Indicates the unique identifier allocated to an Aggregator by the local system.
AdminEnabled	Indicates the current administrative setting for the port. Values include: <ul style="list-style-type: none"> • true: enables the port to participate in LACP. • false: disables the port from participating in LACP.
OperEnabled	Specifies the current operational state for the port: <ul style="list-style-type: none"> • true: the port is participating in LACP. • false: the port is not participating in LACP.
ActorAdminState	Specifies the Actor administrative state for the port. Values include: <ul style="list-style-type: none"> • lacpActive • aggregation • shortTimeout
ActorOperState	Specifies the current operational values of Actor state transmitted by the Actor in LACPDUs.
AggregateOrIndividual	Specifies whether the port represents an Aggregate or an Individual link.
ActorPortPriority	Specifies the priority value assigned to this Aggregation port. RANGE: 0 to 65535.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation Port. RANGE: 1 to 4095.
ActorOperKey	Specifies the current operational value of the Key for the Aggregation Port.
SelectedAggID	Specifies the identifier value of the Aggregator that this Aggregation Port has currently selected. Zero indicates that the Aggregation Port has not selected an Aggregator, either because it is in the process of

Table continues...

Name	Description
	detaching from an Aggregator or because no suitable Aggregator exists for it to select.
AttachedAggID	Specifies the identifier value of the Aggregator that this Aggregation Port is currently attached to. Zero indicates that the Aggregation Port is not currently attached to an Aggregator. This value is read-only..
ActorPort	Specifies the port number locally assigned to the Aggregation Port. The port number is communicated in LACPDU as the Actor_Port. This value is read-only
MltId	Specifies the MLT that the port is assigned to. If the port is not assigned to an MLT, the MltId value is 0.
PartnerOperPort	Specifies the operational port number assigned by the port protocol partner.
OperStatus	Specifies the operational status of the interface. Values include: <ul style="list-style-type: none"> • up: operational • down: not operational

Configuring LACP for specific LAG members using EDM

Use this procedure to configure LACP for LAG members.

Before you begin

- Ensure members you want to configure are not ADAC Call Server or Uplink ports.
- Disable ADAC for members you want configure.

Important:

To configure the port LACP mode to active, you must set the AdminEnabled value to **true** and the ActorAdminState value to **lACPActive**.

Important:

To configure the port LACP mode to passive, you must set the AdminEnabled value to **false** and clear the **lACPActive**, **aggregation**, and **shortTimeout** check boxes in ActorAdminState.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **LACP Ports** tab.
4. To select a port to configure, click the port **Index**.
5. In the port row, double-click the cell in the **AdminEnabled** column.
6. Set a value from the list — **true** to enable LACP for the port, or **false** to disable LACP for the port.

7. In the port row, double-click the cell in the **ActorAdminState** column.
8. Select an individual or combination of check boxes.
9. Click **OK**.
10. In the port row, double-click the cell in the **ActorPortPriority** column.
11. In the dialog box, edit the value as required.
12. In the port row, double-click the cell in the **ActorAdminKey** column.
13. In the dialog box, edit the value as required.
14. On the toolbar, click **Apply**.

LACP Ports field descriptions

The following table describes the fields on the LACP Ports tab.


Name	Description
Index	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
AdminEnabled	Indicates the current administrative setting for the port. Values include: <ul style="list-style-type: none"> • true: enables the port to participate in LACP. • false: disables the port from participating in LACP. <p> Important: You cannot enable ports to participate in LACP if they are members of an enabled MLT.</p>
OperEnabled	Specifies the current operational state for the port: <ul style="list-style-type: none"> • true: the port is participating in LACP. • false: the port is not participating in LACP.
ActorAdminState	Specifies the Actor administrative state. Values include: <ul style="list-style-type: none"> • lacpActive • aggregation • shortTimeout
ActorOperState	Indicates the current Actor operational state. This is a read-only cell.
AggregateOrIndividual	Specifies whether the port represents an Aggregate or an Individual link. This is a read-only cell.
ActorPortPriority	Specifies the priority value assigned to this Aggregation port.

Table continues...

Name	Description
	RANGE: 0 to 65535.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation Port. RANGE: 1 to 4095.
ActorOperKey	Specifies the current operational value of the Key for the Aggregation Port. This is a read-only cell.
SelectedAggID	Specifies the identifier value of the Aggregator that this Aggregation Port has currently selected. Zero indicates that the Aggregation Port has not selected an Aggregator, either because it is in the process of detaching from an Aggregator or because no suitable Aggregator exists for it to select. This is a read-only cell.
AttachedAggID	Specifies the identifier value of the Aggregator that this Aggregation Port is currently attached to. Zero indicates that the Aggregation Port is not currently attached to an Aggregator. This value is read-only.
ActorPort	Specifies the port number locally assigned to the Aggregation Port. The port number is communicated in LACPDU as the Actor_Port. This value is read-only.
MtId	Specifies the MLT that the port is assigned to. If the port is not assigned to an MLT, the MtId value is 0. This is a read-only cell.
PartnerOperPort	Specifies the operational port number assigned by the port's protocol partner. This is a read-only cell.
OperStatus	Specifies the operational status of the interface. Values include: <ul style="list-style-type: none"> • up: operational • down: not operational This is a read-only cell.

LACP configuration for ports using EDM

You can use the information in this section to display or modify the LACP configuration for switch ports.

Displaying the LACP configuration for ports using EDM

Use this procedure to view the existing LACP configuration for switch ports.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.

3. In the Chassis tree, double-click **Ports**
4. Click the **VLACP** tab.

LACP field descriptions

The following table describes the fields on the LACP tab.


Name	Description
Index	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
AdminEnabled	Indicates the current administrative setting for the port. Values include: <ul style="list-style-type: none"> • true: enables the port to participate in LACP. • false: disables the port from participating in LACP. <p> Important: You cannot enable ports to participate in LACP if they are members of an enabled MLT.</p>
OperEnabled	Specifies the current operational state for the port: <ul style="list-style-type: none"> • true: the port is participating in LACP. • false: the port is not participating in LACP. This is a read-only cell.
ActorAdminState	Specifies the Actor administrative state. Values include: <ul style="list-style-type: none"> • lacpActive • aggregation • shortTimeout
ActorOperState	Indicates the current Actor operational state. This is a read-only cell.
AggregateOrIndividual	Specifies whether the port represents an Aggregate or an Individual link. This is a read-only cell.
ActorPortPriority	Specifies the priority value assigned to this Aggregation port. RANGE: 0 to 65535.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation Port. RANGE: 1 to 4095.
ActorOperKey	Specifies the current operational value of the Key for the Aggregation Port. This is a read-only cell.

Table continues...

Name	Description
SelectedAggID	Specifies the identifier value of the Aggregator that this Aggregation Port has currently selected. Zero indicates that the Aggregation Port has not selected an Aggregator, either because it is in the process of detaching from an Aggregator or because no suitable Aggregator exists for it to select. This is a read-only cell.
AttachedAggID	Specifies the identifier value of the Aggregator that this Aggregation Port is currently attached to. Zero indicates that the Aggregation Port is not currently attached to an Aggregator. This value is read-only.
ActorPort	Specifies the port number locally assigned to the Aggregation Port. The port number is communicated in LACPDU as the Actor_Port. This value is read-only.
Mltid	Specifies the MLT that the port is assigned to. If the port is not assigned to an MLT, the Mltid value is 0. This is a read-only cell.
PartnerOperPort	Specifies the operational port number assigned by the port's protocol partner. This is a read-only cell.
OperStatus	Specifies the operational status of the interface. Values include: <ul style="list-style-type: none"> • up: operational • down: not operational This is a read-only cell.

Configuring LACP for specific ports using EDM

Use this procedure to modify the LACP configuration for one or more switch ports.

Before you begin

- Ensure ports you want to configure are not ADAC Call Server or Uplink ports.
- Disable ADAC for ports you want configure.

Important:

To configure the port LACP mode to active, you must set the AdminEnabled value to **true** and the ActorAdminState value to **lACPActive**.

Important:

To configure the port LACP mode to passive, you must set the AdminEnabled value to **false** and clear the **lACPActive**, **aggregation**, and **shortTimeout** check boxes in ActorAdminState.

Procedure

1. In the navigation tree, double-click **Edit**.

2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. Click the **LACP** tab.
5. To select a port to configure, click the port **Index**.
6. In the port row, double-click the cell in the **AdminEnabled** column.
7. Set a value from the list — **true** to enable LACP for the port, or **false** to disable LACP for the port.
8. In the port row, double-click the cell in the **ActorAdminState** column.
9. Select an individual or combination of check boxes.
10. Click **OK**.
11. In the port row, double-click the cell in the **ActorPortPriority** column.
12. In the dialog box, edit the value as required.
13. In the port row, double-click the cell in the **ActorAdminKey** column.
14. In the dialog box, edit the value as required.
15. Repeat steps 5 through 14 to configure LACP for additional ports as required.
16. On the toolbar, click **Apply**.

LACP field descriptions

The following table describes the fields on the LACP tab.


Name	Description
Index	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
ActorSystemPriority	Specifies the priority value associated with the Actor System ID. RANGE: 0 to 65535.
AdminEnabled	Indicates the current administrative setting for the port. Values include: <ul style="list-style-type: none"> • true: enables the port to participate in LACP. • false: disables the port from participating in LACP. <p> Important: You cannot enable ports to participate in LACP if they are members of an enabled MLT.</p>
OperEnabled	Specifies the current operational state for the port: <ul style="list-style-type: none"> • true: the port is participating in LACP.

Table continues...

