



Nortel Ethernet Routing Switch 5500 Series

Configuration — VLANs, Spanning Tree, and Link Aggregation

Document status: Standard
Document version: 03.01
Document date: 27 August 2007

Copyright © 2005-2007, Nortel Networks
All Rights Reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks reserves the right to make changes to the products described in this document without notice.

Nortel Networks does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Nortel Networks software license agreement

This Software License Agreement ("License Agreement") is between you, the end user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other

reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: A) DAMAGES BASED ON ANY THIRD PARTY CLAIM; B) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR C) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The foregoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a) If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b) Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c) Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d) Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e) The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f) This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Revision History

Date Revised	Version	Reason for revision
July 2005	1.00	New document for Software Release 4.2.
June 2006	2.00	Document updated for Software Release 5.0.
June 2006	2.01	Minor revision for Software Release 5.0.
June 2006	2.02	Minor revision for Software Release 5.0.
July 2006	2.03	Minor revision for Software Release 5.0.
August 2007	3.01	Document updated for Software Release 5.1.

6 Revision History

Contents

Preface	15
Nortel Ethernet Routing Switch 5500 Series	15
Related Publications	16
How to get help	17
Getting help from the Nortel web site	17
Getting help over the phone from a Nortel Solutions Center	17
Getting help from a specialist using an Express Routing Code	18
Getting help through a Nortel distributor or reseller	18
Chapter 1 An Introduction to VLANs, Spanning Tree Groups, and MultiLink Trunking	19
Virtual Local Area Networks (VLAN)	19
IEEE 802.1Q Tagging	20
VLANs Spanning Multiple Switches	26
VLAN Summary	29
VLAN Configuration Rules	30
VLAN Configuration Control	31
Multinetting	32
Spanning Tree Protocol groups	32
STG Configuration Guidelines	33
Spanning Tree Fast Learning	35
STG port membership mode	35
802.1t path cost calculation	36
Rapid Spanning Tree Protocol	36
Multiple Spanning Tree Protocol	36
Interoperability with legacy STP	37
Differences in STP and RSTP port roles	37
Rapid convergent	38
Spanning Tree BPDU Filtering	40
Multilink trunks	41
Client-server configuration using multilink trunks	42
Before configuring trunks	43
MultiLink Trunking Configuration Rules	43
Adding and deleting links from existing multilink trunks	45

- How a multilink trunk reacts to losing distributed trunk members 46
- Spanning Tree Considerations for multilink trunks 47
- Port membership in MultiLink Trunking 49
- SMLT 50
 - Overview 50
 - Advantages of SMLT 51
 - How does SMLT work? 52
 - SLT 70
 - Using SMLT with SLT 71
 - SMLT and SLT Configuration steps 73
- IEEE 802.3ad Link Aggregation 86
 - Link aggregation rules 87
 - LACP port mode 88
- VLACP 89
 - Virtual LACP (VLACP) overview 89
 - VLACP features 91

Auto-Detection and Auto-Configuration of Nortel IP Phones 93

- ADAC operation 94
 - Auto-Detection of Nortel IP Phones 94
 - Auto-Detection by MAC address 95
 - Auto-Detection by LLDP (IEEE 802.1ab) 96
 - Auto-Configuration of Nortel IP Phones 97
 - Initial user settings 98
 - Operating modes 99
 - ADAC and stacking 104
 - ADAC and LACP enabled on an Uplink port 105
 - ADAC and EAP configuration 106
 - ADAC user Restrictions 107
- ADAC management 107

Creating and Managing VLANs 109

- VLAN Support 109
- Creating and Managing VLANs using the CLI 109
 - show vlan command 110
 - show vlan interface info command 111
 - show vlan interface vids command 111
 - vlan mgmt command 111
 - default vlan mgmt command 112
 - vlan create command 112
 - vlan delete command 113
 - no vlan command 113
 - vlan name command 114
 - auto-pvid command 114
 - no auto-pvid command 114

vlan ports command	114
vlan members command	115
Configuring VLAN Configuration Control	116
Managing the MAC address forwarding database table	117
IP Directed Broadcasting	121
Configuring ADAC for Nortel IP Phones using the CLI	122
adac command (global)	123
no adac command (global)	124
default adac	124
adac command (per port settings)	125
no adac command (per port settings)	126
default adac command (per port settings)	126
adac detection command	127
no adac detection command	127
default adac detection command	128
adac port enable command	128
no adac port enable command	128
default adac port enable	129
adac mac-range-table command	129
no adac mac-range-table command	129
default adac mac-range-table command	130
show adac command	130
show adac interface command	130
show adac mac-range-table command	131
show adac detection interface command	131
ADAC UFA configuration example	131
ADAC configuration commands	133
Verifying new ADAC settings	133
Creating and Managing VLANs using the Web-based Management Interface	135
Creating a Port-based VLAN	136
Creating a Protocol-based VLAN	137
Modifying a Port-based VLAN	141
Modifying a Protocol-based VLAN	142
Selecting a Management VLAN	144
Deleting a VLAN configuration	144
Flushing the MAC address table using Web-based management	145
Configuring ADAC for Nortel IP Phones using Web-based management	147
Configuring global ADAC properties	147
Configuring ADAC port properties	149
Configuring ADAC MAC address ranges	151
Configuring ADAC Port Detection	153
Creating and Managing VLANs using the Java Device Manager	155
Setting VLAN Configuration Control	156

Enabling AutoPVID	157
Creating a VLAN	158
Modifying a VLAN	160
Deleting VLANs	161
Configuring IGMP snooping	162
Assigning an IP address to a VLAN	163
Configuring VLAN DHCP	164
Graphing DHCP statistics	166
Configuring NSNA per VLAN	166
Deleting an NSNA VLAN	168
Filtering an NSNA VLAN	169
MAC address table maintenance using the Device Manager	170
Flushing the MAC address table	170
Configuration of ADAC for Nortel IP Phones using Device Manager	171

Configuring Spanning Tree Protocol **179**

Configuring Spanning Tree using the Console Interface	179
Spanning Tree configuration in STPG mode	180
Spanning Tree configuration in RSTP mode	190
Spanning Tree configuration in MSTP mode	198
Spanning Tree VLAN Membership screen in MSTP mode	208
Setting the STP mode using the CLI	209
spanning-tree op-mode	209
Configuring STP BPDU Filtering using the CLI	209
Creating and Managing STGs using the CLI	210
spanning-tree cost-calc-mode command	211
spanning-tree port mode command	211
show spanning-tree command	211
spanning-tree stp create command	212
spanning-tree stp delete command	212
spanning-tree stp enable command	213
spanning-tree stp disable command	213
spanning-tree command	213
default spanning-tree command	214
spanning-tree add-vlan command	215
spanning-tree remove-vlan command	215
spanning-tree command by port	216
default spanning-tree command by port	217
no spanning-tree command by port	218
Managing RSTP using the CLI	218
spanning-tree rstp command	219
spanning-tree rstp port command	219
show spanning-tree rstp command	220
show spanning-tree rstp port command	221

Managing MSTP using the CLI	221
spanning-tree mstp command	222
spanning-tree mstp port command	223
spanning-tree mstp region command	224
spanning-tree mstp msti command	224
no spanning-tree mstp msti enable command	225
no spanning-tree mstp msti command	225
show spanning-tree mstp command	225
show spanning-tree mstp port command	226
show spanning-tree mstp msti command	226
Setting the STP mode using the Web-based Management Interface	227
Creating and Managing STGs using the Web-based Management Interface	228
Creating a Spanning Tree Group	228
Modifying a Spanning Tree Group	230
Deleting a Spanning Tree Group	231
Associating an STG with VLAN Membership	231
Spanning Tree Port Configuration	233
Modifying STG Bridge Information	235
Configuring RSTP using Web-based management	238
Configuring RSTP bridge settings	238
Configuring RSTP port settings	240
Configuring MSTP using Web-based management	241
Creating MSTI instances	242
Configuring MSTI bridge settings	243
Configuring CIST bridge settings	244
Adding VLANs to the MSTI	246
Configuring Cist ports	248
Configuring MSTI port properties	250
Setting the STP mode using Device Manager	252
Configuring STP BPDU Filtering using Device Manager	252
Creating and Managing STGs using Device Manager	253
Configuring STG global properties	254
Creating an STG	255
Adding a VLAN to an STG	257
Moving a VLAN between STGs	258
Deleting an STG	258
Displaying STG Status	258
Displaying STG ports	259
Configuring RSTP using Device Manager	263
Configuring MSTP using Device Manager	271

MultiLink Trunking (MLT)

289

Trunk groups	289
Creating and Managing MLTs using the CLI	290

- show mlt command 290
- mlt command 290
- no mlt command 291
- show mlt spanning-tree command 291
- mlt spanning-tree command 291
- Creating and Managing MLTs using the Web-based Management Interface 292
 - Creating a multilink trunk 292
 - Configuring Spanning Tree Group Participation 294
 - Monitoring an MLT 295
- Creating and Managing MLTs using the Java Device Manager 296
 - Setting up MLTs 296
 - Adding MLT Ports 300
- Configuring SMLT using the CLI 301
 - interface mlt command 301
 - smlt command 302
 - ist command 302
 - smlt command 303
 - no smlt command 303
 - no ist command 304
 - no smlt command 304
 - default smlt command 304
 - default ist command 304
 - default smlt command 305
 - show ist command 305
 - show ist stat command 305
 - show smlt command 306
- Configuring an SMLT using Device Manager 307
 - Adding an MLT-based SMLT 307
 - Viewing SLTs configured on your switch 308
 - Configuring an IST MLT 309
 - Removing an IST MLT 311
 - Viewing IST statistics 311
 - Configuring an SLT 313
 - Deleting an SLT 315
- Troubleshooting IST problems 316
 - Troubleshooting IST problems 316

Configuring LACP and VLACP 319

- Configuring LACP and VLACP using the CLI 319
 - Configuring Link Aggregation using the CLI 319
 - Configuring VLACP using the CLI 325
- Configuring LACP and VLACP using Device Manager 331
 - Configuring LACP using Device Manager 331
 - Configuring VLACP using Device Manager 335

Configuring LACP using Web-based management	338
Bridge Configuration page	339
Port Configuration page	339
Port Statistics page	340

Index

343

Preface

This guide provides information and instructions on the configuration of Virtual Local Area Networks (VLANs), Spanning Tree Protocol (STP), and MultiLink Trunking (MLT) on the Nortel Ethernet Routing Switch 5500 Series. Please consult any documentation included with the switch and the product release notes (see "[Related Publications](#)" ([page 16](#))) for any errata before beginning the configuration process.

Nortel Ethernet Routing Switch 5500 Series

"[5500 Series Switch Platforms](#)" ([page 15](#)) outlines the switches that are part of the 5500 Series of Nortel Ethernet Routing Switches.

5500 Series Switch Platforms

5500 Series Switch Model	Key Features
Nortel Ethernet Routing Switch 5510-24T	A 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains two shared SFP ports.
Nortel Ethernet Routing Switch 5510-48T	A 48 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains two shared SFP ports.
Nortel Ethernet Routing Switch 5520-24T-PWR	A 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch with full Power over Ethernet (PoE) capability on all copper ports. This switch contains four shared SFP ports.
Nortel Ethernet Routing Switch 5520-48T-PWR	A 48 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch with full Power over Ethernet (PoE) capability on all copper ports. This switch contains four shared SFP ports.
Nortel Ethernet Routing Switch 5530-24TFD	A 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains twelve shared SFP ports and two XFP ports.

Related Publications

For more information about the management, configuration, and usage of the Nortel Ethernet Routing Switch 5500 Series, refer to the publications listed in "[Nortel Ethernet Routing Switch 5500 Series Documentation](#)" (page 16).

Nortel Ethernet Routing Switch 5500 Series Documentation

Title	Description	Part Number
<i>Nortel Ethernet Routing Switch 5500 Series Installation</i>	Instructions for the installation of a switch in the Nortel Ethernet Routing Switch 5500 Series. It also provides an overview of hardware key to the installation, configuration, and maintenance of the switch.	NN47200-300
<i>Nortel Ethernet Routing Switch 5500 Series Configuration — System</i>	Instructions for the general configuration of switches in the 5500 Series that are not covered by the other documentation.	NN47200-500
<i>Nortel Ethernet Routing Switch 5500 Series Configuration — Security</i>	Instructions for the configuration and management of security for switches in the 5500 Series.	NN47200-501
<i>Nortel Ethernet Routing Switch 5500 Series Configuration — VLANs, Spanning Tree, and Link Aggregation</i>	Instructions for the configuration of spanning and trunking protocols on 5500 Series switches.	NN47200-502
<i>Nortel Ethernet Routing Switch 5500 Series Configuration — IP Routing Protocols</i>	Instructions for the configuration of IP routing protocols on 5500 Series switches.	NN47200-503
<i>Nortel Ethernet Routing Switch 5500 Series Configuration — Quality of Service</i>	Instructions for the configuration and implementation of QoS on 5500 Series switches.	NN47200-504
<i>Nortel Ethernet Routing Switch 5500 Series Configuration — System Monitoring</i>	Instructions for the configuration, implementation, and usage of system monitoring on 5500 Series switches.	NN47200-505
<i>Nortel Ethernet Routing Switch 5500 Series Release Notes — Release 5.1</i>	Provides an overview of new features, fixes, and limitations of the 5500 Series switches. Also included are any supplementary documentation and document errata.	NN47200-400

Title	Description	Part Number
<i>Installing the Nortel Ethernet Redundant Power Supply Unit 15</i>	Instructions for the installation and use of the Nortel Ethernet RPSU 15.	217070-A
<i>DC-DC Converter Module for the Baystack 5000 Series Switch</i>	Instructions for the installation and use of the DC-DC power converter.	215081-A
<i>Nortel Ethernet Routing Switch 5500 Series Installation — SFP</i>	Instructions for the installation and use of small form-factor pluggable transceivers.	NN47200-302

How to get help

This section explains how to get help for Nortel products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Chapter 1

An Introduction to VLANs, Spanning Tree Groups, and MultiLink Trunking

The Nortel Ethernet Routing Switch 5500 Series provides a robust set of tools for working with Virtual Local Area Networks (VLAN), Spanning Tree Protocol (STP) and MultiLink Trunking (MLT). This chapter provides an introduction to these concepts and gives a general overview of switch capabilities. Subsequent chapters provide a more detailed description of switch capabilities and how to configure them on the switch.