Name	Description
	<ul style="list-style-type: none"> • false: the port is not participating in LACP. This is a read-only cell.
ActorAdminState	Specifies the Actor administrative state. Values include: <ul style="list-style-type: none"> • lacpActive • aggregation • shortTimeout
ActorOperState	Indicates the current Actor operational state. This is a read-only cell.
AggregateOrIndividual	Specifies whether the port represents an Aggregate or an Individual link. This is a read-only cell.
ActorPortPriority	Specifies the priority value assigned to this Aggregation port. RANGE: 0 to 65535.
ActorAdminKey	Specifies the current administrative value of the Key for the Aggregation port. RANGE: 1 to 4095.
ActorOperKey	Specifies the current operational value of the Key for the Aggregation Port. This is a read-only cell.
SelectedAggID	Specifies the identifier value of the Aggregator that this Aggregation Port has currently selected. Zero indicates that the Aggregation Port has not selected an Aggregator, either because it is in the process of detaching from an Aggregator or because no suitable Aggregator exists for it to select. This is a read-only cell.
AttachedAggID	Specifies the identifier value of the Aggregator that this Aggregation Port is currently attached to. Zero indicates that the Aggregation Port is not currently attached to an Aggregator. This value is read-only.
ActorPort	Specifies the port number locally assigned to the Aggregation Port. The port number is communicated in LACPDU as the Actor_Port. This value is read-only.
MtId	Specifies the MLT that the port is assigned to. If the port is not assigned to an MLT, the MtId value is 0. This is a read-only cell.
PartnerOperPort	Specifies the operational port number assigned by the port's protocol partner. This is a read-only cell.

Table continues...

Name	Description
OperStatus	Specifies the operational status of the interface. Values include: <ul style="list-style-type: none"> • up: operational • down: not operational This is a read-only cell.

Mapping the LACP key mapping

Use this procedure to map the LACP key mapping.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **LACP key mapping** tab.

LACP key mapping field descriptions

The following table describes the fields on the LACP key mapping tab.

Name	Description
LacpKeyValue	Specifies the value of the LACP administration key.
MltId	Specifies the ID of the MLT.

Graphing port LACP statistics using EDM

Use this procedure to display and graph LACP statistics for switch ports.

Procedure

1. From the Device Physical View, click a port.
2. In the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **LACP** tab.
5. Select a **Poll Interval** from the list.
6. Select a value from the list.
7. To select LACP statistics to graph, click a static type row under one of the displayed columns.
8. Click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

LACP field descriptions

The following table describes the fields on the LACP tab.

Name	Description
LACPDUsRx	Specifies the number of valid LACPDUs received on this Aggregation Port. This value is read-only.
MarkerPDUsRx	Specifies the number of valid Marker PDUs received on this Aggregation Ports. This value is read-only.
MarkerResponse PDUsRx	Specifies the number of valid Marker Response PDUs received on this Aggregation Port. This value is read-only.
UnknownRx	Specifies the number of frames that <ul style="list-style-type: none"> • Can carry the Slow Protocols Ethernet Type value (43B.4), but contain an unknown PDU. • Are addressed to the Slow Protocols group MAC Address (43B.3), but do not carry the Slow Protocols Ethernet Type. This value is read-only.
IllegalRx	Specifies the number of frames received that carry the Slow Protocols Ethernet Type value (43B.4), but contain a badly formed PDU or an illegal value of Protocol Subtype (43B.4). This value is read-only.
LACPDUsTx	Specifies the number of LACPDUs that are transmitted on this Aggregation Port. This value is read-only.
MarkerPDUsTx	Specifies the number of Marker PDUs transmitted on this Aggregation Port. This value is read-only.
MarkerResponse PDUsTx	Specifies the number of Marker Response PDUs that are transmitted on this Aggregation Port. This value is ready only.

Configuring Static LACP Key to Trunk ID binding using EDM

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

 **Note:**

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

Binding an LACP key to a specific trunk ID using EDM

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

Procedure

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

2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **LACP key mapping** tab.
4. Click **Insert**.
5. In the **LacpKeyValue** dialog box, type a value.
6. In the **MltId** dialog box, type a value.
7. Click **Insert**.
8. Click **Apply**.

Deleting an LACP key binding to a trunk ID using EDM

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

Procedure

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **LACP key mapping** tab.
4. To select an LACP key binding to a trunk ID, click the LACPKeyValue ID.
5. Click **Delete**.
6. Click **Yes** to confirm.

The selected LACP Key binding is deleted from the LACP key mapping tab.

Viewing LACP key bindings to trunk IDs using EDM

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

Procedure

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **LACP key mapping** tab.

Configuring MLT and VLACP global settings using EDM

Use the information in this section to:

- enable or disable VLACP globally
- set the VLACP Multicast MAC Address
- enable or disable MLT whole trunk mode globally

Configuring MLT whole trunk using EDM

Use this procedure to configure the MLT whole trunk mode of a switch or stack.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. On the work area, click the **Global** tab.
4. Select **MltDisablePortsOnShutdown** to enable or disable the MLT whole trunk feature.
5. On the toolbar, click **Apply**.

Enabling or disabling global VLACP using EDM

Use this procedure to enable or disable VLACP for the switch.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **Global** tab.
4. Do one of the following:
 - To enable VLACP, select the **VlACPEnable** check box.
 - To disable VLACP, deselect the **VlACPEnable** check box.
5. Type a value in the **VlACPMulticastMACAddress** dialog box.
6. On the toolbar, click **Apply**.

Global field descriptions

The following table describes the fields on the Global tab.

Name	Description
VlACPEnable	Enables or disables VLACP on the switch.
VlACPMulticastMACAddress	Identifies a multicast MAC address used exclusively for VLACPDU. DEFAULT: 01:80:c2:00:11:00.

VLACP configuration for ports using EDM

Use the procedures in this section to view and configure VLACP at the port level.

Displaying the VLACP configuration for ports using EDM

Use this procedure to view the VLACP tab for ports.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. Click the **VLACP** tab.

VLACP field descriptions

The following table describes the fields on the VLACP tab.



Name	Description
rePortIndex	Specifies the switch and port number.
AdminEnable	Enables (True) or disables (False) VLACP on a port. DEFAULT: Disabled (False)
OperEnable	Specifies whether the VLACP is operationally enabled or disabled. This is a read-only field.
FastPeriodicTimer	Specifies the number of milliseconds between periodic transmissions using short timeouts. RANGE: 400 to 20000 milliseconds DEFAULT: 500
SlowPeriodicTimer	Specifies the number of milliseconds between periodic transmissions using long timeouts. RANGE: 10000 to 30000 milliseconds DEFAULT: 30000
Timeout	Specifies whether the timeout control value is a short or long timeout.
TimeoutScale	Specifies a timeout scale for the port, where timeout = (periodic time) * (timeout scale)  Note: With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port

Table continues...

Name	Description
	<p>receiving the same VLACPDU. However, if the timeout-scale is set to 1, the port timeout value does not take into account the normal travel time of the VLACPDU. The port expects to receive a VLACPDU at the same moment the partner port sends it. Therefore, the delayed VLACPDU results in the link being blocked, and then enabled again when the packet arrives. To prevent this scenario from happening, set the timeout-scale to a value larger than 1.</p> <p>RANGE: 1 to 10</p> <p>DEFAULT: 3</p>
EtherType	<p>Specifies VLACP protocol identification. The ID value is a 4–digit Hex number, with a default of 8103.</p>
EtherMacAddress	<p>Specifies the MAC address of the switch or stack to which this port is sending VLACPDUs. It cannot be configured as</p> <p> Note:</p> <p>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 EtherMACAddressss 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 EtherMACAddressss. 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 EtherMACAddressss field with the desired destination MAC address. With EtherMACAddressss configured, the intermediate switches do not misinterpret the VLACP packets.</p> <p>DEFAULT: 00:00:00:00:00:00.</p>
PortState	<p>Specifies whether the VLACP port state is up or down. This is a read-only field.</p>

Configuring VLACP for specific ports using EDM

Use this procedure to configure VLACP for a single port or multiple ports.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. Click the **VLACP** tab.
5. To select a port to edit, click the port **rePortIndex** row.
6. In the port row, double-click the cell in the **AdminEnabled** column.
7. Set a value from the list — **true** to enable VLACP for the port, or **false** to disable VLACP for the port.
8. In the port row, double-click the cell in the **FastPeriodicTimer** column.
9. Type a value in the dialog box.
10. In the port row, double-click the cell in the **SlowPeriodicTimer** column.
11. Type a value in the dialog box.
12. In the port row, double-click the cell in the **Timeout** column.
13. Type a value in the dialog box.
14. In the port row, double-click the cell in the **TimeoutScale** column.
15. Type a value in the dialog box.
16. In the port row, double-click the cell in the **EtherType** column.
17. Type a value in the dialog box.
18. In the port row, double-click the cell in the **EtherMacAddress** column.
19. Type a value in the dialog box.
20. Repeat steps 5 through 19 to configure VLACP for additional ports as required.
21. On the toolbar, click **Apply**.

VLACP field descriptions



The following table describes the fields on the VLACP tab.

Name	Description
rePortIndex	Specifies the switch and port number.

Table continues...

Name	Description
AdminEnable	Indicates whether VLACP is enabled (True) or disabled (False) on ports. DEFAULT: Disabled (False)
OperEnable	Specifies whether the VLACP is operationally enabled or disabled. This is a read-only field. ! Important: VLACP is only operational when OperEnable is true and PortState is up.
FastPeriodicTimer	Specifies the number of milliseconds between periodic transmissions using short timeouts. RANGE: 400 to 20000 milliseconds DEFAULT: 500
SlowPeriodicTimer	Specifies the number of milliseconds between periodic transmissions using long timeouts. RANGE: 10000 to 30000 milliseconds DEFAULT: 30000
Timeout	Specifies whether the timeout control value is a short or long timeout.
TimeoutScale	Specifies a scale value used to calculate timeout from periodic time. * Note: With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. However, if the timeout-scale is set to 1, the port timeout value does not take into account the normal travel time of the VLACPDU. The port expects to receive a VLACPDU at the same moment the partner port sends it. Therefore, the delayed VLACPDU results in the link being blocked, and then enabled again when the packet arrives. To prevent this scenario from happening, set the timeout-scale to a value larger than 1. RANGE: 1 to 10 DEFAULT: 3
EtherType	Specifies VLACP protocol identification. The value can be entered as a numerical value ranging from 33025–33279 or a hexadecimal equivalent (8101–81ff). Use the prefix 0x to type a hexadecimal value

Table continues...