This chapter contains information about the following topics:

- "Virtual Local Area Networks (VLAN)" (page 19)
- "Spanning Tree Protocol groups" (page 32)
- "Rapid Spanning Tree Protocol" (page 36)
- "Multiple Spanning Tree Protocol" (page 36)
- "Multilink trunks" (page 41)
- "SMLT" (page 50)
- "IEEE 802.3ad Link Aggregation" (page 86)
- "VLACP" (page 89)

Virtual Local Area Networks (VLAN)

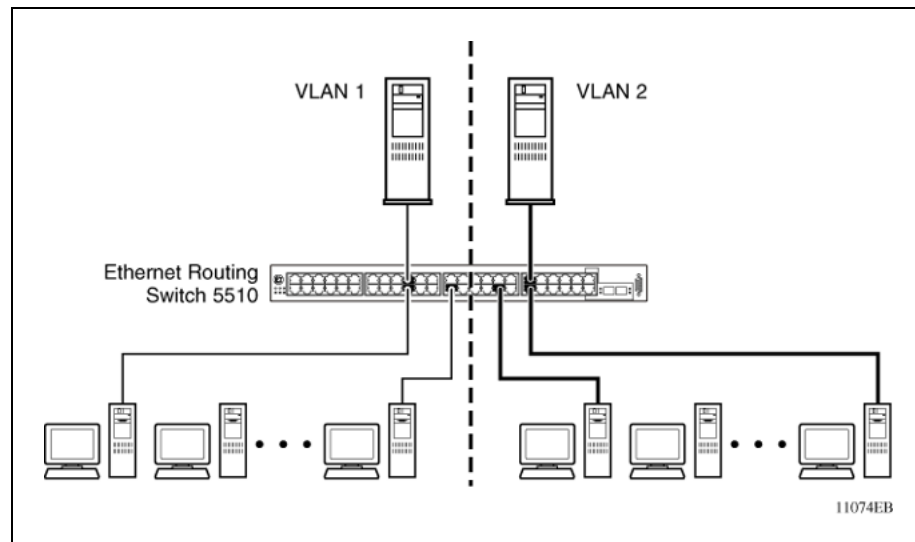
The Nortel Ethernet Routing Switch 5500 Series supports up to 256 VLANs.

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.

Setting up virtual LANs (VLAN) is a way to segment networks to increase network capacity and performance without changing the physical network topology ("[Port-based VLAN](#)" (page 20)). With network segmentation, each

switch port connects to a segment that is a single broadcast domain. When you configure a switch port to be a member of a VLAN, you add it to a group of ports (workgroup) that belong to one broadcast domain.

Port-based VLAN



The Nortel Ethernet Routing Switch 5500 Series allows ports to be assigned to VLANs using the Command Line Interface, Web-based Management Interface, or the Java Device Manager. Different ports (and their devices) can be assigned to different broadcast domains. This feature provides network flexibility because VLANs can be reassigned to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.

IEEE 802.1Q Tagging

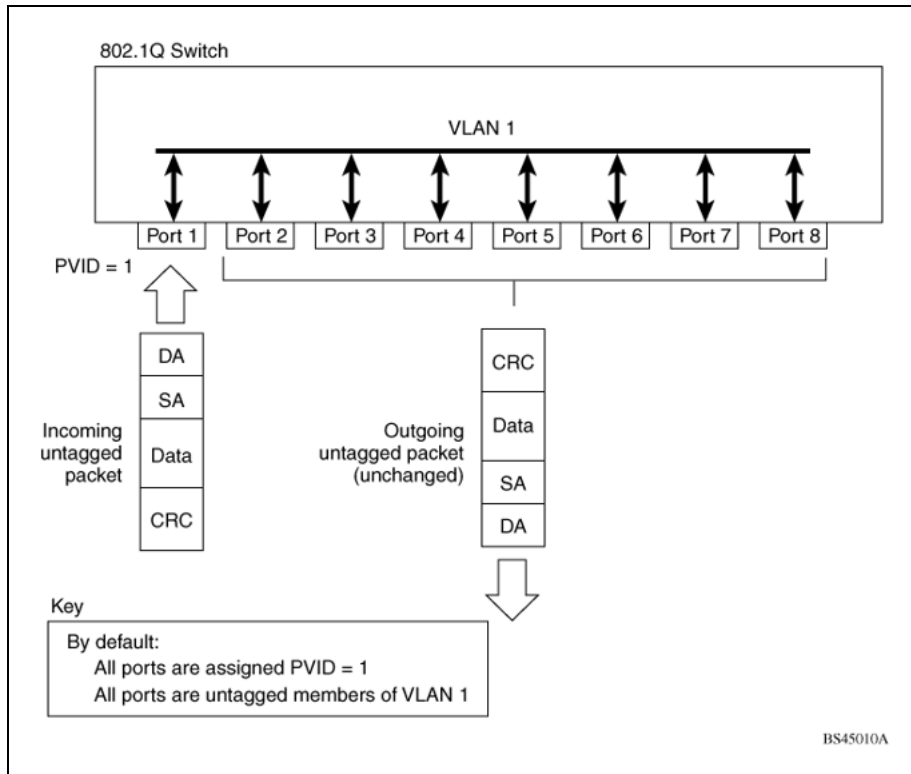
The Nortel Ethernet Routing Switch 5500 Series operates in accordance with the IEEE 802.1Q tagging rules. Important terms used with the 32-bit 802.1Q tagging feature are:

- VLAN identifier (VID) -- the 12-bit portion of the VLAN tag in the frame header that identifies an explicit VLAN. When other types of VLANs are enabled, this default value can be overridden by the values enabled in the management interfaces.
- Port VLAN identifier (PVID) -- a classification mechanism that associates a port with a specific VLAN. For example, a port with a PVID of 3 (PVID =3) assigns all untagged frames received on this port to VLAN 3.
- Tagged frame -- a frame that contains the 32-bit 802.1q field (VLAN tag). This field identifies the frame as belonging to a specific VLAN.
- Untagged frame -- a frame that does not carry any VLAN tagging information in the frame header.

- VLAN port members -- a group of ports that are all members of a particular VLAN. A port can be a member of one or more VLANs.
- Untagged member -- a port that has been configured as an untagged member of a specific VLAN. When an untagged frame exits the switch through an untagged member port, the frame header remains unchanged. When a tagged frame exits the switch through an untagged member port, the tag is stripped and the tagged frame is changed to an untagged frame.
- Tagged member -- a port that has been configured as a tagged member of a specific VLAN. When an untagged frame exits the switch through a tagged member port, the frame header is modified to include the 32-bit tag associated with the ingress port PVID. When a tagged frame exits the switch through a tagged member port, the frame header remains unchanged (original VID remains).
- User priority -- a three-bit field in the header of a tagged frame. The field is interpreted as a binary number, therefore has a value of 0 - 7. This field allows the tagged frame to carry the user-priority across bridged LANs where the individual LAN segments may be unable to signal priority information.
- Port priority -- the priority level assigned to untagged frames received on a port. This value becomes the user priority for the frame. Tagged packets get their user priority from the value contained in the 32-bit 802.1Q frame header.
- Unregistered packet -- a tagged frame that contains a VID where the receiving port is not a member of that VLAN.
- Filtering database identifier (FID) -- the specific filtering/forwarding database within the Nortel Ethernet Routing Switch 5500 Series switch that is assigned to each VLAN. Each VLAN has its own filtering database, which is called independent VLAN learning (IVL). IVLs can have duplicate MAC addresses in different VLANs.

The default configuration settings for the Nortel Ethernet Routing Switch 5500 Series have all ports set as untagged members of VLAN 1 with all ports configured as PVID = 1. Every VLAN is assigned a unique VLAN identifier (VID) that distinguishes it from all other VLANs. In the default configuration example shown in "[Default VLAN Settings](#)" (page 22), all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID =1). Untagged packets enter and leave the switch unchanged.

Default VLAN Settings

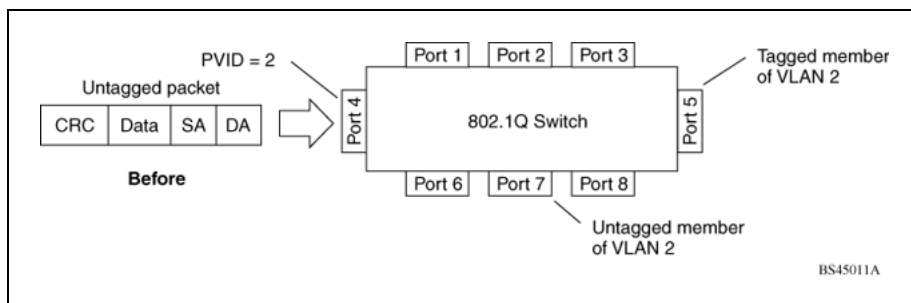


Switch ports can be configured to transmit frames tagged on some VLANs, and untagged on other VLANs.

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

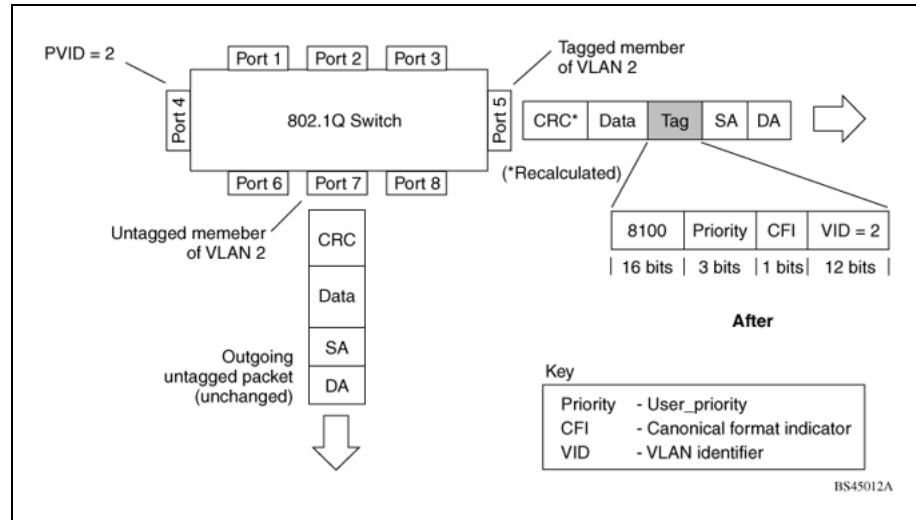
In "Port-based VLAN assignment" (page 22), untagged incoming packets are assigned directly to VLAN 2 (PVID = 2). Port 5 is configured as a *tagged* member of VLAN 2, and port 7 is configured as an *untagged* member of VLAN 2.

Port-based VLAN assignment



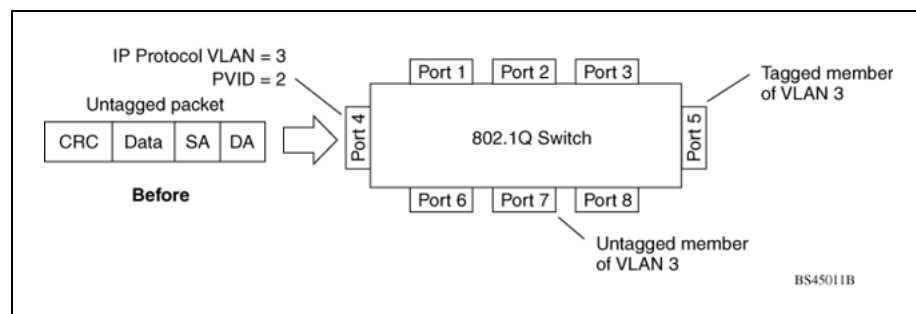
As shown in "802.1Q tagging (after port-based VLAN assignment)" (page 23), the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.

802.1Q tagging (after port-based VLAN assignment)



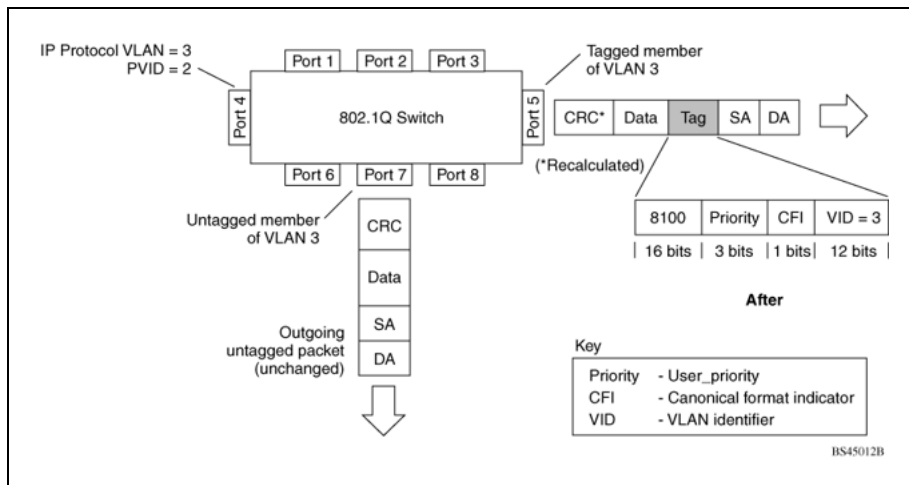
In "Protocol-based VLAN assignment" (page 23), untagged incoming packets are assigned to VLAN 3 (protocol-based VLAN = 3, PVID = 2). Port 5 is configured as a tagged member of VLAN 3, and port 7 is configured as an untagged member of VLAN 3.

Protocol-based VLAN assignment



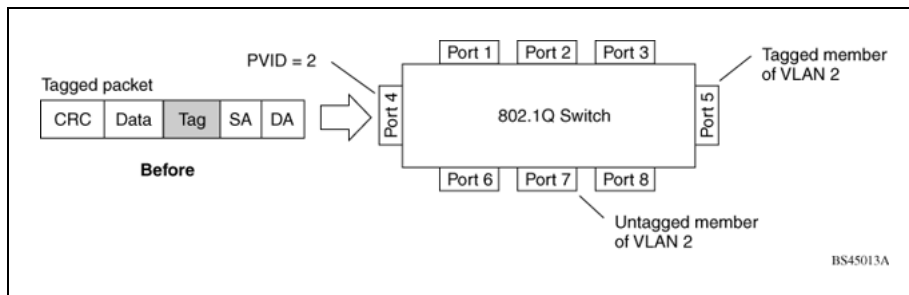
As shown in "802.1Q tagging (after protocol-based VLAN assignment)" (page 24), the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of VLAN 3. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of VLAN 3.

802.1Q tagging (after protocol-based VLAN assignment)

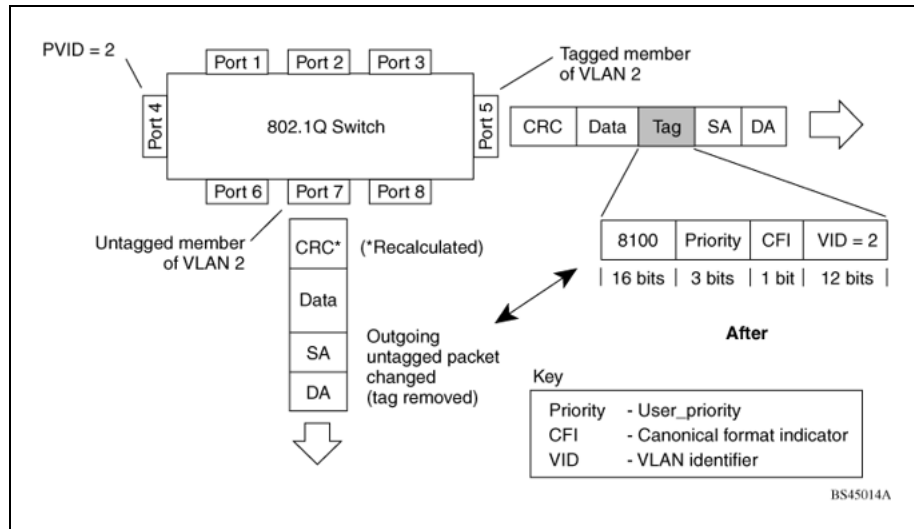


In "802.1Q tag assignment" (page 24), tagged incoming packets are assigned directly to VLAN 2 because of the tag assignment in the packet. Port 5 is configured as a tagged member of VLAN 2, and port 7 is configured as an untagged member of VLAN 2.

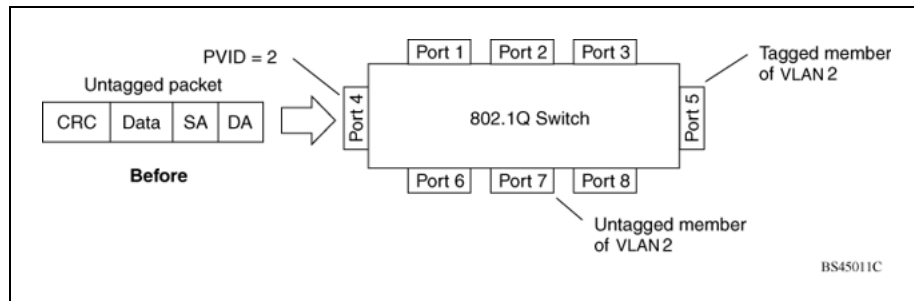
802.1Q tag assignment



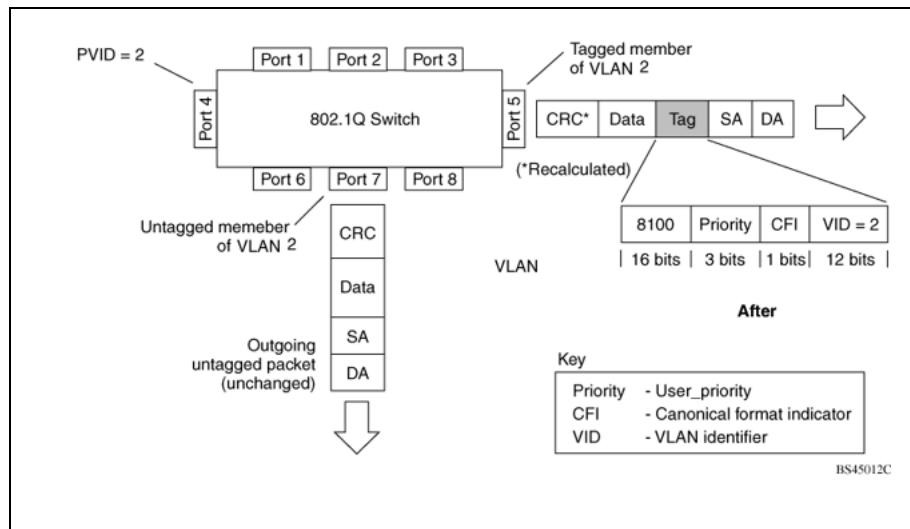
As shown in "802.1Q tagging (after 32-bit 802.1Q tag assignment)" (page 25), the tagged packet remains unchanged as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. However, the tagged packet is stripped (untagged) as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.

802.1Q tagging (after 32-bit 802.1Q tag assignment)

In "802.1Q tag assignment" (page 25), untagged incoming packets are assigned directly to VLAN 2. Port 5 is configured as a tagged member of VLAN 2, and port 7 is configured as an untagged member of VLAN 2.

802.1Q tag assignment

As shown in "802.1Q tagging (after 30-bit 802.1Q tag assignment)" (page 26), 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.

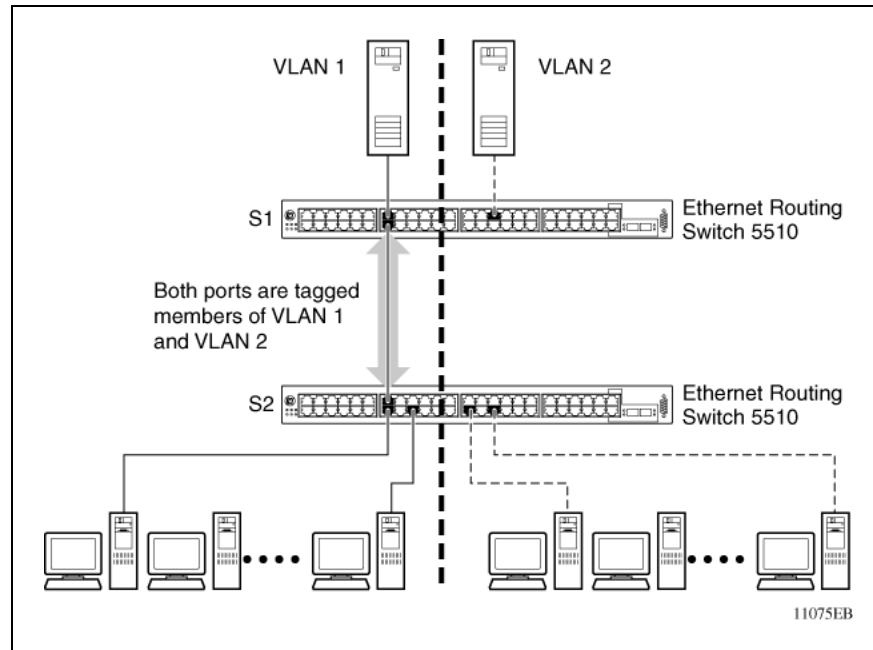
802.1Q tagging (after 30-bit 802.1Q tag assignment)**VLANs Spanning Multiple Switches**

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

With 32-bit 802.1Q tagging enabled on a port for a VLAN, all frames leaving the port for that VLAN are marked as belonging to that specific VLAN. Specific switch ports can be assigned 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

"VLANs spanning multiple 802.1Q tagged switches" (page 27) shows VLANs spanning two Nortel Ethernet Routing Switch 5500 Series switches. The 32-bit 802.1Q tagging is enabled on S1, port 14 and on S2, port 13 for VLAN 1 and VLAN 2. Both ports are tagged members of VLAN 1 and VLAN 2.

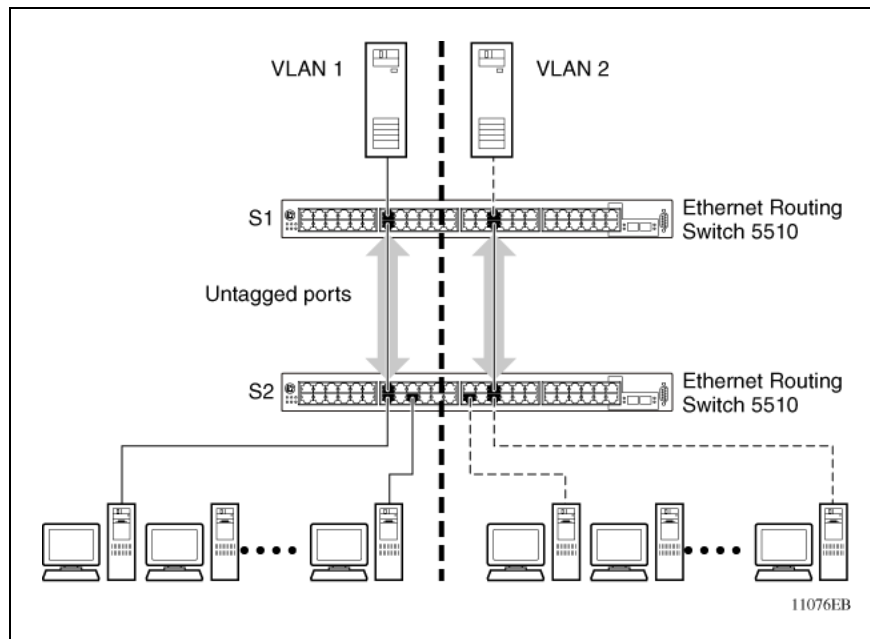
VLANs spanning multiple 802.1Q tagged switches

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

VLANs spanning multiple untagged switches

"[VLANs spanning multiple untagged switches](#)" (page 28) shows VLANs spanning multiple untagged switches. In this configuration, Switch S2 does not support 32-bit 802.1Q tagging and you must use a single switch port on each switch for each VLAN.

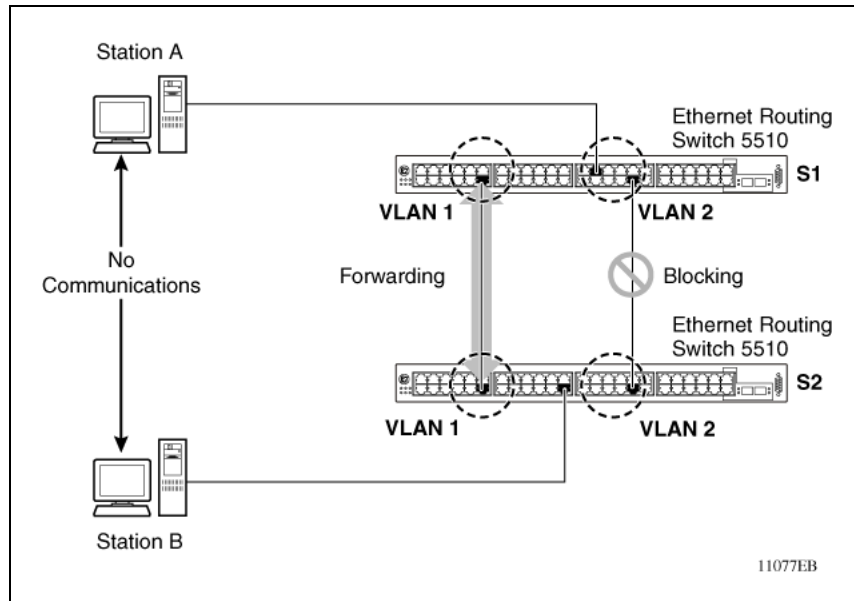
For this configuration to work properly, you must set spanning tree participation to Disabled (the STP is not supported across multiple LANs).

VLANs spanning multiple untagged switches

When the STP is enabled on these switches, only one link between the pair of switches forwards traffic. Because each port 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. ["Possible problems with VLANs and Spanning Tree Protocol"](#) (page 29) shows possible consequences of enabling the STP when using VLANs between untagged (non-802.1Q tagged) switches.

Possible problems with VLANs and Spanning Tree Protocol



As shown in "Possible problems with VLANs and Spanning Tree Protocol" (page 29), with STP enabled, only one connection between Switch S1 and Switch S2 is forwarding at any time. Communications failure occurs between VLAN 2 of S1 and VLAN 2 of S2, blocking communications between Stations A and B.

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

VLAN Summary

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

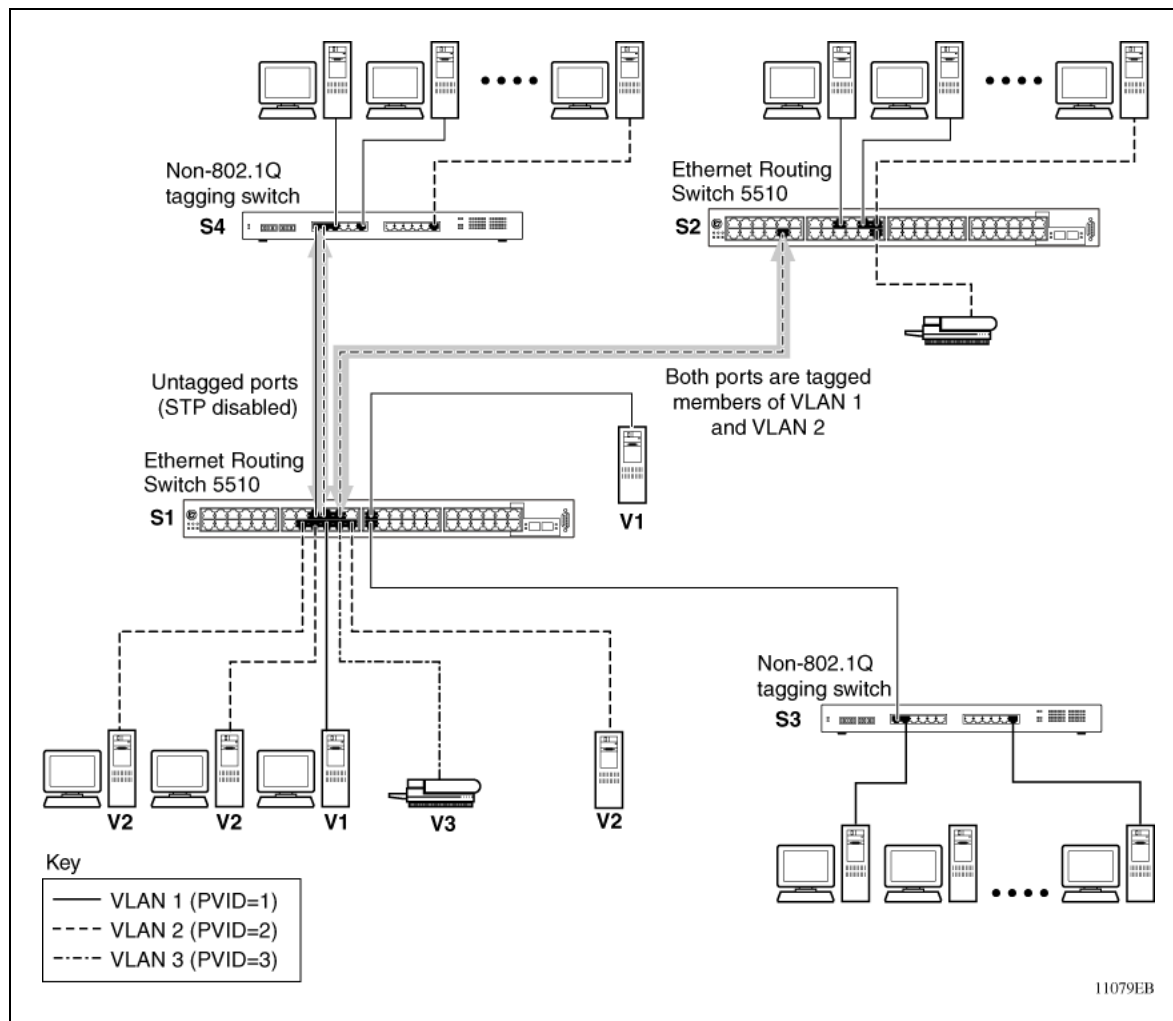
As shown in "VLAN configuration spanning multiple switches" (page 30), Switch S1 (Nortel Ethernet Routing Switch 5510) is configured with multiple VLANs:

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

Because S4 does not support 32-bit 802.1Q tagging, a single switch port on each switch must be used for each VLAN (see "VLANs spanning multiple untagged switches" (page 28)).

The connection to S2 requires only one link between the switches because S1 and S2 are both Nortel Ethernet Routing Switch 5500 Series switches that support 32-bit 802.1Q tagging (see " VLANs spanning multiple 802.1Q tagged switches" (page 26)).

VLAN configuration spanning multiple switches



VLAN Configuration Rules

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

- If a port is a trunk group member, all trunk members are added or deleted from the VLAN.
- All ports involved in trunking must have the same VLAN configuration.
- VLANs are not dependent on Rate Limiting settings.

- If a port is an Internet Gateway Management Protocol (IGMP) member on any VLAN, and is removed from a VLAN, the port's IGMP membership is also removed.
- If you add a port to a different VLAN, and it is already configured as a static router port, you configure the port as an IGMP member on that specific VLAN.

VLAN Configuration Control

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

VLAN Configuration Control offers four options for controlling VLAN modification:

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

Note: 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. 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 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. Using this option an untagged port can have membership in multiple VLANs.
4. **Flexible** -- This option functions in a similar manner to disabling AutoPVID functionality. When this option is used, an untagged port can belong to an unlimited number of VLANs. Any new additions of an untagged port to a new VLAN does not change the PVID of that port.