Name	Description
	<p>in the dialog box. Only hexadecimal values display in the EtherType column of the VLACP work area.</p> <p>DEFAULT: 8103</p>
EtherMacAddress	<p>Specifies the MAC address of the switch or stack to which this port is sending VLACPDUs. It cannot be configured as</p> <p> Note:</p> <p>VLACP uses only the multicast MAC address configured when VLACP is enabled globally. This is the Layer 2 destination address used for the VLACPDUs. If you do not type a value for the EtherMACAddress, the first VLACP-enabled switch or stack that receives the PDUs from a sending port becomes the intended recipient and processes the PDUs. If you want an intermediate switch to drop VLACP packets, configure the EtherMACAddress field with the desired destination MAC address. With EtherMACAddress configured, the intermediate switches do not misinterpret the VLACP packets.</p> <p>DEFAULT: 00:00:00:00:00:00.</p>
PortState	<p>Specifies whether the VLACP port state is up or down. This is a read-only field.</p> <p> Important:</p> <p>VLACP is only operational when OperEnable is true and PortState is up.</p>

Chapter 14: Configuring Spanning Tree Groups using Enterprise Device Manager

This chapter describes using Enterprise Device Manager (EDM) to manage Spanning Tree Groups (STG). It also discusses Rapid Spanning Tree Protocol (RSTP), and the Multiple Spanning Tree Protocol (MSTP).

Changing the Spanning Tree mode using EDM

Procedure

1. In the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **Spanning Tree**.
3. In the Spanning Tree navigation tree, double-click **Globals**.
4. In the **SpanningTreePortMode** section, click a radio button.
5. On the toolbar, click **Apply**.

A warning message appears reminding you that you must reset the switch for the change to take effect.

6. Click **Yes**.
7. Reset the switch.

For information about how to reset the switch, see [Resetting the switch using EDM](#) on page 175.

8. Rediscover the switch.

For information about how to rediscover the switch, see [Rediscovering the switch using EDM](#) on page 175.

Resetting the switch using EDM

Use this procedure to reset the switch.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Chassis**.
4. In the work area, click the **System** tab.
5. In the ReBoot section, click the **reboot** radio button.
6. On the toolbar, click **Apply**.

 **Note:**

The rebooting process can take several minutes.

Rediscovering the switch using EDM

Use this procedure to rediscover the switch after performing the switch reset procedure.

Procedure

1. In the navigation tree, double-click **Device**.
2. Double-click **Rediscover Device**.

 **Note:**

The rediscover process can take several minutes.

Configuring STP BPDU Filtering using EDM

Use this procedure to configure STP BPDU Filtering.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. On the work area, click the **STP BPDU-Filtering** tab.

5. In the table, double-click a cell under the column heading for the parameter you want to change.
6. Select a parameter or value from the list.
7. Repeat the previous two steps until you have amended all of the parameters you want to change.
8. On the toolbar, click **Apply**.

STP BPDU-Filtering field descriptions

The following table describes the fields on the STP BPDU-Filtering tab.

Name	Description
rcPortIndex	Indicates the switch and port number.
AdminEnabled	Enables and disables BPDU filtering on the port.
OperEnabled	Indicates the current operational status of BPDU filtering on the port: <ul style="list-style-type: none"> • true: enabled • false: disabled
Timeout	When BPDU filtering is enabled, this indicates the time (in 1/100 seconds) during which the port remains disabled after it receives a BPDU. The port time is disabled if this value is set to 0. DEFAULT: 12000 (120 seconds)
TimeCount	Displays the time remaining for the port to stay in the disabled state after receiving a BPDU.

Spanning Tree Group configuration using EDM

Use the information in this section to configure and manage a Spanning Tree Group (STG).

Configuring STG globally using EDM

Use this procedure to configure Spanning Tree Group (STG) globally to select the STG configuration for the switch.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.

3. Double-click **STG** to open the STG work area.
4. Select the **Globals** tab.
5. Select a **SpanningTreePathCostCalculationMode** radio button.
6. Select a **SpanningTreePortMode** radio button.
7. Select or clear the **port802dot1dLearning** check box as required.
8. On the toolbar, click **Apply**.

Globals field descriptions

The following table describes the fields on the Globals tab.

Name	Description
SpanningTreePathCostCalculationMode	Indicates the current spanning-tree path cost calculation mode. Values include: <ul style="list-style-type: none"> • ieee802dot1dCompatible • ieee802dot1tCompatible The value ieee802dot1dCompatible is valid only after the switch is running in STPG mode.
SpanningTreePortMode	Specifies the STP port mode. Values include: <ul style="list-style-type: none"> • normal • auto
SpanningTreeAdminCompatibility	Specifies the STP compatibility mode for various features. If port802dot1dLearning is selected, the port goes to a Disabled state when the port operational status fails. If port802dot1dLearning is not selected, the port remains in the Forwarding state when the port operational status fails.
SpanningTreeOperCompatibility	Indicates the STP compatibility mode for various features if applicable.

Displaying STG configuration general information using EDM

Use this procedure to view general information for the Spanning Tree Group.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **STG** to open the STG work area.
4. Select the **Configuration** tab.

Configuration field descriptions

The following table describes the fields on the Configuration tab.




Name	Description
Id	Identifies an STG in the device.
BridgeAddress	Identifies the MAC address used by a bridge. Extreme Networks recommends that the number has to be the smallest MAC address of all ports belonging to the bridge. However, it is only required to be unique. When concatenated with Priority, a unique bridge identifier is formed that is used in the Spanning Tree Protocol.
NumPorts	Identifies the number of ports controlled by this bridging entity.
ProtocolSpecification	Specifies the version of the spanning tree protocol being run. Values include: <ul style="list-style-type: none"> • decLb100: Indicates the DEC LANbridge 100 Spanning Tree Protocol. • ieee8021d: IEEE802.1d implementations will return this entity. When future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version, a new value will be defined.
Priority	Specifies the value of the writable portion of the bridge ID. That is, the first two octets of the (8-octet long) bridge ID. The last six octets of the bridge ID are given by the value of BridgeAddress.
BridgeMaxAge	Specifies the value, in units of hundredths of a second, that all bridges use for the maximum age of a bridge when it is acting as the root. <p> Important:</p> 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error can be returned if the value set is not a whole number.
BridgeHelloTime	Specifies the value, in units of hundredths of a second, that all bridges use for HelloTime when a bridge is acting as the root. <p> Important:</p> The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error

Table continues...

Name	Description
	can be returned if the value set is not a whole number.
BridgeForwardDelay	<p>Specifies the value, in units of hundredths of a second, that all bridges use for ForwardDelay when this bridge is acting as the root.</p> <p> Important:</p> <p>802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error can be returned if the value set is not a whole number.</p>

Displaying STG status information using EDM

Use this procedure to view STG status information.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **STG** to open the STG work area.
4. Select the **Status** tab.

Status field descriptions

The following table describes the fields on the Status tab.

Name	Description
Id	Identifies an STG in the device.
BridgeAddress	Identifies the MAC address used by a bridge. Extreme Networks recommends that the number has to be the smallest MAC address of all ports belonging to the bridge. However, it is only required to be unique. When concatenated with Priority, a unique bridge identifier is formed that is used in the Spanning Tree Protocol.
NumPorts	Identifies the number of ports controlled by this bridging entity.

Table continues...

Name	Description
ProtocolSpecification	<p>Specifies the version of the spanning tree protocol being run. Values include:</p> <ul style="list-style-type: none"> • decLb100: Indicates the DEC LANbridge 100 Spanning Tree Protocol. • ieee8021d: IEEE802.1d implementations will return this entity. When future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version, a new value will be defined.
TimeSinceTopologyChange	<p>Specifies the time (in hundredths of seconds) since the last topology change was detected by the bridge entity.</p>
TopChanges	<p>Specifies the number of topology changes detected by the bridge since the management entity was last reset or initialized.</p>
DesignatedRoot	<p>Specifies the bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol. The value is used as the root identifier parameter in all configuration bridge PDUs originated by this node.</p>
RootCost	<p>Indicates the cost of the path to the root as seen from the bridge.</p>
RootPort	<p>Identifies the port that has the lowest cost path from the bridge to the root bridge.</p>
MaxAge	<p>Specifies the maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in units of hundredths of a second. This is the actual value that this bridge is currently using.</p>
HelloTime	<p>Specifies the amount of time between the transmission of configuration bridge PDUs by this node on any port when it is the root of the spanning tree (in hundredths of a second). This is the actual value that this bridge is currently using.</p>
HoldTime	<p>Specifies the value of the interval length during which no more than two configuration bridge PDUs shall be transmitted by this node (in hundredths of a second).</p>
ForwardDelay	<p>Specifies the time value (in hundredths of a second) that controls how fast a port changes its spanning state when moving towards the forwarding state.</p> <p>Value determines how long the port stays in each of the listening and learning states, which precede the</p>

Table continues...

Name	Description
	<p>forwarding state. This is also used when a topology change has been detected and is underway, to age all dynamic entries in the forwarding database.</p> <p>! Important:</p> <p>This value is the one that this bridge is currently using, in contrast to BridgeForwardDelay which is the value that this bridge and all other would start using if/when this bridge were to become the root.</p>

Displaying STG port information using EDM

Use this procedure to view port information for the STG.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **STG** to open the STG work area.
4. Select the **Ports** tab.

Ports field descriptions

The following table describes the fields on the Ports tab.

Name	Description
Port	Indicates the switch position in a stack and port number. For a standalone switch, the default value of 1 is used for the switch position.
StgId	Specifies the STG identifier assigned to this port.
Priority	Indicates the value of the priority field contained in the first octet of the port ID. The other octet is given by the value of the "rcStgPort."
State	Specifies the current state of the port as defined by application of the Spanning Tree Protocol. These are the instructions the port takes on a frame when it is received. If the bridge detects a port is malfunctioning, it will list it as "broken(6)." For ports that are disabled, the value is "disabled(1)."
EnableStp	Enables (True) or disables (False) the spanning tree of the port.