VLAN Configuration Control is only applied to ports with the tagging modes of **Untag All** and **Tag PVID Only**. Ports with the tagging modes of **Tag All** and **Untag PVID Only** are not governed by VLAN Configuration Control.

Ports with the tagging modes of **Tag All** and **Untag PVID Only** can belong to multiple VLANs regardless of VLAN Configuration Control settings and must have their PVID manually changed.

Multinetting

The Nortel Ethernet Routing Switch 5500 Series supports the definition and configuration of secondary interfaces on each VLAN. For more information about IP Multinetting, refer to *Nortel Ethernet Routing Switch 5500 Series Configuration - IP Routing Protocols*, part number NN47200-503.

Spanning Tree Protocol groups

The Nortel Ethernet Routing Switch 5500 Series supports the Spanning Tree Protocol (STP) as defined in IEEE 802.1D. The Spanning Tree Protocol detects and eliminates logical loops in a bridged or switched network. When multiple paths exist, the spanning tree algorithm configures the network so that a bridge or switch uses only the most efficient path. If that path fails, the protocol automatically reconfigures the network to make another path become active, thus sustaining network operations.

The Nortel Ethernet Routing Switch 5500 Series supports multiple spanning tree groups (STG). The Nortel Ethernet Routing Switch 5500 Series supports a maximum of 8 STGs, either all in one stand-alone switch or across a stack. Multiple STGs provide multiple data paths, which can be used for load-balancing and redundancy. Load balancing is enabled between two switches using multiple STGs by configuring each path with a different VLAN and then assigning each VLAN to a separate STG. Each STG is independent. Each STG sends its own Bridge Protocol Data Units (BPDU), and each STG must be independently configured.

The STG, or bridge group, forms a loop-free topology that includes one or more virtual LANs (VLAN). The Nortel Ethernet Routing Switch 5500 Series supports multiple instances (8) of STGs running simultaneously.

The Nortel Ethernet Routing Switch 5500 Series supports a maximum of 256 VLANs. With a maximum of 8 STGs, on average, each STG can have 32 VLANs.

In the default configuration of the Nortel Ethernet Routing Switch 5500 Series, a single STG with the ID of 1 includes all ports on the switch. This STG is the default STG. Although ports can be added to or deleted from the default STG, the default STG (STG1) itself cannot be deleted from the system. Also you cannot delete the default VLAN (VLAN1) from STG1.

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

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

All other STGs, except the Default STG, must be created by the user. To become active, each STG must be enabled by the user after creation. Each STG is assigned an ID number from 2 to 8 (the Default STG is assigned the ID number 1). Ports or VLANs are assigned to an active STG. However, a port that is not a member of a VLAN is not allowed to join an STG.

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

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

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

Note 1: If a unique multicast address for an STG is configured, each device in that STG must also be configured with the same spanning tree multicast address.

Note 2: If Virtual LACP is enabled, the number of unique multicast addresses that can be configured for STGs is reduced to 3 (1 to 3).

STG Configuration Guidelines

This section provides important information about configuring STGs:

- An STG must be created by following these steps:
 - Create the STG
 - Add the existing VLAN and port memberships
 - Enable the STG
- When a VLAN is created, that VLAN automatically belongs to STG 1, the default STG. If the VLAN is to be in another STG, it must be moved by assigning it to another STG.
- A newly created VLAN must be moved to an existing STG by following these steps:

- Create the VLAN
- Add the VLAN to an existing STG
- VLAN1 cannot be moved or deleted from STG1.
- You can create and add VLAN X directly to STG Y with `vlan create x type port y` from the CLI if STG Y exists.
- VLANs must be contained within a single STG; a VLAN cannot span multiple STGs. By confining VLANs within a single STG, you avoid problems with spanning tree blocking ports and causing a loss of connectivity within the VLAN. When a VLAN spans multiple switches, the VLAN must be within the same spanning tree group (have the same STG ID) across all the switches.
- A port that is not a member of any VLAN cannot be added to any STG. The port must be added to a VLAN, and that VLAN added to the desired STG.
- Tagged ports can belong to more than one STG, but untagged ports can belong to only one STG.
- When a tagged port belongs to more than one STG, the egress BPDUs are tagged to distinguish the BPDUs of one STG from those of another STG.
- Because some STP-compliant devices do not support tagging, you can configure whether to send tagged or untagged BPDUs, even from tagged ports. The VLAN ID for the tagged BPDUs is 4000+STG ID.
- The default VLAN ID for tagged BPDUs is as follows:
 - 4001--STG1
 - 4002--STG2
 - 4003--STG3
 - 4004--STG4
 - 4005--STG5
 - 4006--STG6
 - 4007--STG7
 - 4008--STG8
- A VLAN ID can be selected for tagged BPDUs for each STG. Valid VLAN IDs are 1 to 4094.
- Tagged BPDUs cannot use the same VID as an active VLAN.
- An untagged port cannot span multiple STGs.

- When a port is removed from a VLAN that belongs to an STG, that port is also removed from the STG. However, if that port belongs to another VLAN in the same STG, the port remains in the STG.
- As an example, assume that port 1 belongs to VLAN1, and that VLAN1 belongs to STG1. When you remove port 1 from VLAN1, port 1 is also removed from STG1.

However, if port 1 belongs to both VLAN1 and VLAN2 and both VLANs belong to STG1, removing port 1 from VLAN1 does not remove port 1 from STG1 because VLAN2 is still a member of STG1.

An STG cannot be deleted until you disable it.

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

Spanning Tree Fast Learning

Spanning Tree Fast Learning is an enhanced port mode supported by the Nortel Ethernet Routing Switch 5500 Series. If Spanning Tree Fast Learning is enabled on a port with no other bridges, the port is brought up more quickly after a switch initialization or a spanning tree change. The port goes through the normal blocking and learning states before the forwarding state, but the hold times for these states is the bridge hello timer (2 seconds by default) instead of the bridge forward delay timer (15 seconds by default).

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

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

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

STG port membership mode

In release 5.0 software and later, IEEE 802.1D STGs support two different STP port membership modes: normal and auto. In the normal mode, when a port is assigned to VLAN X and VLAN X is in STP group Y, the port does not automatically become a member of STP group Y. In the auto mode, when a port is assigned to VLAN X and VLAN X is in STP group Y, the port automatically becomes a member of STP group Y.

To set the STG port membership mode using the CLI, see "[spanning-tree port mode command](#)" (page 211) and using JDM, see "[Configuring STG global properties](#)" (page 254).

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.

To set the path cost calculation mode for the switch, see "[spanning-tree cost-calc-mode command](#)" (page 211).

Rapid Spanning Tree Protocol

The standard Spanning Tree implementation in 5500 Series switches is based on IEEE 802.1d, which is slow to respond to a topology change in the network (for example, a dysfunctional link in a network).

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

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

Multiple Spanning Tree Protocol

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

RSTP and MSTP enable the 5500 Series switch to achieve the following:

- Reduction of converging time from 30 seconds to less than 1 or 2 seconds when a topology change occurs in the network (that is, the port going up or down).
- Elimination of unnecessary flushing of the MAC database and flooding of traffic to the network with a new Topology Change mechanism.
- Backward compatibility with other switches that are running legacy 802.1d STP or Nortel MSTG (STP group 1 only).

- Under MSTP mode, simultaneous support of eight instances of RSTP. Instance 0 or CIST is the default group, which includes default VLAN 1. Instances 1 to 7 are called MSTIs 1-7.
- Ability to run Nortel MSTG, RSTP, or MSTP.

Interoperability with legacy STP

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

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

Differences in STP and RSTP port roles

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

"Differences in port roles for STP and RSTP" (page 37) lists the differences in port roles for STP and RSTP. STP supports 2 port roles, while RSTP supports four port roles.

Differences in port roles for STP and RSTP

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

Edged Port

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

Path cost values

RSTP and MSTP recommend new path cost values that support a wide range of link speeds. "Recommended path cost values" (page 38) lists the recommended path cost values.

Recommended path cost values

Link speed	Recommended value
Less than or equal to 100 Kbit/s	200 000 000
1 Mbit/s	20 000 000
10 Mbit/s	2 000 000
100 Mbit/s	200 000
1 Gbit/s	20 000
10 Gbit/s	2 000
100 Gbit/s	200
1 Tbit/s	20
10 Tbit/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 moves to the Forwarding State without any delay. This procedure is called the Negotiation Process.

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

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

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

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

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

Switch A is the Root.

Negotiation Process

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

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

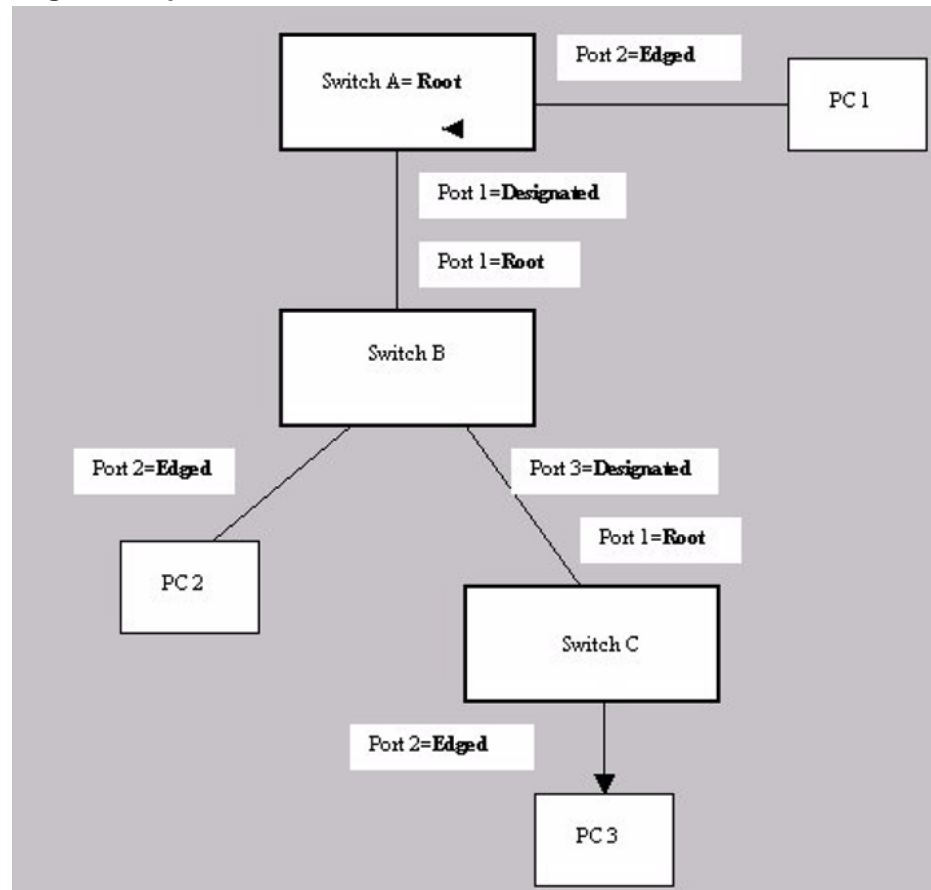
Switch A starts the negotiation process by sending a BPDU with a proposal bit set.

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

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

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

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

Negotiation process

The RSTP convergent time depends on how quickly the switch can exchange BPDUs during the negotiation process, and the number of switches in the network. For a 5500 Series switch, the convergent time depends on the hardware platform and the number of active applications running on the switch.

Spanning Tree BPDU Filtering

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

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

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

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

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

Note: The STP BPDU-Filtering feature is not supported on MultiLink 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.

For details on configuring BPDU Filtering, refer to: "[Configuring STP BPDU Filtering using the CLI](#)" (page 209) and "[Configuring STP BPDU Filtering using Device Manager](#)" (page 252).

Multilink trunks

With multilink trunks, you can group up to eight switch ports together to form a link to another switch or server, thus increasing aggregate throughput of the interconnection between the devices (up to 8 Gigabits

in full-duplex mode). Up to 32 multilink trunks can be configured. The trunk members can reside on a single unit or on multiple units within the same stack configuration as a distributed trunk. MultiLink Trunking software detects misconfigured (or broken) trunk links and redirects traffic on the misconfigured or broken trunk link to other trunk members within that trunk.

The Command Line Interface (CLI), Web-based Management Interface, or Java Device Manager (JDM) can be used to create switch-to-switch and switch-to-server multilink trunk links.

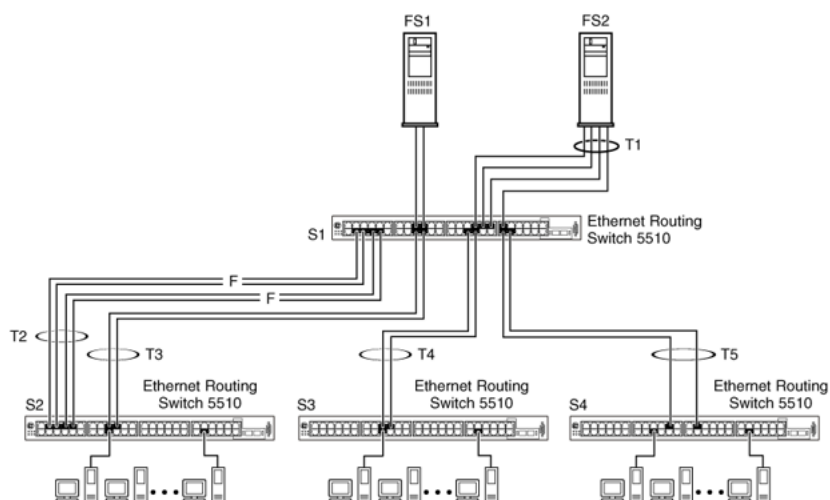
Client-server configuration using multilink trunks

"Client/server configuration example" (page 42) shows an example of how MultiLink Trunking can be used in a client/server configuration. In this example, both servers connect directly to Switch S1. FS2 is connected through a trunk configuration. The switch-to-switch connections are through trunks.

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

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

Client/server configuration example



Before configuring trunks

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

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

1. Read the configuration rules provided in the next section, "[MultiLink Trunking Configuration Rules](#)" (page 43).
2. Determine which switch ports (up to eight) are to become trunk members (the specific ports making up the trunk). A minimum of two ports are required for each trunk.

Note: With release 5.0 software, disabled ports can belong to MLTs. For traffic to flow to your configured MLT ports, be sure they are enabled.

3. Ensure that the trunk member ports have the same VLAN configuration.
4. To avoid configuration errors, all network cabling must be complete and stable before configuring any trunks.

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

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

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

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

MultiLink Trunking Configuration Rules

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

- With release 5.0 software, disabled ports can belong to MLTs. For traffic to flow to your configured MLT ports, be sure they are enabled (set to Enabled through the Port Configuration screen or through network management).
- All trunk members must have the same VLAN configuration before the Trunk Status field on the Trunk Configuration screen can be set to Enabled using the CLI.

Note: Only the first six trunks can be configured on this screen. You must use CLI, WEB or JDM to configure trunks with an ID greater than 6.

- When an active port is configured in a trunk, the port becomes a trunk member when the Trunk Status field is set to Enabled. The spanning tree parameters for the port then change to reflect the new trunk settings.
- If the spanning tree participation of any trunk member is changed to Enabled or Disabled, the spanning tree participation of all members of that trunk changes similarly.
- If the VLAN settings of any trunk member is changed, the VLAN settings of all members of that trunk change similarly.
- A trunk member cannot be configured as a monitor port.
- Entire trunks cannot be monitored by a monitor port; however, trunk members can be monitored.
- All trunk members must have identical Internet Gateway Management Protocol (IGMP) configurations.
- If you change the IGMP snooping configuration for any trunk member, the IGMP snooping settings for all trunk members change.
- Nortel recommends that you do not enable MAC Address Security on trunk ports.
- MLT ports can be set to participate in different STGs. They must have the same spanning tree learning in every group but not necessarily have the same learning between different groups to consistently update their state in the port driver.
- Like normal ports, MLT ports can be set to participate with different spanning tree learning for different spanning tree groups. Trunk ports that are in multiple spanning tree groups must be tagged, and all MLT members must belong to the same spanning tree group.

MLT load-balancing

Prior to release 5.0 software, MLTs were confined to MAC-based load balancing. In release 5.0 and later, you can choose between MAC-based (basic) or IP-based (advanced) load balancing. You can configure this option using the CLI.

The 5500 Series switch uses the following formula to perform MLT load-balancing:

$$\{(A \text{ XOR } B) \text{ MOD } x\}$$

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

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

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

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

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

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

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

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

Removal of MLT restrictions

With release 5.0 software and later, if any trunk member is set to Disabled (not active) through the Port Configuration screen or through network management, the trunk member is no longer removed from the trunk. The trunk member remains a disabled member of the trunk, and so no longer has to be reconfigured to rejoin the trunk. A trunk member can also now be disabled if only two trunk members exist on the trunk.

The lowest numbered port in the trunk can now be disabled as well. However, Nortel does not recommend disabling the lowest numbered port if Spanning Tree is enabled on the trunk.

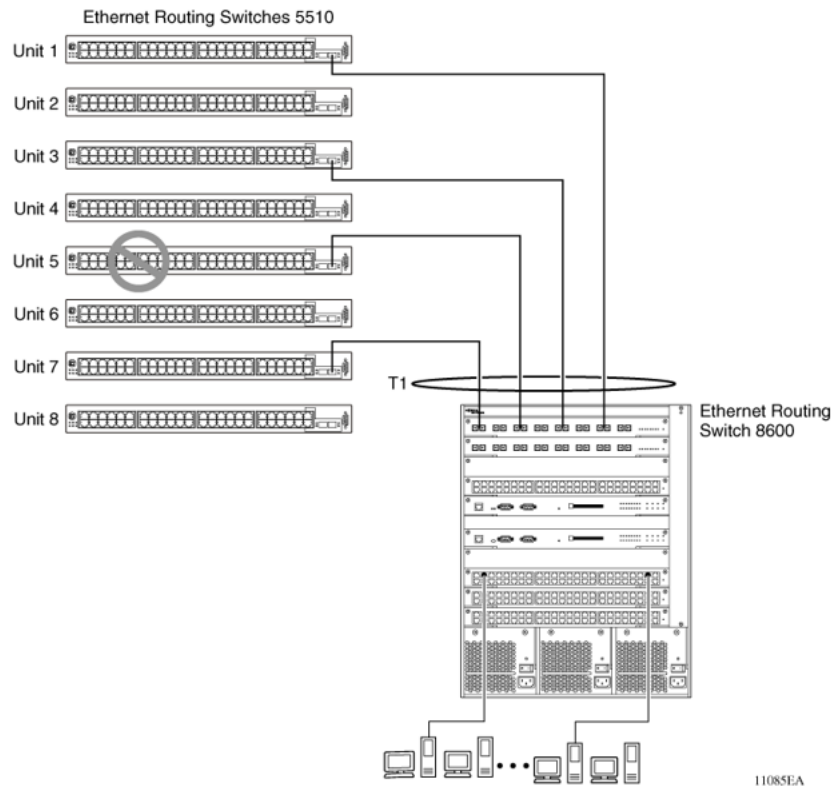
Adding and deleting links from existing multilink trunks

Ports cannot be added or removed from a Nortel Ethernet Routing Switch 5500 Series switch MLT, unless MLT is first disabled. When MLT is disabled, the ports assigned to the MLT are not disabled. The ports form separate links and create a network loop.

How a multilink trunk reacts to losing distributed trunk members

A multilink trunk (" [Loss of distributed trunk member](#)" (page 46)) can cover separate units in a stack configuration. If a unit in the stack becomes inactive due to loss of power or unit failure, the unaffected trunk members remain operational.

Loss of distributed trunk member



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

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

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

Spanning Tree Considerations for multilink trunks

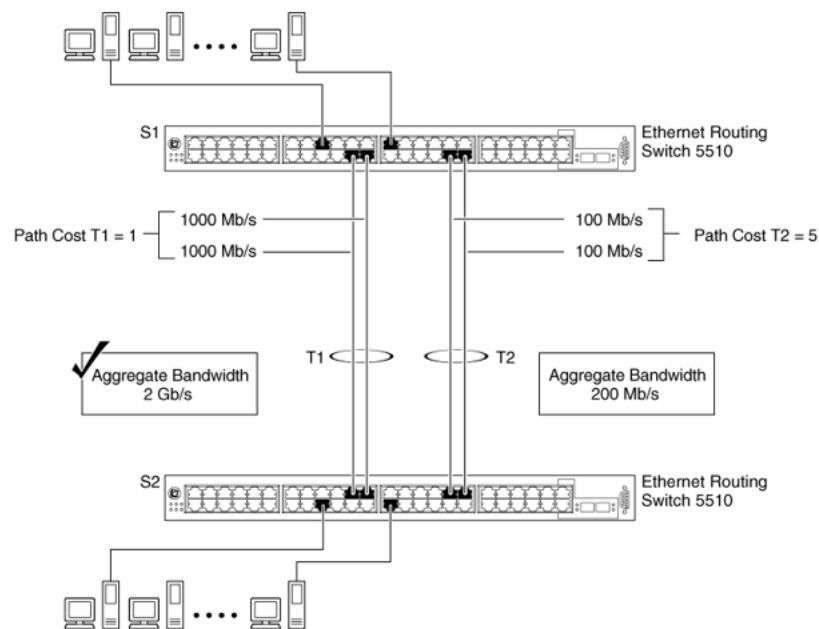
The spanning tree Path Cost parameter is recalculated based on the aggregate bandwidth of the trunk. For example, "Path Cost Arbitration" (page 47) shows a two-port trunk (T1) with two port members operating at an aggregate bandwidth of 2 GB, with a comparable Path Cost of 1. Trunk 2 has two ports at 100 Mbit/s with a Path Cost of 5.

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

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

Be careful when configuring trunks so as to not add one gigabit link physically in front of another trunk; the trunk will be blocked because they both have a Path Cost of 1.

Path Cost Arbitration



11084EA

The switch can also detect trunk member ports that are physically misconfigured. For example, in "Correctly Configured Trunk" (page 48), trunk member ports 2, 4, and 6 of Switch S1 are configured correctly to trunk member ports 7, 9, and 11 of Switch S2. The Spanning Tree Port Configuration screen for each switch shows the port state field for each port in the Forwarding state.

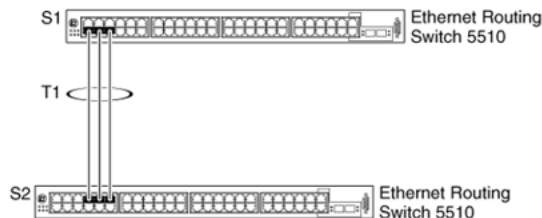
Correctly Configured Trunk

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

More...

Press Ctrl-N to display choices for ports 13-24.
Use space bar to display choices press <Return> or <Enter> to select choice.
Press Ctrl-B to return to previous menu. Press Ctrl-C to return to Main Menu.

S1 Port Configuration screen



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

More...

Press Ctrl-N to display choices for ports 13-24.
Use space bar to display choices press <Return> or <Enter> to select choice.
Press Ctrl-B to return to previous menu. Press Ctrl-C to return to Main Menu.

S2 Port Configuration screen

11087EA

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

If trunk member port 11 of root Switch S2 is physically disconnected and then reconnected to port 13, the Spanning Tree Port Configuration screen for Switch S1 changes to show port 6 in the Blocking state ("[Detecting a Misconfigured Port](#)" (page 49))

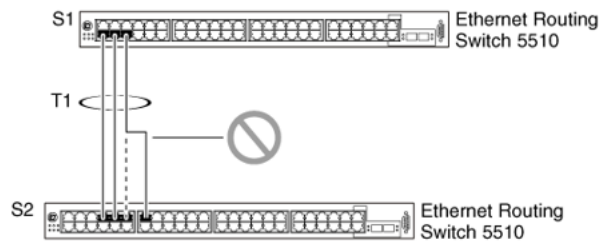
Detecting a Misconfigured Port

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

More...

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

S1 Port Configuration screen



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

More...

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

S2 Port Configuration screen

11088EA

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

Port membership in MultiLink Trunking

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

To change port membership in MultiLink Trunking:

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

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

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

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

SMLT

This section describes the Split MultiLink Trunking (SMLT) feature and includes the following topics:

- ["Overview" \(page 50\)](#)
- ["Advantages of SMLT" \(page 51\)](#)
- ["How does SMLT work?" \(page 52\)](#)
- ["Triangle SMLT configuration" \(page 52\)](#)
- ["Square SMLT configuration" \(page 57\)](#)
- ["SMLT in stack configuration" \(page 66\)](#)
- ["SLT" \(page 70\)](#)
- ["Using SMLT with SLT" \(page 71\)](#)
- ["SMLT and SLT Configuration steps" \(page 73\)](#)

Overview

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

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

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

ATTENTION

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

SMLT is supported on standalone units in triangle or square configuration (see "[SMLT in triangle configuration](#)" (page 52) and "[SMLT in square configuration](#)" (page 58)) and on stacks in triangle configuration.

In this release, you cannot configure SMLT data when SMLT is running. To modify an SLT or SMLT, you must disable SMLT on that port or trunk. As well, in this release, IGMP over SMLT is not supported.

Note 1: With release 5.0 and 5.1 software, the Ethernet Routing Switch 5500 does not support LACP (IEEE 802.3ad) over SMLT. Layer 2 Edge switches must support MultiLink Trunking to allow communications with SMLT aggregation switches.

Note 2: To enable SMLT on the Ethernet Routing Switch 5500, you must first enable Global IP Routing.

Advantages of SMLT

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

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

SMLT compared to Spanning Tree Protocol

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

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

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

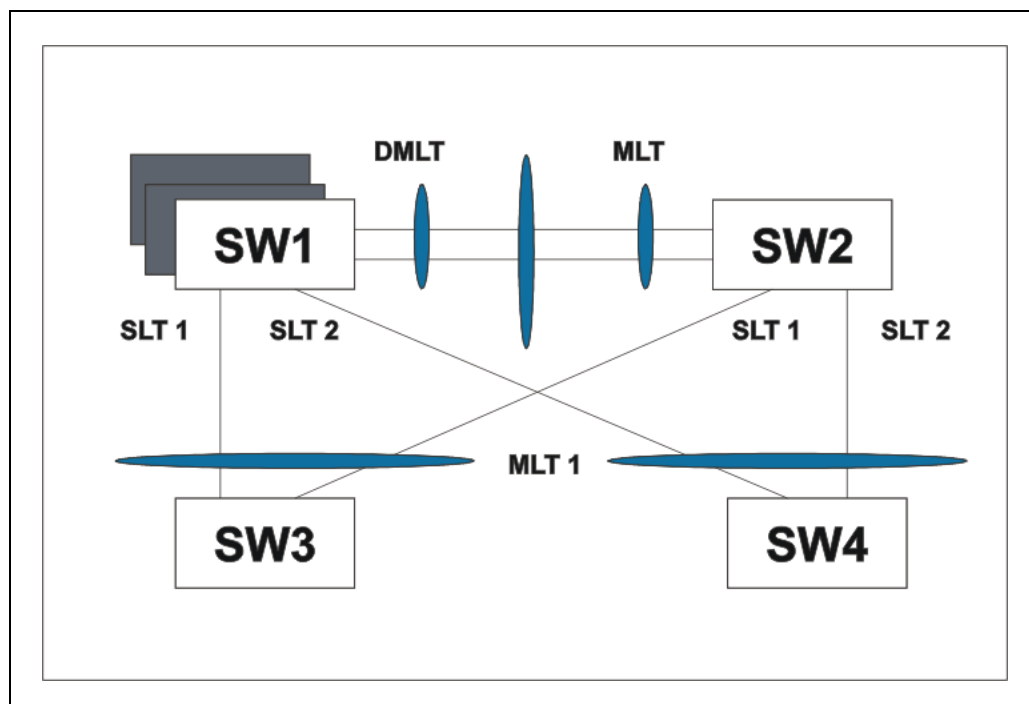
How does SMLT work?

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

Triangle SMLT configuration

Triangle SMLT configuration requires one pair of aggregation switches as shown in "SMLT in triangle configuration" (page 52). Triangle SMLT can be set up with standalone switches or in a stack configuration.

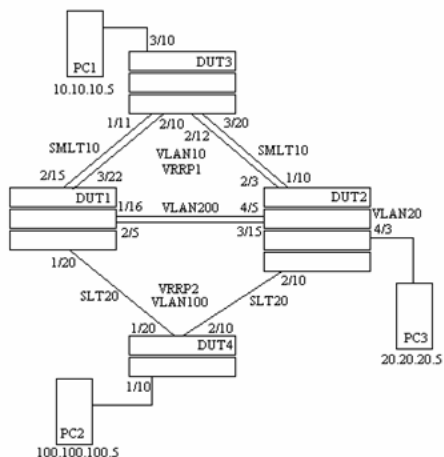
SMLT in triangle configuration



Detailed configuration example for SMLT triangle configuration

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

SMLT triangle configuration



SMLT triangle configuration

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

Configure DUT1

```

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

```

```
ip routing
in vlan 200
ip add 200.200.200.1 255.255.255.0
exit
in vlan 10
ip add 10.10.10.2 255.255.255.0
exit
in vlan 100
ip add 100.100.100.3 255.255.255.0
exit
mlt 10 ena mem 2/15,3/22
mlt spanning-tree 10 stp all learning disable
mlt 30 ena mem 1/16,2/5
mlt spanning-tree 30 stp all learning disable
in mlt 30
ist peer-ip 200.200.200.2
ist vlan 200
ist ena
exit
in mlt 10
smlt 10
exit
in fast 1/20
smlt 20
exit
in vlan 100
ip vrrp address 1 100.100.100.1
ip vrrp 1 enable backup-master enable
ip ospf enable
exit
in vlan 10
ip vrrp address 2 10.10.10.1
ip vrrp 2 enable backup-master enable
ip ospf enable
```

```
exit
in vlan 200
ip ospf enable
exit
router vrrp ena
router ospf ena
Configure DUT2.

vlan create 10 type port
vlan create 100 type port
vlan create 200 type port
vlan create 20 type port
vlan port 2/10,4/5,3/15,1/10,2/3 tag enable
vlan mem add 200 4/5,3/15
vlan mem add 10 2/3,1/10,4/5,3/15
vlan mem rem 1 2/10,4/5,3/15,1/10,2/3
vlan mem rem 1 4/3
vlan mem add 20 4/3
vlan port 4/3 pvid 20
ip routing
in vlan 200
ip add 200.200.200.2 255.255.255.0
exit
in vlan 10
ip add 10.10.10.3 255.255.255.0
exit
in vlan 100
ip add 100.100.100.2 255.255.255.0
exit
in vlan 20
ip add 20.20.20.1 255.255.255.0
exit
mlt 10 ena mem 2/3,1/10
mlt spanning-tree 10 stp all learning disable
```

```
mlt 30 ena mem 4/5,3/15
mlt spanning-tree 30 stp all learning disable
in mlt 30
ist peer-ip 200.200.200.1
ist vlan 200
ist ena
exit
in mlt 10
smlt 10
exit
in fast 2/20
smlt 20
exit
in vlan 100
ip vrrp address 1 100.100.100.1
ip vrrp 1 enable backup-master enable
ip ospf enable
exit
in vlan 10
ip vrrp address 1 10.10.10.1
ip vrrp 2 enable backup-master enable
ip ospf enable
exit
in vlan 200
ip ospf enable
exit
in vlan 20
ip ospf enable
exit
router vrrp ena
router ospf ena
Configure DUT3.

vlan create 10 type port
```

```
vlan port 1/11,2/10,2/12,3/20 tag enable
vlan mem add 10 1/11,2/10,2/12,3/20
vlan mem rem 1 1/11,2/10,2/12,3/20,3/10
vlan mem add 10 3/10
vlan port 3/10 pvid 10
mlt 10 ena mem 1/11,2/10,2/12,3/20
mlt spanning-tree 10 stp all learning disable
```