Table continues...

Name	Description
FastStart	When enabled (True), the port moves to forwarding or blocking state in 4 seconds.
AdminPathCost	Specifies the administrative value of PathCost.
PathCost	Specifies the contribution of the port to the pathcost of paths towards the spanning tree root, including the current port. 802.1D-1990 specifications recommends that the default of this parameter be in inverse proportion to the speed of the attached LAN.
DesignatedRoot	Specifies the unique "Bridge Identifier." This is recorded as Root in the configuration bridge PDUs transmitted by the Designated Bridge for the segment to that the port is attached.
DesignatedCost	Specifies the path cost of the Designated Port of the segment connected to the port. The value is compared to the Root Path Cost field in received bridge PDUs.
DesignatedBridge	Identifies the Bridge identifier that this port considers to be the Designated Bridge for this port's segment.
DesignatedPort	Identifies the Port identifier of the port on the designated Bridge for this port's segment.
ForwardTransitions	Defines the number of times this port has transitioned from the learning state to the forwarding state.

Configuring STG for a single port using EDM

Use this procedure to view the status and modify the configuration of a port's spanning tree parameters.

Before you begin

The switch must be operating in STG mode to access the **STG** tab.

Procedure

1. From the Device Physical View, right click a port.
2. Double-click **Edit**.
3. In the Edit tree, double-click **Chassis**.
4. In the Chassis tree, click **Ports**.
5. To select an STG to edit, click the STG ID.
6. In the STG row, double-click the cell in the **Priority** row.
7. Type a priority value.

8. In the STG row, double-click the cell in the **EnableStp** column.
9. Select a value from the list — **true** to enable STP for the STG, or **false** to disable STP for the STG.
10. In the STG row, double-click the cell in the **FastStart** column.
11. Select a value from the list — **true** to enable fast start for the STG, or **false** to disable fast start for the STG.
12. In the STG row, double-click the cell in the **AdminPathCost** column.
13. Type an administrative path cost value.
14. In the STG row, double-click the cell in the **PathCost** column.
15. Type a path cost value.
16. On the toolbar, click **Apply**.

STG field descriptions

The following table describes the fields on the STG tab.

Name	Description
StgId	Indicates the STG identifier assigned to this port. This is a read-only value.
Priority	Specifies the value of the priority contained in the first octet of the port ID. The other octet is given by the value of the "rcStgPort."
State	Indicates the current port state as defined by application of the Spanning Tree Protocol. This state controls the action a port takes after it receives a frame. If the bridge detects a port that is malfunctioning, it places that port into the broken state. For ports that are disabled (see EnableStp), this object has a value of disabled. This is a read-only value.
EnableStp	Enables (true) or disables (false) STP for the port.
FastStart	Enables (true) or disables (false) fast start for the port.
AdminPathCost	Specifies the administrative value of PathCost.
PathCost	Specifies the contribution of this port to the cost of paths toward the spanning tree root, which include this port. The IEEE802.1D-1990 standard recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN.
DesignatedRoot	Specifies the unique Bridge Identifier of the bridge recorded as the Root in the Configuration BPDUs

Table continues...

Name	Description
	transmitted by the Designated Bridge for the segment to which the port is attached. This is a read-only value.
DesignatedCost	Specifies the path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs. This is a read-only value.
DesignatedBridge	Specifies the Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port's segment. This is a read-only value.
DesignatedPort	Specifies the Port Identifier of the port on the Designated Bridge for this port's segment. This is a read-only value.
ForwardTransitions	Specifies the number of times this port has transitioned from the Learning state to the Forwarding state. This is a read-only value.

Rapid Spanning Tree Protocol

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

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

Rapid Spanning Tree Protocol

The Rapid Spanning Tree Protocol (RSTP or IEEE 802.1w) reduces the recovery time after a network break down. It also maintains a backward compatibility with the IEEE 802.1d which was the Spanning Tree implementation prior to RSTP. In certain configurations the recovery time of RSTP can be reduced to less than 1 second.

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

! Important:

You can access the RSTP menu command only after the switch is operating in the RSTP mode.

Displaying RSTP general information using EDM

Use this procedure to view general information about Rapid Spanning Tree Protocol (RSTP) when RSTP is in active mode.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **RSTP**.

RSTP field descriptions

The following table describes the fields on the RSTP tab.

Name	Description
PathCostDefault	Sets the version of the Spanning Tree default Path Costs that the Bridge uses: <ul style="list-style-type: none"> • The value of 16-bit uses the 16-bit default Path Costs from IEEE Std. 802.1D-1998. • A value of 32-bit uses the 32-bit default Path Costs from IEEE Std. 802.1t.
TxHoldCount	Specifies the value used by the Port Transmit state machine to limit the maximum transmission rate. RANGE: 1 to 10
Version	Specifies the version of the Spanning Tree Protocol the bridge is currently running: <ul style="list-style-type: none"> • 'stpCompatible' indicates that the bridge uses the Spanning Tree Protocol specified in IEEE 802.1D. • 'rstp' indicates that the bridge uses Rapid Spanning Tree Protocol specified in IEEE 802.1w.
Priority	Specifies the value of the writable portion of the Bridge Identifier comprising of the first two octets. The values that are set for Priority must be in steps of 4096.
BridgeMaxAge	Specifies the value that all bridges use for MaxAge when this bridge is acting as the root. The granularity of this timer is specified to be 1 second. An agent

Table continues...

Name	Description
	can return a badValue error if a set is attempted to a value which is not a whole number of seconds.
BridgeHelloTime	Specifies the value that all bridges use for HelloTime when this bridge is acting as the root. The granularity of this timer is specified by 802.1D-1990 to be 1 second. An agent can return a badValue error if a set is attempted to a value which is not a whole number of seconds. Reference IEEE 802.1D-1990: Section 4.5.3.9.
BridgeForwardDelay	Specifies the value that all bridges use for ForwardDelay when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of rcStgBridgeMaxAge. The granularity of this timer is specified by 802.1D-1990 to be 1 second. An agent can return a badValue error if a set is attempted to a value which is not a whole number of seconds.
DesignatedRoot	Specifies the unique identifier of the Bridge recorded as the Root in the Configuration BPDUs that are transmitted by the Designated Bridge for the segment to which the port is attached. Reference IEEE 802.1D-1990: Section 4.5.5.4.
RootCost	Specifies the cost of the path to the root as seen from this bridge.
RootPort	Specifies the port number of the port which offers the lowest cost path from this bridge to the root bridge.
MaxAge	Specifies the maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded . The maximum age is specified in units of hundredths of a second. This is the actual value that bridge uses.
HelloTime	Sets the amount of time required for transmission of the configuration BPDUs by the node on any port when it is the root of the spanning tree or trying to become the root. This is specified in units of hundredths of a second. This is the actual value that bridge uses.
ForwardDelay	Specifies the time (measured in units of hundredths of a second), which control how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state. This value is also used when a topology change has been

Table continues...

Name	Description
	detected, and is underway to age all dynamic entries in the Forwarding Database.
RstpUpCount	Specifies the number of times the RSTP Module has been enabled. A Trap is generated on the occurrence of this event.
RstpDownCount	Specifies the number of time the RSTP Module has been disabled. A Trap is generated on the occurrence of this event.
NewRootIdCount	Specifies the number of times this Bridge has detected a Root Identifier change. A Trap is generated on the occurrence this event.
TimeSinceTopologyChange	Specifies the time (in hundredths of a second) since the TcWhile Timer for any port in this Bridge was non-zero for Common Spanning Tree context.
TopChanges	Specifies the total number of topology changes detected by this bridge since the management entity was last reset or initialized.

Displaying RSTP ports information using EDM

Use this procedure to view RSTP Ports information.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **RSTP**.
4. Select the **RSTP Ports** tab.

RSTP Ports field descriptions

The following table describes the fields on the RSTP Ports tab.

Name	Description
Port	Specifies the port number.
State	Every 2 bitfields identifies a port state in this STG. Port state is cataloged as non-stp(0), blocking(1), learning(2), and forwarding(3).
Priority	The value of the priority field is contained in the first (in network byte order) octet of the (2 octet long) Port ID.

Table continues...

Name	Description
PathCost	Specifies the contribution of this port to the path cost of paths towards the spanning tree root which include this port.
ProtocolMigration	<p>Specifies the number of times this port has migrated from one STP protocol version to another. The relevant protocols are:</p> <ul style="list-style-type: none"> • STP-COMPATIBLE • RSTP <p>A Trap is generated on the occurrence of this event.</p>
AdminEdgePort	Specifies the administrative value of the Edge Port parameter. A value of TRUE(1) indicates that this port should be assumed as an edge-port and a value of FALSE(2) indicates that this port should be assumed as a non-edge-port.
OperEdgePort	Specifies the operational value of the Edge Port parameter. The object is initialized to FALSE on reception of a BPDU.
AdminPointToPoint	<p>Specifies the administrative point-to-point status of the LAN segment attached to this port. A value of forceTrue(0) indicates that this port should always be treated as if it is connected to a point-to-point link.</p> <ul style="list-style-type: none"> • A value of forceFalse or 1 indicates that this port should be treated as having a shared media connection. • A value of auto or 2 indicates that this port is considered to have a point-to-point link if it is an Aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means.
OperPointToPoint	Specifies the operational point-to-point status of the LAN segment attached to this port. It indicates whether a port is considered to have a point-to-point connection or not. The value is determined by management or by auto-detection.
Participating	Specifies whether a port is participating in the 802.1w protocol.
DesignatedRoot	Specifies the bridge identifier of the old root of the Spanning Tree as determined by the Spanning Tree Protocol as executed by this node.
DesignatedCost	Specifies the path cost of the Designated Port of the segment connected to this port. This value is

Table continues...