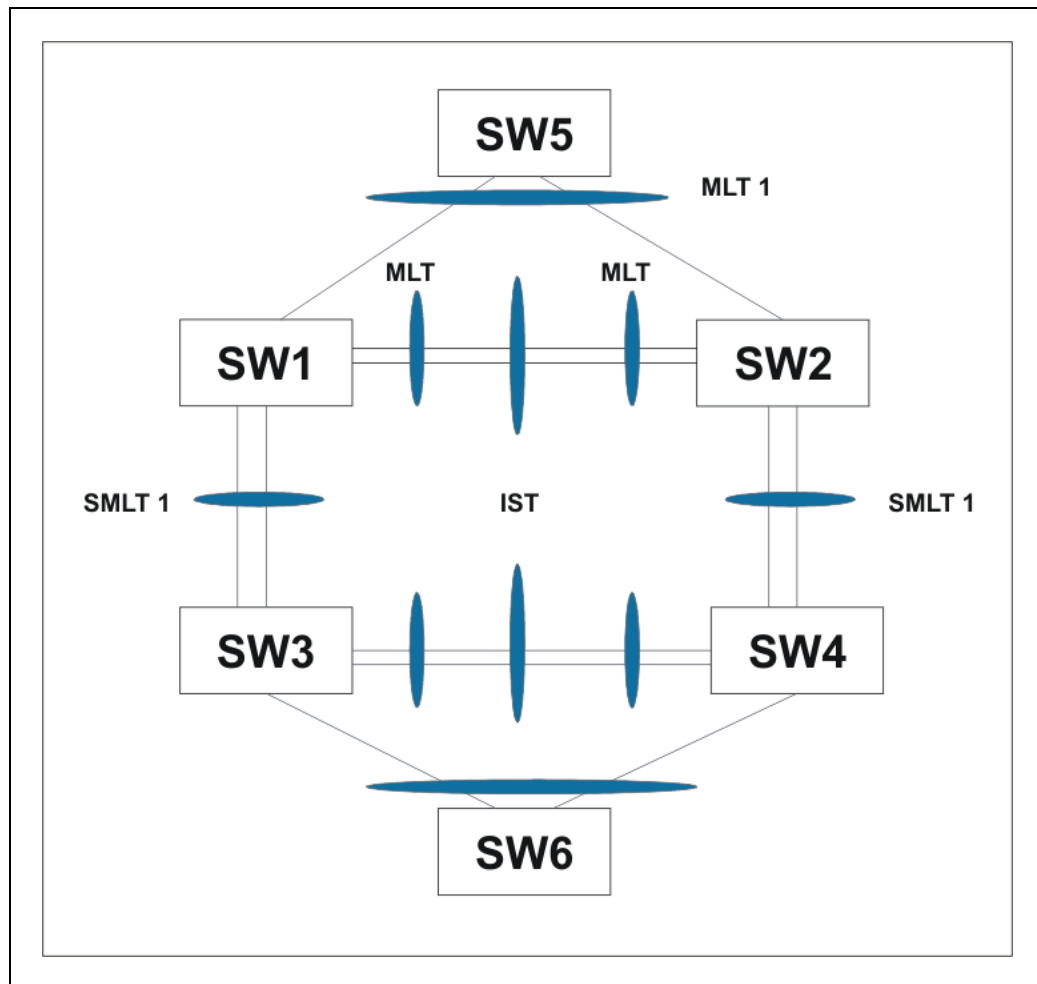
Configure DUT4.

```
vlan create 10 type port
vlan port 1/20,2/10 tag enable
vlan mem add 100 1/20,2/10
vlan mem rem 1 1/20,2/10,1/10
vlan mem add 100 1/10
vlan port 1/10 pvid 100
mlt 20 ena mem 1/20,2/10
mlt spanning-tree 20 stp all learning disable
```

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

Square SMLT configuration

Square SMLT configuration requires two pairs of aggregation switches connected back to back (see "[SMLT in square configuration](#)" (page 58)). Square configuration supports standalone switches.

SMLT in square configuration**Detailed configuration example for SMLT in square configuration**

The following three diagrams describe the setup of SMLT in square configuration using VRRP for L3 routing. All devices are assumed to be BayStack 5500 devices.

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

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

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

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

IST ports on all switches need to be tagged ports. SMLT ports may be tagged or untagged.

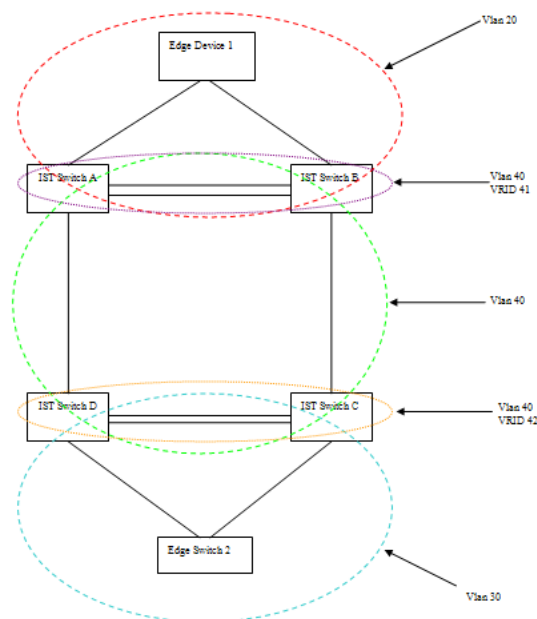
Each of the IST switches will be running 2 VRRP instances.

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

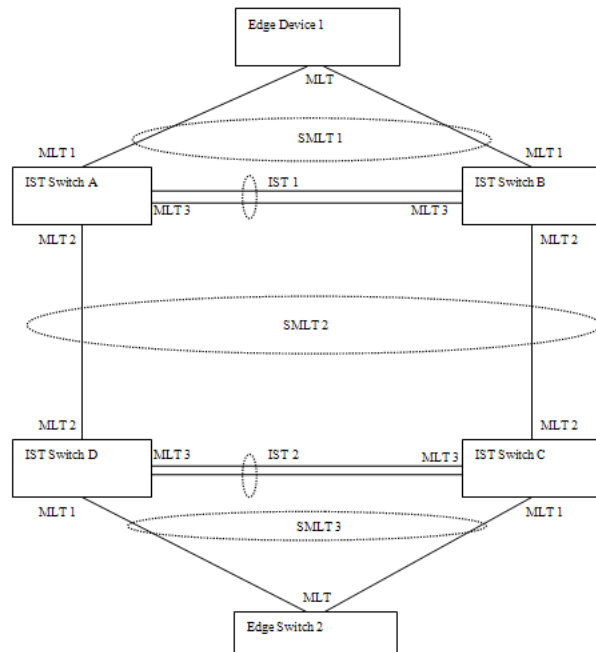
Additionally, backup-master needs to be enabled on all switches for all VRs.

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

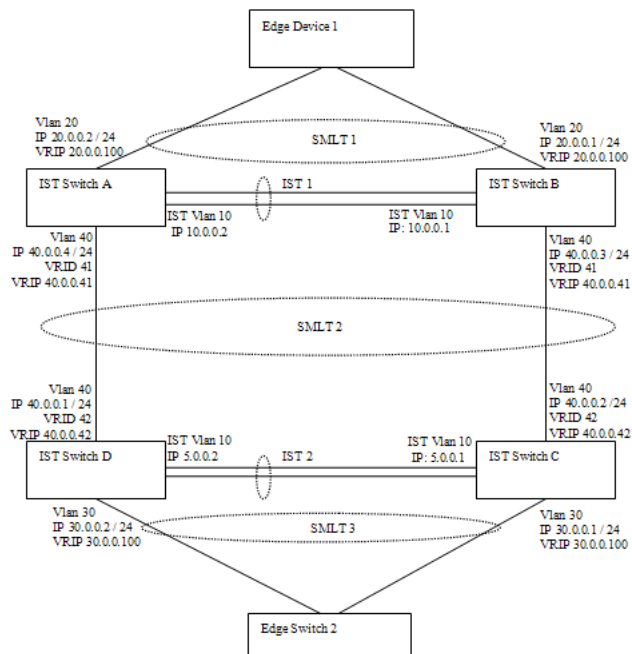
Square VRRP SMLT setup. Vlans and VRRP (IST vlans not indicated)



Square VRRP SMLT setup. SMLTs and ISTs



Square VRRP SMLT setup. Interface and VRRP IP addresses



The following paragraphs provide the configuration commands.

Edge Device 1

Nortel Ethernet Routing Switch 5500 Series
 Configuration — VLANs, Spanning Tree, and Link Aggregation
 NN47200-502 03.01 Standard
 5.1 27 August 2007


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

Edge Device 2

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

IST switch A

```
enable
configure terminal
vlan configcontrol autopvid
ip routing
router vrrp enable
vlan create 10 type port
vlan members add 10 3,4,5,6
interface vlan 10
ip address 10.0.0.2 255.255.255.0
exit
vlan port 3,4,5,6 tagging enable pvid 10
mlt 3 enable members 3,4,5,6 learning disable
interface mlt 3
ist enable peer-ip 10.0.0.1 vlan 10
exit
vlan create 20 type port
vlan members add 20 3,4,5,6,13,14
interface vlan 20
ip address 20.0.0.2 255.255.255.0
```

```
ip vrrp address 20 20.0.0.100
ip vrrp 20 enable backup-master enable
exit
mlt 1 enable members 13,14 learning disable
interface mlt 1
smlt 1
exit
vlan create 40 type port
vlan members add 40 3,4,5,6,17,18
interface vlan 40
ip address 40.0.0.4 255.255.255.0
ip vrrp address 41 40.0.0.41
ip vrrp 41 enable back-master enable
exit
mlt 2 enable members 17,18 learning disable
interface mlt 2
smlt 2
exit
ip route 30.0.0.0 255.255.255.0 40.0.0.42 1
```

IST switch B

```
enable
configure terminal
vlan configcontrol autopvid
ip routing
router vrrp enable
vlan create 10 type port
vlan members add 10 3,4,5,6
interface vlan 10
ip address 10.0.0.1 255.255.255.0
exit
vlan port 3,4,5,6 tagging enable pvid 10
mlt 3 enable members 3,4,5,6 learning disable
interface mlt 3
```

```
ist enable peer-ip 10.0.0.2 vlan 10
exit
vlan create 20 type port
vlan members add 20 3,4,5,6,13,14
interface vlan 20
ip address 20.0.0.1 255.255.255.0
ip vrrp address 20 20.0.0.100
ip vrrp 20 enable backup-master enable
exit
mlt 1 enable members 13,14 learning disable
interface mlt 1
smlt 1
exit
vlan create 40 create type port
vlan members add 40 3,4,5,6,17,18
interface vlan 40
ip address 40.0.0.3 255.255.255.0
ip vrrp address 41 40.0.0.41
ip vrrp 41 enable back-master enable
exit
mlt 2 enable members 17,18 learning disable
interface mlt 2
smlt 2
exit
ip route 30.0.0.0 255.255.255.0 40.0.0.42 1
```

IST switch C

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

```
interface vlan 10
ip address 5.0.0.1 255.255.255.0
exit
vlan port 3,4,5,6 tagging enable pvid 10
mlt 3 enable members 3,4,5,6 learning disable
interface mlt 3
ist enable peer-ip 5.0.0.2 vlan 10
exit
vlan create 30 type port
vlan members add 30 3,4,5,6,13,14
interface vlan 30
ip address 30.0.0.1 255.255.255.0
ip vrrp address 30 30.0.0.100
ip vrrp 30 enable backup-master enable
exit
mlt 1 enable members 13,14 learning disable
interface mlt 1
smlt 1
exit
vlan create 40 create type port
vlan members add 40 3,4,5,6,17,18
interface vlan 40
ip address 40.0.0.2 255.255.255.0
ip vrrp address 42 40.0.0.42
ip vrrp 42 enable back-master enable
exit
mlt 2 enable members 17,18 learning disable
interface mlt 2
smlt 2
exit
ip route 20.0.0.0 255.255.255.0 40.0.0.41 1
IST switch D

enable
```

```
configure terminal
vlan configcontrol autopvid
ip routing
router vrrp enable
vlan create 10 type port
vlan members add 10 3,4,5,6
interface vlan 10
ip address 5.0.0.2 255.255.255.0
exit
vlan port 3,4,5,6 tagging enable pvid 10
mlt 3 enable members 3,4,5,6 learning disable
interface mlt 3
ist enable peer-ip 5.0.0.1 vlan 10
exit
vlan create 30 type port
vlan members add 30 3,4,5,6,13,14
interface vlan 30
ip address 30.0.0.2 255.255.255.0
ip vrrp address 30 30.0.0.100
ip vrrp 30 enable backup-master enable
exit
mlt 1 enable members 13,14 learning disable
interface mlt 1
smlt 1
exit
vlan create 40 create type port
vlan members add 40 3,4,5,6,17,18
interface vlan 40
ip address 40.0.0.1 255.255.255.0
ip vrrp address 42 40.0.0.42
ip vrrp 42 enable back-master enable
exit
mlt 2 enable members 17,18 learning disable
interface mlt 2
```

```
smlt 2
exit
ip route 20.0.0.0 255.255.255.0 40.0.0.41 1
```

SMLT in stack configuration

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

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

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

Each nonbase unit will get the SMLT configuration data from the base unit and will save it to its own NVRAM.

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

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

If one or more of these checks is not successful, the SMLT application will stop running, but SMLT will still be administratively enabled.