Name	Description
	compared to the Root Path Cost field in received BPDUs.
DesignatedBridge	Specifies the Bridge Identifier of the bridge which this port considers to be the Designated Bridge for this port's segment.
DesignatedPort	Specifies the Port Identifier for the port segment which is on the Designated Bridge for this port's segment.
ForwardTransitions	Specifies the number of times this port has transitioned from the Learning state to the Forwarding state.

Displaying RSTP status using EDM

Use this procedure to view RSTP status.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **RSTP**.
4. Select the **RSTP Status** tab.

RSTP Status field descriptions

The following table describes the fields on the RSTP Status tab.

Name	Description
Port	Specifies the port number.
Role	Specifies the functionality characteristic or capability of a resource to which policies are applied.
OperVersion	Indicates whether the Port is operationally in the RSTP mode or the STP-compatible mode for example, whether the Port is transmitting RST BPDUs or Config/TCN BPDUs.
EffectivePortState	Specifies the effective Operational state of the port. This object will be set to TRUE only when the port is operationally up in the interface manager and the force Port State for this port and specified port state is enabled. Otherwise this object is set to FALSE

Graphing RSTP port statistics using EDM

Use this procedure to display RSTP port statistics.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **RSTP**.
4. Select the **RSTP Status** tab.
5. Select a port and click on **Graph** to get the statistics for the selected port.

RSTP Status Graph field descriptions

The following table describes the fields on the RSTP Status Graph tab.

Name	Description
RxRstBpduCount	Displays the number of RST BPDUs that were received on this port.
RxConfigBpduCount	Displays the number of Configuration BPDUs that were received on this port.
RxTcnBpduCount	Displays the number of TCN BPDUs that were received on this port.
TxRstBpduCount	Displays the number of RST BPDUs transmitted from this port.
TxConfigBpduCount	Displays the number of Configuration BPDUs transmitted from this port.
TxTcnBpduCount	Displays the number of TCN BPDUs transmitted from this port.
InvalidRstBpduRxCount	Displays the number of invalid RST BPDUs received on this port.
InvalidConfigBpduRxCount	Displays the number of invalid Configuration BPDUs received on this port.
InvalidTcnBpduRxCount	Displays the number of invalid TCN BPDUs received on this port.
ProtocolMigrationCount	Displays the number of times this port has migrated from one STP protocol version to another. The relevant migration protocols are STP-COMPATIBLE and RSTP/MSTP. A trap is generated when the port migrates.

Multiple Spanning Tree Protocol

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

The switch uses RSTP and MSTP to achieve the following:

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

Multiple Spanning Tree Protocol

With Multiple Spanning Tree Protocol (MSTP or IEEE 802.1s), the user can configure multiple instances of RSTP on the same switch. Each RSTP instance can include one or more VLANs. The operation of the MSTP is similar to the current Extreme Networks proprietary STG.

In the MSTP mode, a maximum of one Common and Internal Spanning Tree (CIST) and seven Multiple Spanning Tree Instances (MSTI) are supported.

Important:

You can access the MSTP menu command only when the switch is operating in the MSTP mode.

Displaying MSTP general information using EDM

Use this procedure to view MSTP information.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **MSTP**.

The MSTP dialog box with the **Globals** tab is displayed.

MSTP Globals field descriptions

The following table describes the fields on the MSTP Globals tab.

Name	Description
PathCostDefaultType	Specifies the version of the Spanning Tree default Path Costs that are to be used by this Bridge: <ul style="list-style-type: none"> • A 16-bit value uses the 16-bit default path costs from IEEE Standard 802.1D-1998. • A 32-bit value uses the 32-bit default path costs from IEEE Standard 802.1t.
TxHoldCount	Specifies the value used by the Port Transmit state machine to limit the maximum transmission rate.
MaxHopCount	Specifies the Maximum Hop Count value. The granularity of this timer is specified to be 1 second. An agent can return a badValue error if a set is attempted to a value which is not a whole number of seconds.
NoOfInstancesSupported	Indicates maximum number of spanning tree instances supported.
MstpUpCount	Specifies the number of times the MSTP Module has been enabled. A Trap is generated on the occurrence of this event.
MstpDownCount	Specifies the number of times the MSTP Module has been disabled. A Trap is generated on the occurrence of this event.
ForceProtocolVersion	Signifies the version of the Spanning Tree Protocol that the bridge is currently running. <ul style="list-style-type: none"> • stpCompatible indicates that the bridge is using the Spanning Tree Protocol as specified in IEEE 802.1D. • rstp indicates that the bridge is using the Rapid Spanning Tree Protocol as specified in IEEE 802.1w • mstp indicates that the bridge is running the Multiple Spanning Tree Protocol as specified in IEEE 802.1s.
BrgAddress	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.

Table continues...

Name	Description
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 of the first two octets. The values that are set for Bridge Priority must be in steps of 4096.
BridgeMaxAge	Specifies the value that all bridges use for MaxAge when this bridge is acting as the root. The granularity of this timer is specified to be 1 second. An agent can return a badValue error if a set is attempted to a value which is not a whole number of seconds.
BridgeForwardDelay	Specifies the value that all bridges use for ForwardDelay when this bridge is acting as the root. IEEE 802.1D specifies that the range for this parameter is related to the value of BridgeMaxAge. The granularity of this timer is specified to be 1 second. An agent can return a badValue error if a set is attempted to a value which is not a whole number of seconds.
HoldTime	Determines the time interval during which no more than two Configuration BPDUs shall be transmitted by this node. This value is measured in units of hundredths of a second.
MaxAge	Specifies the maximum age of the Spanning Tree Protocol information learned from the network on any port before it is discarded. This value is measured in units of hundredths of a second.
ForwardDelay	Controls how fast a port changes its spanning state when moving towards the Forwarding state. This value determines how long the port stays in a particular state before moving to the next state. It is measured in units of hundredths of a second.

Table continues...

Name	Description
TimeSinceTopology Change	Specifies the value (measured in hundredths of a second) The time since the TcWhile Timer for any port in this Bridge was non-zero for Common Spanning Tree context.
TopChanges	Specifies the number of times that there have been at least one non-zero TcWhile Timer on this Bridge for the Common Spanning Tree context.
NewRootBridgeCount	Specifies the number of times this Bridge has detected a Root Bridge change for the Common Spanning Tree context. A Trap is generated when this event occurs.
RegionName	Signifies the name of the Region's configuration. By default, the Region Name is equal to the Bridge Mac Address.
RegionVersion	Denotes the version of the MST Region.
ConfigIdSel	Specifies the Configuration Identifier Format Selector used by the Bridge. This has a fixed value of 0 which is used to indicate RegionName, RegionVersion as specified in standard.
ConfigDigest	Signifies the Configuration Digest value for this Region. This is an MD5 digest value, and hence must always be 16octets long.
RegionConfigChangeCount	Specifies the number of times a Region Configuration Identifier Change was detected. A Trap is generated when this event occurs.

Displaying CIST port information using EDM

Use this procedure to display CIST port information.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **MSTP**.
4. Select the **CIST Port** tab.

CIST Port field descriptions

The following table describes the fields on the CIST Port tab.

Name	Description
Port	Identifies the port number of the port containing Spanning Tree information.
PathCost	Specifies the contribution of this port to the path cost of paths towards the CIST Root which include this port.
Priority	Displays the four most significant bits of the Port Identifier of the Spanning Tree instance. It can be modified by setting the CistPortPriority value. The values that are set for Port Priority must be in steps of 16.
DesignatedRoot	Specifies the unique Bridge Identifier of the bridge. It is recorded as the CIST Root in the configuration BPDUs which are transmitted.
DesignatedCost	Specifies the path cost of the Designated Port of the segment connected to this port.
DesignatedBridge	Specifies the unique Bridge Identifier of the bridge which the port considers to be the Designated Bridge for the port's segment.
DesignatedPort	Displays the Port identifier of the port on the Designated Bridge which is designated for the port's segment.
RegionalRoot	Displays the unique Bridge Identifier of the bridge. It is recorded as the CIST Regional Root Identifier in the configuration BPDUs which are transmitted.
RegionalPathCost	Displays the contribution of this port to the cost of paths. This value denotes the path of costs for the path towards the CIST Regional Root which include this port.
ProtocolMigration	Display is generated when port protocol migration happens in the port.
AdminEdgeStatus	Specifies the administrative value of the Edge Port parameter. A value of TRUE indicates that this port to be assumed as an edge-port and a value of FALSE indicates that this port to be assumed as a non-edge-port.
OperEdgeStatus	Signifies the operational value of the Edge Port parameter. It is initialized to the value of AdminEdgeStatus and is set to FALSE when the port receives a BPDU.
AdminP2P	Displays the administrative point-to-point status of the LAN segment attached to this port. A value of 0 indicates that this port should always be treated as if it is connected to a point-to-point link. A value of 1

Table continues...

Name	Description
	indicates that this port should be treated as having a shared media connection. A value of 2 indicates that this port is considered to have a point-to-point link if it is an Aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation, or by management means.
OperP2P	Indicates the operational point-to-point status of the LAN segment attached to the port. It also indicates whether a port is considered to have a point-to-point connection or not. The value is determined by management or by auto-detection, as described in the AdminP2P object
HelloTime	Displays the amount of time between the transmission of Configuration BPDUs transmitted by this node on the port. It is measured in units of hundredths of a second.
OperVersion	Indicates whether the port is operationally in the MSTP mode, RSTP mode or the STP-compatible mode for example, whether the port is transmitting MST BPDUs, RST BPDUs, or Config/TCN BPDUs.
EffectivePortState	Displays the effective operational state of the port for CIST. This will be set to TRUE only when the port is operationally up in the Interface level and Protocol level for CIST. This will be set to FALSE for all other times.
State	Displays the current state of the port as defined by the Common Spanning Tree Protocol.
ForcePortState	Displays the current state of the port which can be changed to either Disabled or Enabled for the base Spanning Tree instance.
SelectedPortRole	Displays the elected port role of the port for the Spanning Tree instance.
CurrentPortRole	Displays the current port role of the port for the Spanning Tree instance.

Graphing CIST Port Statistics using EDM

Use this procedure to display CIST Port statistics.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.

3. Double-click **MSTP**.
4. Select the **CIST Port** tab.
5. Select a port and click on **Graph** to get the statistics for the CIST port.

CIST Port field descriptions

The following table describes the fields on the CIST Port tab.

Name	Description
ForwardTransitions	Displays the number of times this port has transitioned to the Forwarding State.
RxMstBpduCount	Displays the number of MST BPDUs that were received on this port.
TxRstBpduCount	Displays the number of RST BPDUs that were received on this port.
RxConfigBpduCount	Displays the number of Configuration BPDUs that were received on this port.
RxTcnBpduCount	Displays the number of TCN BPDUs that were received on this port.
TxMstBpduCount	Displays the number of MST BPDUs transmitted from this port.
TxRstBpduCount	Displays the number of RST BPDUs transmitted from this port.
TxConfigBpduCount	Displays the number of Configuration BPDUs transmitted from this port.
TxTcnBpduCount	Displays the number of TCN BPDUs transmitted from this port.
InvalidMstBpduRxCount	Displays the number of invalid MST BPDUs received on this port.
InvalidRstBpduRxCount	Displays the number of invalid RST BPDUs received on this port.
InvalidConfigBpduRxCount	Displays the number of invalid Configuration BPDUs received on this port.
InvalidTcnBpduRxCount	Displays the number of invalid TCN BPDUs received on this port.
ProtocolMigrationCount	Displays the number of times this port has migrated from one STP protocol version to another. The relevant migration protocols are STP-COMPATIBLE and RSTP/MSTP. A trap is generated when the port migrates.

Displaying MSTI Bridges using EDM

Use this procedure to view the MSTI Bridges information.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **MSTP**.
4. Select the **MSTI Bridges** tab.

MSTI Bridges field descriptions

The following table describes the fields on the MSTI Bridges tab.

Name	Description
Instance	Specifies the Spanning Tree Instance to which the information belongs.
RegionalRoot	Specifies MSTI Regional Root Identifier value for the Instance. This value is used as the MSTI Regional Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
Priority	Specifies the writable portion of the MSTI Bridge Identifier comprising of the first two octets. The values that are set for Bridge Priority must be in steps of 4096.
RootCost	Specifies the cost of the path to the MSTI Regional Root as seen by this bridge.
RootPort	Specifies the port number of the port which offers the lowest path cost from this bridge to the MSTI Region Root Bridge.
Enabled	Defines whether the bridge instance is enabled or disabled.
TimeSinceTopology Change	Specifies the time (measured in hundredths of a second) since theTcWhile Timer for any port in this bridge was non-zero for this Spanning Tree instance.
TopChanges	Specifies the number of times that there have been at least one non-zero TcWhile Timer on this Bridge for this Spanning Tree instance.
NewRootCount	Specifies the number of times that there have been at least one non-zero TcWhile Timer on this Bridge for this Spanning Tree instance.

Table continues...

Name	Description
InstanceUpCount	Specifies the number of times a new Spanning Tree instance has been created. A Trap is generated on the occurrence of this event.
InstanceDownCount	Specifies the number of times a Spanning Tree instance has been deleted. A Trap is generated on the occurrence of this event.

Inserting MSTI Bridges using EDM

Use this procedure to insert MSTI Bridges.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **MSTP**.
4. Select the **MSTI Bridges** tab.
5. Click **Insert**.
6. Type the instance id.
7. Click **Insert**.

Deleting MSTI Bridges using EDM

Use this procedure to delete MSTI Bridges.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **MSTP**.
4. Select the **MSTI Bridges** tab.
5. Click on one or multiple MSTI Bridges.
6. Click **Delete**.
7. To confirm you wish to delete the MSTI bridge, click **Yes**.

Displaying MSTI Port information using EDM

Use this procedure to view MSTI Port information.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **MSTP**.
4. Select the **MSTI Port** tab.

MSTI Port field descriptions

The following table describes the fields on the MSTI Port tab.

Name	Description
Port	Denotes the port number.
Instance	Specifies the number of times a Spanning Tree instance has been deleted. A Trap is generated when this event occurs.
State	Specifies the current state of the port as defined by application of the Multiple Spanning Tree Protocol. The state of a port can be Forwarding state in one instance, and Discarding (Blocking) state in another instance.
ForcePortState	Specifies the current state of the port which can be changed to either Disabled or Enabled for the specific Spanning Tree instance.
PathCost	Specifies the contribution of this port to the cost of paths towards the MSTI root, including the current port.
Priority	Indicates the four most significant bits of the Port Identifier for a given Spanning Tree instance. It can be modified independently for each Spanning Tree instance supported by the bridge. The values that are set for Port Priority must be in steps of 16.
DesignatedRoot	Specifies the unique "Bridge Identifier." This is recorded as the MSTI Regional Root in the configuration BPDUs that are transmitted.
Designated Bridge	Identifies the Bridge Identifier of the bridge which this port considers to be the Designated Bridge for this port's segment.
DesignatedPort	Identifies the Port Identifier of the port on the designated Bridge for this port's segment.

Table continues...

Name	Description
DesignatedCost	Specifies the path cost of the Designated Port of the segment connected to the port.
CurrentPortRole	Specifies the current Port Role of the port for this spanning tree instance.
EffectivePortState	Specifies the effective operational state of the port for specific instance. This is TRUE only when the port is operationally up in the interface level and Protocol level for the specific instance. This is set to FALSE at all other times.

Graphing MSTI port statistics using EDM

Use this procedure to display MSTI port statistics.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **Spanning Tree**.
3. Double-click **MSTP**.
4. Select the **MSTI Port** tab.
5. Select a port and click on **Graph** to get the statistics for the MSTI port.

MSTI Port field descriptions

The following table describes the fields on the MSTI Port tab.

Name	Description
ForwardTransitions	Specifies the number of times this port has transitioned to the Forwarding State for specific instance.
InvalidBPDUsRcvd	Specifies the number of Invalid BPDUs received on this Port for this Spanning Tree instance.
ReceivedBPDUs	Specifies the number of BPDUs received by this port for this Spanning Tree instance.
TransmittedBPDUs	Specifies the number of BPDUs transmitted on this port for this Spanning Tree instance.

Setting up bridging

The Bridge parameters allow you to configure the global Spanning Tree and to view the MAC address table. Bridge information also includes Spanning Tree Group (STG) information.

This section describes how to work with the Base, Transparent, and Forwarding tabs to view bridge parameters, and how to view port bridge statistics.

Viewing Bridge base information using EDM

Use this procedure to view the Base tab. The Base tab displays the MAC address used by the bridge, the number of ports controlled by the bridge, and the type of bridge.

Procedure

1. In the navigation tree, double-click **Edit**.
2. Double-click **Bridge**.
3. In the work area, click the **Base** tab.

Bridge Base field descriptions

The following table describes the fields on the Base tab.

Name	Description
BridgeAddress	Specifies the MAC address used by the bridge which must be referred to in a unique fashion; moreover, it should be the smallest MAC address (numerically) of all ports that belong to the bridge. However, it is only required to be unique when integrated with dot1dStpPriority. A unique BridgeIdentifier is formed that is used in the Spanning Tree Protocol.
NumPorts	Specifies the number of ports controlled by the bridging entity.
Type	Indicates the type of bridging this bridge can perform. If the bridge is actually performing a certain type of bridging, this will be indicated by entries in the port table for the given type.

Viewing information about specific unicast MAC address using EDM


Use this procedure to view information about a specific unicast MAC address that has forwarding information for the bridge.

Procedure

1. In the navigation tree, double-click **Edit**.
2. Double-click **Bridge**.
3. Select the **Transparent** tab.

Bridge Transparent field descriptions

The following table describes the fields on the Transparent tab.

Name	Description
LearnedEntryDiscards	Specifies the number of Forwarding database entries learned that have been discarded due to a lack of space in the Forwarding database. If this counter is increasing, it indicates that the Forwarding database is becoming full regularly. This condition will affect the performance of the subnetwork. If the counter has a significant value and is not presently increasing, it indicates that the problem has been occurring but is not persistent.
AgingTime	Specifies the time-out period in seconds for aging out dynamically learned forwarding information.  Important: The 802.1D-1990 specification recommends a default of 300 seconds.

Displaying current MAC Address Table using EDM

Use this procedure to view the current MAC Address Table (Forwarding table) on the switch.

Procedure

1. In the navigation tree, double-click **Edit**.
2. Double-click **Bridge**.
3. Select the **Forwarding** tab.

Bridge Forwarding field descriptions

The following table describes the fields on the Forwarding tab.

Name	Description
Id	Specifies the VLAN identifier.
Address	Specifies a unicast MAC address for which the bridge has forwarding or filtering information.

Table continues...

Name	Description
Port	Indicates that either the value "0" or the port number on a frame has been seen. The source address must be equal to the value of the corresponding instance of dot1dTpFdbAddress. A value of "0" indicates that the port number has not been learned, so the bridge does not have the forwarding/filtering information for this address (located in the dot1dStaticTable). You should assign the port value to this object whenever it is learned even for addresses for which the corresponding value of dot1dTpFdbStatus is not learned(3).
Status	<p>The values of this field include:</p> <ul style="list-style-type: none"> • 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 would include where some other MIB object (not the corresponding instance of dot1dTpFdbPort or an entry in the dot1dStaticTable) is being used to determine if frames addressed to the value of dot1dTpFdbAddress are being forwarded.

Graphing port bridge statistics using EDM

Use this procedure to graph port bridge statistical information.

Procedure

1. From the Device Physical View, click a port.
2. In the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **Bridge** tab.
5. Click the down arrow to the right of the **Poll Interval** dialog box.

6. Select a value from the list.
7. To reset the statistics counters, click **Clear Counters**.
8. To select bridge statistical information to graph, click an information row.
9. Click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart** column.

Bridge tab field descriptions

The following table describes the fields on the Bridge tab.