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

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

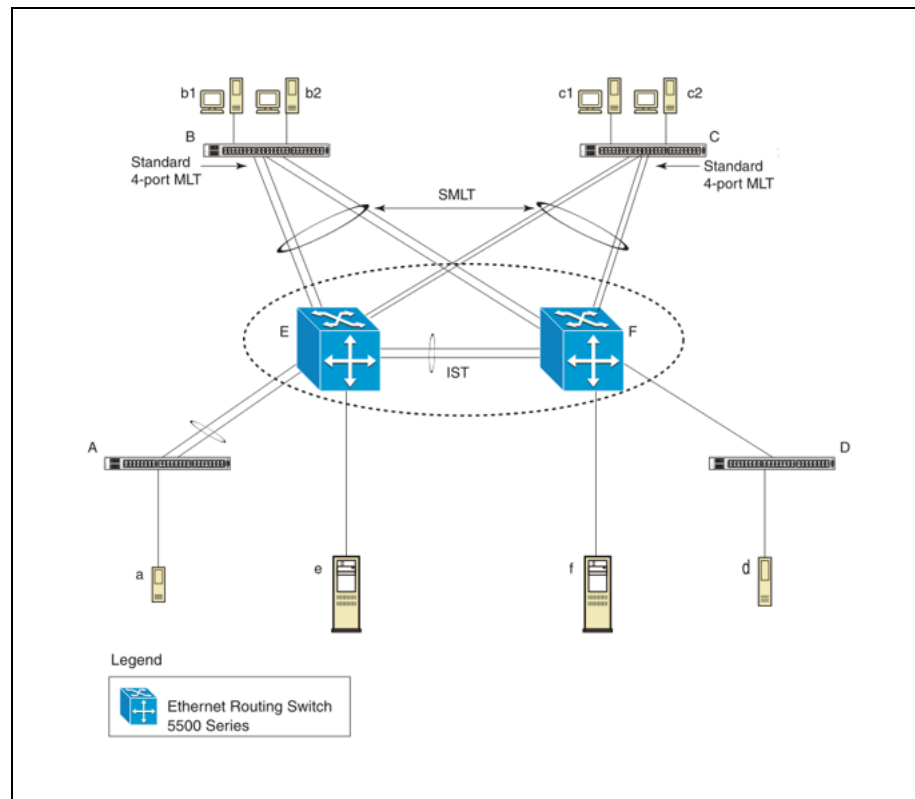
- If the base unit becomes inactive, the temporary base will take over.

- If a nonbase unit becomes inactive, the base unit will notify the rest of the stack with a list of all SMLT and SLT ports lost.
- If all of the IST ports were on the inactive unit, SMLT will stop running.

5500 Series switches as SMLT aggregation switches

"5500 Series switches as SMLT aggregation switches" (page 67) illustrates an SMLT configuration with a pair of Ethernet Routing Switch 5500 devices (E and F) operating as aggregation switches. Also included are four separate user access switches (A, B, C, and D).

5500 Series switches as SMLT aggregation switches



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

- "Inter-switch trunks (IST) " (page 67)
- "Other SMLT aggregation switch connections " (page 69)

Inter-switch trunks (IST)

As shown in "5500 Series switches as SMLT aggregation switches" (page 67), the implementation of SMLT only requires two SMLT-capable aggregation switches. User access switches B and C do not support SMLT. They are connected to the aggregation switches E and F using standard

multilink trunks split between the two aggregation switches. To support this SMLT configuration, the aggregation switches must be connected through an Inter-switch trunk (IST).

ATTENTION

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

Aggregation switches use the IST to:

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

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

When you set IST links between two 5500 Series devices, the switches must be running the identical software version.

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

You can configure IST links on mixed 5500 Series hardware; however, in this case be sure that both devices have matching IST configurations.

5500 Series IST links cannot be partnered with Ethernet Routing Switch 8000 devices.

ATTENTION

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

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

Other SMLT aggregation switch connections

"5500 Series switches as SMLT aggregation switches" (page 67) also includes end stations connected to each of the user access switches.

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

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

The examples that follow explain the process in more detail.

- "Example 1- Traffic flow from a to b1 or b2 " (page 69)
- "Example 2- Traffic flow from b1/b2 to c1/c2 " (page 69)
- "Example 3- Traffic flow from a to d " (page 69)
- "Example 4- Traffic flow from f to c1/c2 " (page 69)

Example 1- Traffic flow from a to b1 or b2

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

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

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

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

Example 3- Traffic flow from a to d

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

Example 4- Traffic flow from f to c1/c2

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

SLT

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

ATTENTION

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

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

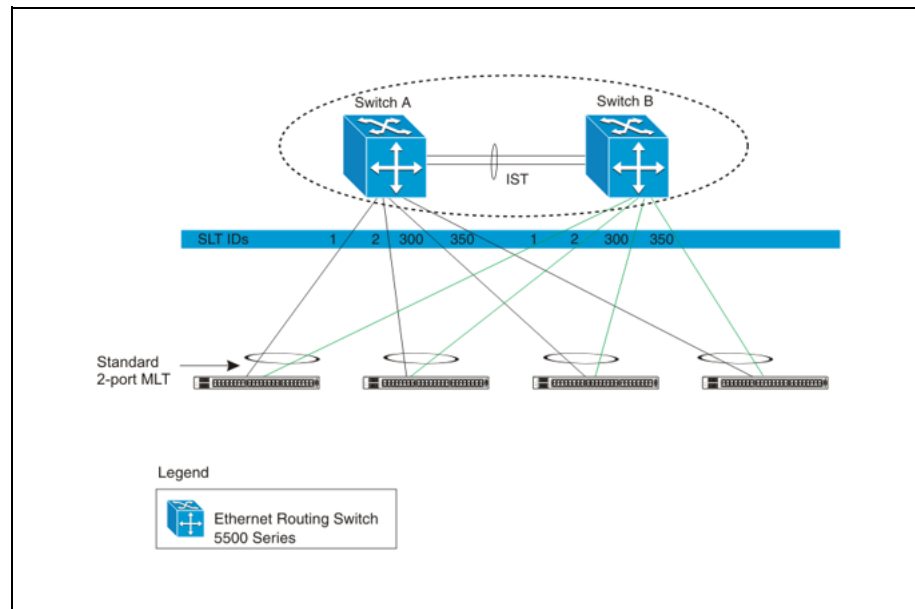
- MLT-based SMLT + MLT-based SMLT
- MLT-based SMLT + SLT
- SLT + SLT

Rules for configuring SLTs:

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

"SLT example" (page 71) shows a configuration in which both aggregation switches have single port SLTs with the same IDs. This configuration allows as many SLTs, as available ports exist on the switch.

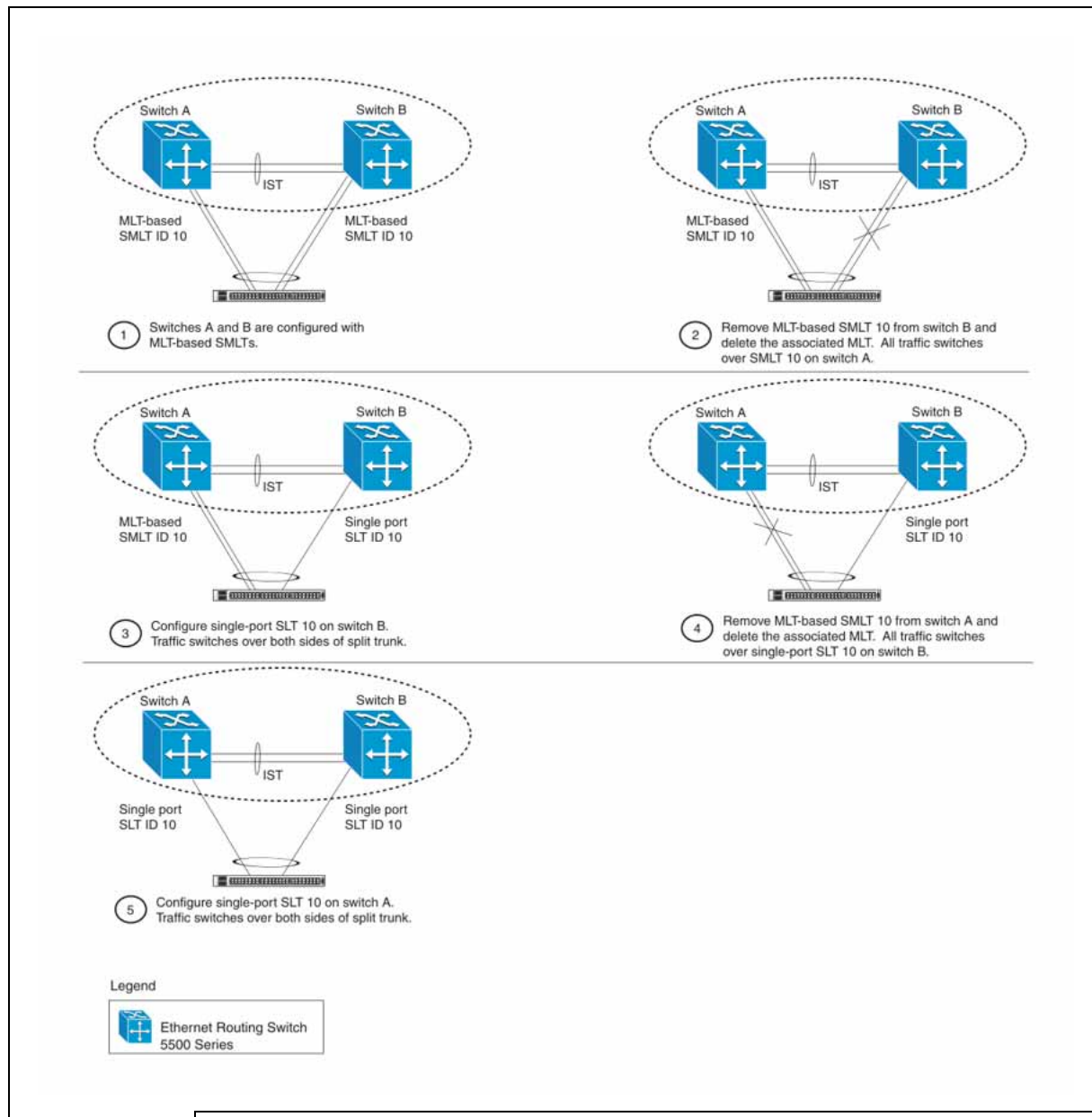
SLT example



Using SMLT with SLT

You can configure a split trunk with an SLT on one side and an MLT-based SMLT on the other. Both must have the same SMLT ID. In addition to general use, ["Changing a split trunk from MLT-based SMLT to SLT"](#) (page 72) shows how this configuration can be used for upgrading an MLT-based SMLT to an SLT without taking down the split trunk.

Changing a split trunk from MLT-based SMLT to SLT

**ATTENTION**

When you perform the steps listed in "Changing a split trunk from MLT-based SMLT to SLT" (page 72) and you remove the MLT-based SMLTs (steps 2 and 4), physically disable the ports by removing the cables or by shutting the ports down using the CLI. Otherwise, because STP is disabled on the ports, a loop can form as soon as the SMLT is removed.

SMLT and SLT Configuration steps

To enable SMLTs, ISTs, and SLTs on the 5500 Series switches, you must complete the following steps in the order indicated.

ATTENTION

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

Step	Action
1	Configure VLANs, including port membership, VLAN IP, and port tagging.
2	Configure STP groups: <ol style="list-style-type: none"> Create STP groups. Assign VLAN membership. Enable STP groups. Set STP port participation.
3	Enable Global IP Routing on the devices (always required).
4	If the switches are to be used for Layer 3 routing, enable VRRP on the units (required for Layer 3 only).
5	Configure MLTs on the devices: <ol style="list-style-type: none"> Create MLT groups by assigning trunk members. Disable STP participation on all trunk member ports. Enable the MLTs.
6	Configure SMLTs on the devices: <ol style="list-style-type: none"> Assign the Peer IP address and VLAN ID to the IST MLT. Enable the IST. Create the SMLTs. Create the SLTs (if applicable).
7	Make IST connections and ensure IST session is running.
8	Make SMLT/SLT connections and check SMLT/SLT status.

—End—

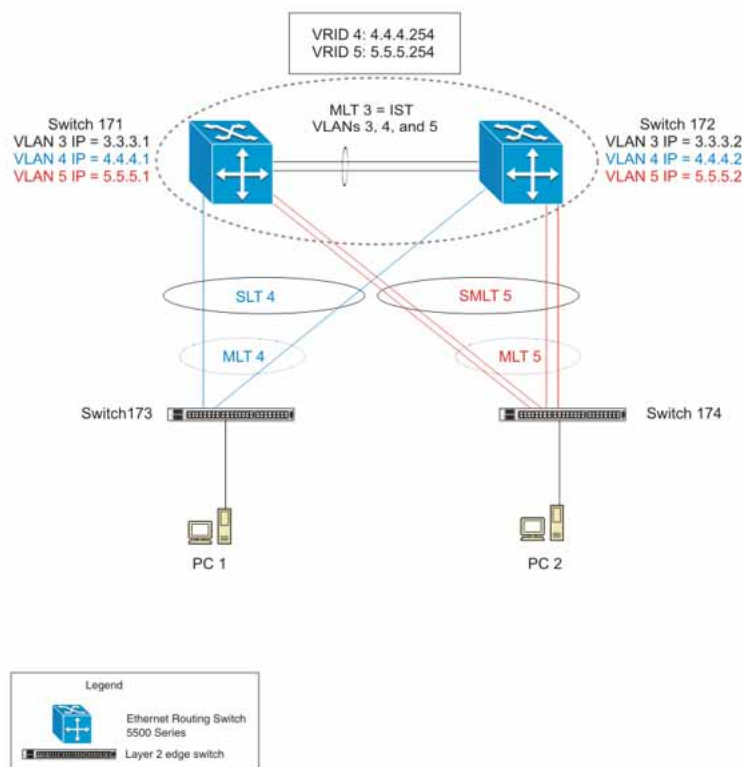
Note: These are the recommended steps for a new installation. For existing networks, perform steps 1 through 6 as closely as possible. To minimize loops, you can perform step 5 before steps 1 through 4.

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

SMLT configuration example with VRRP and OSPF

"[SMLT configuration example with VRRP and OSPF](#)" (page 74) shows an example of aggregation switches configured with SMLT, VRRP, and OSPF. For more information on VRRP and OSPF, see *Nortel Ethernet Routing Switch 5500 Series Configuration — IP Routing Protocols* (NN47200-503).