Name	Description
DelayExceededDiscards	Specifies the number of frames discarded by the port due to excessive transit delays through the bridge. It is incremented by both transparent and source route bridges.
MtuExceededDiscards	Specifies the number of frames discarded by the port due to an excessive size. It is incremented by both transparent and source route bridges.
InFrames	Specifies the number of frames that have been received by this port from its segment.
OutFrames	Specifies the number of frames that have been received by this port from its segment.
InDiscards	Provides count of valid frames received which were discarded (filtered) by the Forwarding Process.

Chapter 15: Configuring Multi-Link Trunking using Enterprise Device Manager

Multi-Link Trunking (MLT) is a point-to-point connection that aggregates multiple ports so that they logically act like a single port with the aggregated bandwidth. You can achieve higher aggregate throughput on a switch-to-switch or switch-to-server application by grouping multiple ports into a logical link . Multi-Link Trunking provides media and module redundancy.

Multi-Link Trunk features

Multi-Link Trunking has the following general features and requirements:

- A unit can have up to six Multi-Link Trunks (MLTs).
- Up to four ports can belong to an MLT.
- Multi-Link Trunking is supported on 10BASE-T, 100BASE-TX, 1000Base-T, and SFP ports.
- Multi-Link Trunking is compatible with the Spanning Tree Protocol
- IEEE 802.1Q tagging is supported on an MLT.
- The distribution algorithm is user-programmable. The default algorithm that distributes traffic across an MLT is based on the source and destination MAC addresses (BASIC mode). An algorithm that distributes traffic based on the source and destination IP addresses (ADVANCE mode) is also available.
- Distributed MLT (DMLT) is supported. DMLT is MLT with ports from two or more stack units.

Configuring Multi-Link Trunks using EDM

Use this procedure to display and configure MLT and LACP global settings using EDM.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **MLT/LACP**.

3. In the work area, click the **Global** tab.
4. Configure the optional configuration settings.
5. On the toolbar, click **Apply**.

Configuring Multi-Link Trunks using EDM

Use this procedure to display and configure MLTs using EDM.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **MLT/LACP**.
3. In the work area, click the **Multi-Link Trunks** tab.
4. To select a trunk to create, click the trunk ID.
5. In the trunk row, double-click the cell in the **Name** column.
6. In the field, type a name for the MLT, or accept the default name.
7. In the trunk row, double-click the cell in the **PortMembers** column.
8. From the list, select multiple ports to add to the trunk.
9. Click **OK**.
10. In the trunk row, double-click the cell in the **Loadbalance(Mode)** column.
11. From the list, select a load balancing mode.
12. In the trunk row, double-click in the **Enable** column.
13. From the list, select **true** to enable the MLT, or **false** to disable the MLT.
14. To create additional MLTs, repeat steps 4 to 13.
15. On the toolbar, click **Apply**.

Multi-Link Trunks field descriptions

The following table describes the fields on the Multi-Link Trunks tab.

Name	Description
Id	Specifies the MLT identification number (assigned consecutively).
PortType	Specifies the access or trunk port.
Name	Specifies the name given to the MLT.
PortMembers	Specifies the ports assigned to the MLT.
VlanIds	Specifies the VLANs assigned to the MLT.

Table continues...

Name	Description
Loadbalance(Mode)	Specifies the load balance mode. Values include: <ul style="list-style-type: none"> • basic • advanced
Enable	Specifies enabling of the MLT.

Displaying MLT utilization using EDM

Use this procedure to views MLT utilization information during the last hour.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the work area, click the **MLT Utilization** tab.

MLT Utilization field descriptions

The following table describes the fields on the MLT Utilization tab.

Name	Description
Mtld	Specifies the MLT Identification number.
PortIdIndex	Specifies the port identification number.
TrafficType	Specifies the traffic type.
TrafficLast5Min	Specifies the MLT traffic in the last five minutes.
TrafficLast30Min	Specifies the MLT traffic in the last thirty minutes.
TrafficLast1Hour	Specifies the MTL traffic in the last hour.

Graphing Multi-Link Trunk statistics using EDM

Use this procedure to display and graph MLT interface statistics.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **MLT/LACP**.
3. In the work area, click the **Multi-Link Trunks**
4. To select an MLT to graph, click the trunk Id.
5. Click **Graph**.
6. Click the **Interface** tab.

7. Select a **Poll Interval** from the list.
8. From the list, select a poll interval time.
9. To reset the MLT statistics counters, click **Clear Counters**.
10. To select statistics to graph, click a statistic type row under one of the display columns.
11. Click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.
12. To return to the Multi-Link Trunks — Graph work area, click **Close**.

Multi-Link Trunks field descriptions

The following table describes the fields on the Multi-Link Trunks tab.

Name	Description
InMulticastPkts	Specifies the number of packets delivered to this MLT that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.
OutMulticastPkts	Specifies the total number of packets that higher-level protocols requested to be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
InBroadcastPkts	Specifies the number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
OutBroadcastPkts	Specifies the total number of packets that higher-level protocols requested to be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.
HCInOctets	Specifies the total number of octets received on the MLT interface, including framing characters.
HCOctets	Specifies the total number of octets transmitted out of the MLT interface, including framing characters.
HCInUcastPkts	Specifies the number of packets delivered by this MLT to a higher MLT that were not addressed to a multicast or broadcast address at this sublayer.
HCOctets	Specifies the number of packets that high-level protocols requested to be transmitted that were not addressed to a multicast address at this MLT. This total number includes those packets discarded or unsent.
HCInMulticastPkts	Specifies the number of packets delivered to this MLT that were addressed to a multicast address at

Table continues...

Name	Description
	this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.
HcOutMulticast	Specifies the total number of packets that high-level protocols requested to be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
HCinBroadcastPkt	Specifies the number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
HCOutBroadcast	Specifies the total number of packets that high-level protocols requested to be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.

Graphing Multi-Link Trunk Ethernet error statistics using EDM

Use this procedure to display and graph Multi-Link Trunk Ethernet error statistics.

Procedure

1. In the navigation tree, double-click **VLAN**.
2. Double-click **MLT/LACP**.
3. In the work area, click the **Multi-Link Trunks**
4. To select an MLT to graph, click the trunk Id.
5. Click **Graph**.
6. Click the **Ethernet Errors** tab.
7. Select a **Poll Interval** from the list.
8. From the list, select a poll interval time.
9. To reset the MLT statistics counters, click **Clear Counters**.
10. To select statistics to graph, click a statistic type row under one of the display columns.
11. Click **Line Chart, Area Chart, Bar Chart, or Pie Chart**.
12. To return to the Multi-Link Trunks — Graph work area, click **Close**.

Ethernet Errors field descriptions

The following table describes the fields on the Ethernet Errors tab.

Name	Description
AlignmentErrors	Specifies the count of frames received on a particular MLT that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
FCSErrors	Specifies the count of frames received on an MLT that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
IMacTransmitError	Specifies the count of frames for which transmission on a particular MLT fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object.
IMacReceiveError	Specifies the count of frames for which reception on a particular MLT fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLong object, the AlignmentErrors object, or the FCSErrors object. The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object can represent a count of received errors on a particular interface that are not otherwise counted.
CarrierSenseError	Specifies the number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular MLT. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.

Table continues...

Name	Description
FrameTooLong	Specifies the count of frames received on a particular MLT that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
SQETestError	Specifies the count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular MLT. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
DeferredTransmiss	Specifies the count of frames for which the first transmission attempt on a particular MLT is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollFrames	Specifies the count of successfully transmitted frames on a particular MLT for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object.
MultipleCollFrames	Specifies the count of successfully transmitted frames on a particular MLT for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	Specifies the number of times that a collision is detected on a particular MLT later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is

Table continues...

Name	Description
	also considered as a (generic) collision for purposes of other collision-related statistics.
ExcessiveCollis	Specifies the count of frames for which transmission on a particular MLT fails due to excessive collisions.

Selecting an SLPP Guard Ethernet type using EDM

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

Important:

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

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **SLPP**.
3. In the work area, click the **Global** tab.
4. Type a value in the **SlppGuardEtherType** box.
5. On the toolbar, click **Apply**.

Configuring SLPP Guard using EDM

Use this procedure to configure SLPP Guard for switch ports.

Note:

SLPP packets are generated only on switches that are configured with SLPP. SLPP is not supported on this switch. When you enable SLPP Guard, the switch must be connected to another switch that supports SLPP and that has SLPP enabled.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **SLPP**.
3. In the work area, click the **SLPP Guard** tab.
4. To select a specific switch port, click an **IfIndex**.
5. In the IfIndex row, double-click the cell in the **Enabled** column.
6. Select a value from the list—**true** to enable SLPP Guard, **false** to disable SLPP Guard.
7. In the IfIndex row, double-click the cell in the **Timeout** column.
8. Type a value in the **Timeout** box.

9. On the toolbar, click **Apply**.

Variable definition

Variable	Value
IfIndex	Specifies the port on which to configure SLPP Guard.
Enable	Enables (true) or disables (false) SLPP Guard for the port.
Timeout	Specifies the time period, in seconds, for which SLPP Guard disables the port. After the timeout period expires, the switch re-enables the port. The timeout value can be 0 or a value ranging from 10 to 65535. With a value of 0, the port remains disabled until it is manually re-enabled. The default Timeout value is 60 seconds.
Status	Displays the SLPP Guard status for the port.
TimerCount	Indicates the time, in seconds, that elapses after SLPP Guard disables a port. When the TimerCount value equals the Timeout value, the switch re-enables the port.

Chapter 16: Configuring ADAC for IP phones using Enterprise Device Manager

This chapter provides procedure you can use to configure Auto-Detection and Auto-Correction (ADAC) using Enterprise Device Manager.

Related links

[Configuring ADAC globally using EDM](#) on page 215

[ADAC port information management using EDM](#) on page 217

[ADAC MAC address range configuration using EDM](#) on page 221

Configuring ADAC globally using EDM

Use this procedure to configure ADAC settings for the switch.

Procedure

1. In the navigation tree, double-click **Edit**.
2. Double-click **ADAC** to open the ADAC work area.
3. Click the **ADAC** tab.
4. Select the **AdminEnable** box to enable ADAC globally.
OR
Clear the **AdminEnable** to disable ADAC globally.
5. Click an **OperatingMode** radio button.
6. Select the **NotificationControlEnable** check box to enable trap notifications globally.
OR
Clear the **NotificationControlEnable** check box to disable trap notifications.
7. In the **VoiceVlan** dialog box, type a value.
8. Click the **CallServerPortList** elipsis (...).

9. From the Call Server Port list, select Call Server ports.
10. Click **OK**.
11. Click the **UplinkPortList** elipsis (...).
12. From the uplink port list, select uplink ports.
13. Click **OK**.
14. Click a **MacAddrRangeControl** radio button.
15. On the toolbar, click **Apply**.

 **Important:**

You cannot apply the global ADAC configuration if VoiceVlan, CallServerPortList, or UplinkPortList fields are set to 0 or empty when AdminEnable is selected and the operating mode is tagged frames or advanced untagged frames.

 **Important:**

You cannot configure the same port values for Call Server and Uplink.

ADAC field descriptions

The following table describes the fields on the ADAC tab.


Name	Description
AdminEnable	Enables and disables ADAC
OperEnable	Indicates ADAC operational state: true is enabled and false is disabled.  Important: If AdminEnable is True and OperEnable is False, this indicates an error condition such as missing Uplink and Call Server ports.
OperatingMode	Specifies the ADAC operation mode: <ul style="list-style-type: none"> • untaggedFramesBasic: IP Phones send untagged frames, and the Voice VLAN is not created. • untaggedFramesAdvanced: IP Phones send untagged frames, and the Voice VLAN is created. • taggedFrames: IP Phones send tagged frames.
NotificationControlEnable	Enables or disables ADAC trap notifications.
VoiceVlan	Specifies the Voice VLAN ID. The assigned VLAN ID must previously be created as a voice VLAN.

Table continues...

Name	Description
CallServerPortList	Specifies the Call Server port. A maximum of 8 Call Server ports are supported.
UplinkPortList	Specifies the Uplink port. A maximum of 8 uplink ports are supported.
MacAddrRangeControl	Provides two options for configuring the MAC address range table: <ul style="list-style-type: none"> • none: no MAC address range table selected • clearTable: clears the MAC address range table. • defaultTable: sets the MAC address range table to its default values.

ADAC port information management using EDM

Use the information in this section to configure ADAC for switch ports and to display port-based ADAC information.

Displaying port ADAC for information using EDM

Use this procedure to view ADAC configuration information for switch ports.

Procedure

1. In the navigation tree, double-click **Edit**.
2. Double-click **Chassis**.
3. Double-click **Ports**.
4. Double-click **ADAC**.
5. In the **Ports** work area, click the **ADAC** tab.

OR

In the **ADAC** work area, click the **ADAC Ports** tab.

6. On the toolbar, you can click **Refresh** to update the data.

ADAC or ADAC Ports field descriptions

The following table describes the fields on the ADAC or ADAC Ports tab.

Name	Description
Index	Indicates the switch position in a stack and the port number. DEFAULT: 1
AdminEnable	Indicates whether ADAC is enabled (true) or disabled (false) for the port.
OperEnable	Indicates ADAC operational state: true (enabled) or false (disabled).
ConfigStatus	Indicates the ADAC status for the port. Values include: <ul style="list-style-type: none"> • configApplied: the ADAC configuration is applied to this port. • configNotApplied: the ADAC configuration is not applied to this port.
TaggedFramesPvid	Indicates a unique PVID between 1 and 4094. A value of 0 indicates that Auto-Configuration cannot change the PVID for the port.
TaggedFramesTagging	Indicates the ADAC operating mode. Values include: <ul style="list-style-type: none"> • tagAll: tags all frames • tagPvidOnly: tags frames by the unique PVID • untagPvidOnly: untags frames by the unique PVID • noChange: accepts frames without change
AdacPortType	Indicates how ADAC classifies the port. Values include: <ul style="list-style-type: none"> • telephony: when Auto-Detection is enabled for the port. • telephony: auto-detection is enabled.. • callServer: port is configured as a call server • uplink: port is configured as an uplink or is part of the same trunk as the uplink port. • other: the port is not classified as either telephony, callServer, or uplink.
MacDetectionEnable	Indicates whether Auto-Detection of IP Phones, based on MAC address, is enabled (true) or disabled (false) on the interface.
LldpDetectionEnable	Indicates whether Auto-Detection of IP Phones, based on 802.1AB, is enabled (true) or disabled (false) on the interface. When cleared, indicates that

Table continues...

Name	Description
	Auto- Detection of IP Phones, based on 802.1AB, is disabled on the interface.

Configuring ADAC for specific ports using EDM

Use this procedure to configure ADAC for one or more ports in a standalone switch or switch stack.

Procedure



1. In the navigation tree, double-click **Edit**.
2. Double-click **Chassis**.
3. Double-click **Ports**
OR
Double-click **ADAC**.
4. In the Ports work area, click the **ADAC** tab.
OR
In the ADAC work area, click **ADAC Ports** tab.
5. To select a port to edit, click the port **Index**.
6. In the port row, double-click the cell in the **AdminEnable** column.
7. Select a value from the list — true to enable ADAC for the port, or false to disable ADAC for the port.
8. In the port row, double-click the cell in the **TaggedFramesPvid** column.
9. Type a value in the dialog box.
10. In the port row, double-click the cell in the **TaggedFramesTagging** column.
11. Select a value from the list.
12. In the port row, double-click the cell in the **MacDetectionEnable** column.
13. Select a value from the list — true to enable MAC address detection for the port, or false to disable MAC address detection for the port.
14. In the port row, double-click the cell in the **LldpDetectionEnable** column.
15. Select a value from the list — true to enable LLDP detection for the port, or false to disable LLDP detection for the port.
16. Repeat steps 5 through 15 to configure ADAC for additional ports.
17. On the toolbar, click **Apply**.

ADAC or ADAC Ports field descriptions

The following table describes the fields on the ADAC or ADAC Ports tab.

Name	Description
Index	Indicates the switch position in a stack and the port number. DEFAULT: 1
AdminEnable	Indicates whether ADAC is enabled (true) or disabled (false) for the port.
OperEnable	Indicates ADAC operational state: true (enabled) or false (disabled). This is a read-only cell. ! Important: If OperEnable is False and AdminEnable is True, then Auto-Detection/Auto-Configuration is disabled. This can occur due to a condition such as reaching the maximum number of devices supported per port.
ConfigStatus	Indicates the ADAC status for the port. This is a read-only cell. Values include: <ul style="list-style-type: none"> • configApplied: the ADAC configuration is applied to this port. • configNotApplied: the ADAC configuration is not applied to this port.
TaggedFramesPvid	Indicates a unique PVID between 1 and 4094. A value of 0 indicates that Auto-Configuration cannot change the PVID for the port.
TaggedFramesTagging	Indicates the ADAC operating mode. Values include: <ul style="list-style-type: none"> • tagAll: tags all frames • tagPvidOnly: tags frames by the unique PVID • untagPvidOnly: untags frames by the unique PVID • noChange: accepts frames without change
AdacPortType	Indicates how ADAC classifies the port. This is a read-only cell. Values include: <ul style="list-style-type: none"> • telephony: when Auto-Detection is enabled for the port. • telephony: auto-detection is enabled.. • callServer: port is configured as a call server • uplink: port is configured as an uplink or is part of the same trunk as the uplink port.

Table continues...

Name	Description
	<ul style="list-style-type: none"> • other: the port is not classified as either telephony, callServer, or uplink.
MacDetectionEnable	<p>Indicates whether Auto-Detection of IP phones, based on MAC address, is enabled (true) on the interface. When cleared, this indicates that Auto-Detection of IP phones, based on MAC address, is disabled on the interface.</p> <p> Important:</p> <p>MacDetectionEnable cannot be set to false if no other supported detection mechanism is enabled on the port.</p>
LldpDetectionEnable	<p>Indicates whether Auto-Detection of IP phones, based on 802.1AB, is enabled (true) or disabled (false) on the interface. When cleared, indicates that Auto- Detection of IP phones, based on 802.1AB, is disabled on the interface.</p> <p> Important:</p> <p>LLdpDetectionEnable cannot be set to False if no other supported detection mechanism is enabled on the port.</p>

ADAC MAC address range configuration using EDM

Use the information in this section to manage the ADAC MAC address range table.

Displaying the MAC address range table using EDM

Use this procedure to display the MAC address range table.

Procedure

1. In the navigation tree, double-click **Edit**.
2. Double-click **ADAC** to open the Chassis work area.
3. Select the **ADAC MAC Ranges** tab.

ADAC MAC Ranges field descriptions

The following table describes the fields on the ADAC MAC Ranges tab.

Name	Description
MacAddrRangeLowEndIndex	Indicates the low-end MAC address of the range.
MacAddrRangeHighEndIndex	Indicates the high-end MAC address of the range.

Creating MAC address ranges using EDM

Use this procedure to add new MAC address ranges to the ADAC MAC address range table.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **ADAC**.
3. Click the **ADAC MAC Ranges** tab.
4. Click **Insert**.
5. In the **MacAddrRangeLowEndIndex** box, type the MAC address for the low end of the IP Phone MAC address range.
6. In the **MacAddrRangeHighEndIndex** box, type the MAC address for the high end of the IP Phone MAC address range.
7. Click **Insert**.
8. On the toolbar, click **Apply**.

Deleting MAC address ranges using EDM

Use this procedure to remove MAC address ranges from the ADAC MAC address range table.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **ADAC**.
3. Click the **ADAC MAC Ranges** tab.
4. Click the MAC address range to delete.
5. Click **Delete**.
6. Click **Yes** to confirm the deletion of the MAC address range from the table.