SMLT configuration example with VRRP and OSPF



To configure the example shown in "[SMLT configuration example with VRRP and OSPF](#)" (page 74), you must perform the following tasks:

For aggregation switch 171

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

—End—

For aggregation switch 172

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

—End—

For edge switch 173

Step Action

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

—End—

For edge switch 174

Step Action

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

—End—

Detailed configuration commands
Aggregation switch 171 configuration
IST, SMLT and SLT configuration

```

5520-48T-PWR(config)#vlan create 3 type port
5520-48T-PWR(config)#vlan create 4 type port
5520-48T-PWR(config)#vlan create 5 type port
5520-48T-PWR(config)#vlan port 1-5 tagging enable
5520-48T-PWR(config)#vlan member add 3 1-2
5520-48T-PWR(config)#vlan member add 4 1-2
5520-48T-PWR(config)#vlan member add 5 1-2
5520-48T-PWR(config)#vlan member remove 1 1-5
5520-48T-PWR(config)#vlan member add 4 3
5520-48T-PWR(config)#vlan member add 5 4,5
5520-48T-PWR(config)#ip routing
5520-48T-PWR(config)#interface vlan 3
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 3.3.3.1 255.255.255.0
5520-48T-PWR(config-if)#exit

```

```

5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 4.4.4.1 255.255.255.0
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 5.5.5.1 255.255.255.0
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#mlt 3 member 1-2
5520-48T-PWR(config)#mlt spanning-tree 3 stp
all learning disable
5520-48T-PWR(config)#mlt 3 enable
5520-48T-PWR(config)#interface mlt 3
5520-48T-PWR(config-if)#ist enable peer-ip 3.3.3.2 vlan 3
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface fastEthernet 3
5520-48T-PWR(config-if)#spanning-tree learning disable
5520-48T-PWR(config-if)#smlt 4
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#mlt 5 member 4-5
5520-48T-PWR(config)#mlt spanning-tree 5 stp
all learning disable
5520-48T-PWR(config)#mlt 5 enable
5520-48T-PWR(config-if)#interface mlt 5
5520-48T-PWR(config-if)#smlt 5
5520-48T-PWR(config-if)#exit

```

VRRP and OSPF

```

5520-48T-PWR(config)#router vrrp enable
5520-48T-PWR(config)#router ospf enable
5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip vrrp address 4 4.4.4.254
5520-48T-PWR(config-if)#ip vrrp 4 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip vrrp address 5 5.5.5.254
5520-48T-PWR(config-if)#ip vrrp 5 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit

```

Aggregation switch 172 configuration

IST, SMLT and SLT configuration

```

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

```

```
5520-48T-PWR(config)#vlan member add 4 1-2
5520-48T-PWR(config)#vlan member add 5 1-2
5520-48T-PWR(config)#vlan member remove 1 1-5
5520-48T-PWR(config)#vlan member add 4 3
5520-48T-PWR(config)#vlan member add 5 4,5
5520-48T-PWR(config)#ip routing
5520-48T-PWR(config)#interface vlan 3
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 3.3.3.2 255.255.255.0
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 4.4.4.2 255.255.255.0
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 5.5.5.2 255.255.255.0
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#mlt 3 member 1-2
5520-48T-PWR(config)#mlt spanning-tree 3 stp
all learning disable
5520-48T-PWR(config)#mlt 3 enable
5520-48T-PWR(config)#interface mlt 3
5520-48T-PWR(config-if)#ist enable peer-ip 3.3.3.1 vlan 3
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface fastEthernet 3
5520-48T-PWR(config-if)#spanning-tree learning disable
5520-48T-PWR(config-if)#smlt 4
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#mlt 5 member 4-5
5520-48T-PWR(config)#mlt spanning-tree 5 stp
all learning disable
5520-48T-PWR(config)#mlt 5 enable
5520-48T-PWR(config-if)#interface mlt 5
5520-48T-PWR(config-if)#smlt 5
5520-48T-PWR(config-if)#exit
```

VRRP and OSPF

```
5520-48T-PWR(config)#router vrrp enable
5520-48T-PWR(config)#router ospf enable
5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip vrrp address 4 4.4.4.254
5520-48T-PWR(config-if)#ip vrrp 4 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip vrrp address 5 5.5.5.254
5520-48T-PWR(config-if)#ip vrrp 5 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit
```

Edge switch 173 configuration (5500 Series)

```
5510-48T(config)#vlan create 4 type port
5510-48T(config)#vlan port 3-4 tagging enable
5510-48T(config)#vlan member add 4 3-4
5510-24T(config)#mlt 4 member 3-4
5510-24T(config)#mlt spanning-tree 4 stp all learning disable
5510-24T(config)#mlt 4 enable
```

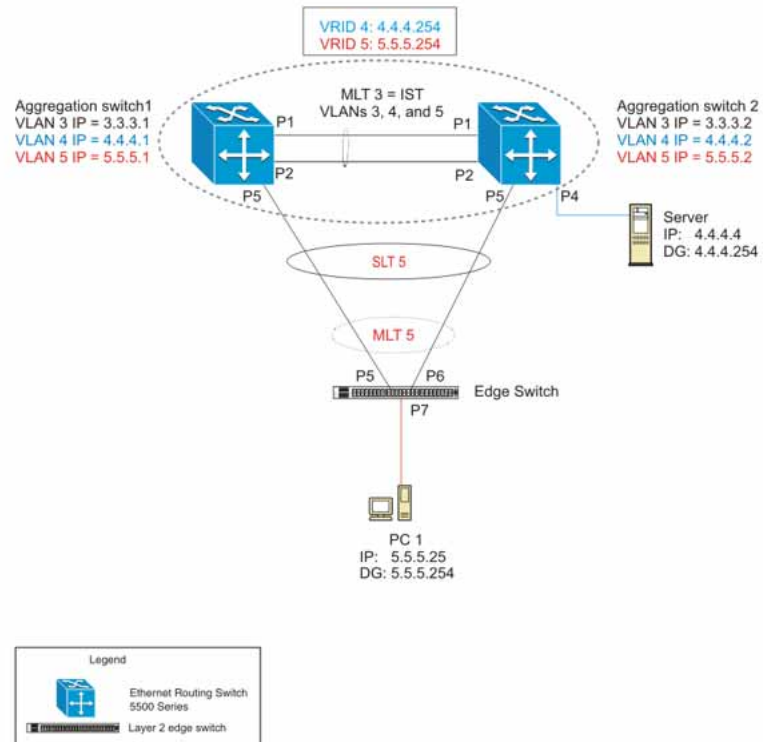
Edge switch 174 configuration (5500 Series)

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

SLT configuration example with VRRP and OSPF

"[SLT configuration example with VRRP and OSPF](#)" (page 81) shows an example of aggregation switches configured with SLT, VRRP and OSPF. For more information on VRRP and OSPF, see *Nortel Ethernet Routing Switch 5500 Series Configuration — IP Routing Protocols* (NN47200-503).

SLT configuration example with VRRP and OSPF



To configure the example shown in "SLT configuration example with VRRP and OSPF" (page 81), you must perform the following tasks.

For aggregation switch 1:

Step	Action
1	Create VLANs 3, 4, and 5.
2	Set ports 1 to 5 as tagging.
3	Assign ports 1 and 2 to VLAN 3.
4	Assign ports 1, 2 and 4 to VLAN 4.
5	Assign ports 1, 2, and 5 to VLAN 5.
6	Set VLAN 3 IP to 3.3.3.1 .
7	Set VLAN 4 IP to 4.4.4.1 .

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

—End—

For aggregation switch 2:

Step	Action
-------------	---------------

- | | |
|---|------------------------------------|
| 1 | Create VLANs 3, 4, and 5. |
| 2 | Set ports 1 to 5 as tagging. |
| 3 | Assign ports 1 and 2 to VLAN 3. |
| 4 | Assign ports 1, 2 and 4 to Vlan 4. |
| 5 | Assign ports 1, 2 and 5 to Vlan 5. |
| 6 | Set Vlan 3 IP to 3.3.3.2. |
| 7 | Set Vlan 4 IP to 4.4.4.2. |
| 8 | Set Vlan 5 IP to 5.5.5.2. |
| 9 | Enable IP routing. |

-
- 10 Create MLT 3 with ports 1 and 2.
 - 11 Disable STP on ports 1 and 2.
 - 12 Set IST = MLT 3, Peer IP=3.3.3.1, Vlan 3.
 - 13 Disable STP on port 5.
 - 14 Set port 5 as SLT 5.
 - 15 Enable VRRP globally.
 - 16 Enable VRRP on Vlan 4 with VRID 4 and VRIP 4.4.4.254.
 - 17 Enable VRRP back up master.
 - 18 Enable VRRP on Vlan 5 with VRID 5 and VRIP 5.5.5.254.
 - 19 Enable VRRP back up master.
 - 20 Enable OSPF globally.
 - 21 Enable OSPF on Vlan 3, 4 and 5.

—End—

For edge switch 1:

Step	Action
------	--------

- | | |
|---|--------------------------------|
| 1 | Create Vlan 4. |
| 2 | Assign ports 5 to 7 to Vlan 4. |
| 3 | Create Vlan 5. |
| 4 | Assign ports 5 to 7 to Vlan 5. |
| 5 | Create MLT 5 with ports 5 to 6 |
-

—End—

Detailed configuration commands

The following sections describe the detailed CLI commands required to carry out the configuration described in ["SLT configuration example with VRRP and OSPF" \(page 81\)](#)

Aggregation switch 1 configuration

IST, SMLT and SLT configuration

```
5520-48T-PWR(config)#vlan create 3 type port
5520-48T-PWR(config)#vlan create 4 type port
5520-48T-PWR(config)#vlan create 5 type port
5520-48T-PWR(config)#vlan port 1,2,4,5 tagging enable
5520-48T-PWR(config)#vlan member add 3 1-2
5520-48T-PWR(config)#vlan member add 4 1-2,4
5520-48T-PWR(config)#vlan member add 5 1,2,5
5520-48T-PWR(config)#vlan member remove 1 1-5
5520-48T-PWR(config)#ip routing
5520-48T-PWR(config)#interface vlan 3
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 3.3.3.1 255.255.255.0
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 4.4.4.1 255.255.255.0
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 5.5.5.1 255.255.255.0
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#mlt 3 member 1-2
5520-48T-PWR(config)#mlt spanning-tree 3 stp
all learning disable
5520-48T-PWR(config)#mlt 3 enable
5520-48T-PWR(config)#interface mlt 3
5520-48T-PWR(config-if)#ist enable peer-ip 3.3.3.2 vlan 3
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface fastEthernet 5
5520-48T-PWR(config-if)#spanning-tree learning disable
5520-48T-PWR(config-if)#smlt 5 5520-48T-PWR(config-if)#exit
```

VRRP and OSPF

```
5520-48T-PWR(config)#router vrrp enable
5520-48T-PWR(config)#router ospf enable
5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip vrrp address 4 4.4.4.254
5520-48T-PWR(config-if)#ip vrrp 4 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip vrrp address 5 5.5.5.254
5520-48T-PWR(config-if)#ip vrrp 5 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit
```

Aggregation switch 2 configuration

IST, SMLT and SLT configuration

```

5520-48T-PWR(config)#vlan create 3 type port
5520-48T-PWR(config)#vlan create 4 type port
5520-48T-PWR(config)#vlan create 5 type port
5520-48T-PWR(config)#vlan port 1-5 tagging enable
5520-48T-PWR(config)#vlan member add 3 1-2
5520-48T-PWR(config)#vlan member add 4 1,2,4
5520-48T-PWR(config)#vlan member add 5 1,2,5
5520-48T-PWR(config)#vlan member remove 1 1-5
5520-48T-PWR(config)#ip routing
5520-48T-PWR(config)#interface vlan 3
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 3.3.3.2 255.255.255.0
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 4.4.4.2 255.255.255.0
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip routing
5520-48T-PWR(config-if)#ip address 5.5.5.2 255.255.255.0
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#mlt 3 member 1-2
5520-48T-PWR(config)#mlt spanning-tree 3 stp
all learning disable
5520-48T-PWR(config)#mlt 3 enable
5520-48T-PWR(config)#interface mlt 3
5520-48T-PWR(config-if)#ist enable peer-ip 3.3.3.1 vlan 3
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface fastEthernet 5
5520-48T-PWR(config-if)#spanning-tree learning disable
5520-48T-PWR(config-if)#smlt 5
5520-48T-PWR(config-if)#exit

```

VRRP and OSPF

```

5520-48T-PWR(config)#router vrrp enable
5520-48T-PWR(config)#router ospf enable
5520-48T-PWR(config)#interface vlan 4
5520-48T-PWR(config-if)#ip vrrp address 4 4.4.4.254
5520-48T-PWR(config-if)#ip vrrp 4 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit
5520-48T-PWR(config)#interface vlan 5
5520-48T-PWR(config-if)#ip vrrp address 5 5.5.5.254
5520-48T-PWR(config-if)#ip vrrp 5 enable backup-master enable
5520-48T-PWR(config-if)#ip ospf enable
5520-48T-PWR(config-if)#exit

```

Edge switch configuration (5500 Series)

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

IEEE 802.3ad Link Aggregation

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

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

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

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

Link aggregation employs the following principles and concepts:

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

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

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

- Each port is assigned a unique, globally administered MAC address.

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

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

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

Link aggregation rules

The 5500 Series switch link aggregation groups operate under the following rules:

- Link aggregation groups are formed using LACP.
- All ports in a link aggregation group must be connected to the same far-end system.
- All ports in a link aggregation group must be operating in full-duplex mode.
- All ports in a link aggregation group must be configured to the same port speed.
- All ports in a link aggregation group must be in the same VLANs.
- In stack mode, ports in a link aggregation group can be on different units to form a distributed LAG (DLAG).
- LACPDUs are transmitted and received on all ports in the link aggregation group.
- Link aggregation is compatible with the Spanning Tree Protocol (STP).
- Link aggregation group(s) must be in the same STP groups.
- STP BPDUs are transmitted and received only on the first link in the group.

- A maximum of 32 link aggregation groups are supported.
- A maximum of 8 active links are supported per LAG.
- Unlimited standby links that are supported per LAG (for example, if a switch or stack is configured with one LAG, all nonactive LAG link ports can be configured as standby ports for that LAG).

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

The failover process is as follows:

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

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

LACP port mode

The IEEE 802.3ad standard specifies that links that are not successful candidates for aggregation (for example, links to devices that cannot perform aggregation, or links that are manually set as non-aggregatable) can continue to operate as individual LACP links. However, LACP-enabled, STP-disabled ports that operate as individual links can potentially cause network loops.

With release 5.0, you can specify the desired behavior of non-aggregatable LACP links on the switch:

- **Default mode:** In the default mode, if an LACP-enabled port is connected to a non-LACP partner port and the link fails to converge with the link partner, the port state moves to the forwarding state. This is the standard behavior from earlier software releases. The default mode is compatible with standard LACP.
- **Advance mode:** In the Advance mode, if an LACP-enabled port is connected to a non-LACP partner port and the link fails to converge with the link partner, the port state remains in the blocking state. This behavior is applied only to LACP-enabled ports that have STP disabled and prevents potential loops from forming in the network.

Note: The Advance mode is not compatible with IEEE 802.3 ad standard LACP.

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

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

VLACP

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

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

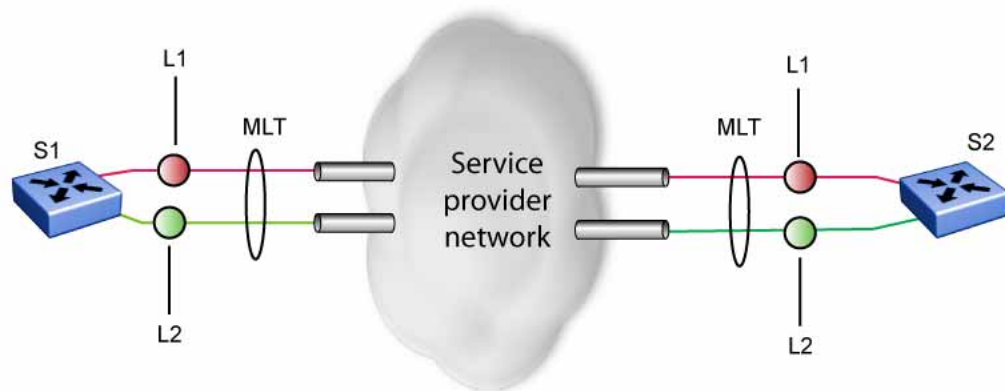
Virtual LACP (VLACP) overview

While Ethernet 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.

["Problem description \(1 of 2\)" \(page 90\)](#) provides an illustration of these limitations. While the Enterprise networks shown can connect their aggregated Ethernet trunk groups through a service provider network connection (for example, through a VPN), far-end failures cannot be signaled with Ethernet-based functions that operate end-to-end through the service provider cloud.

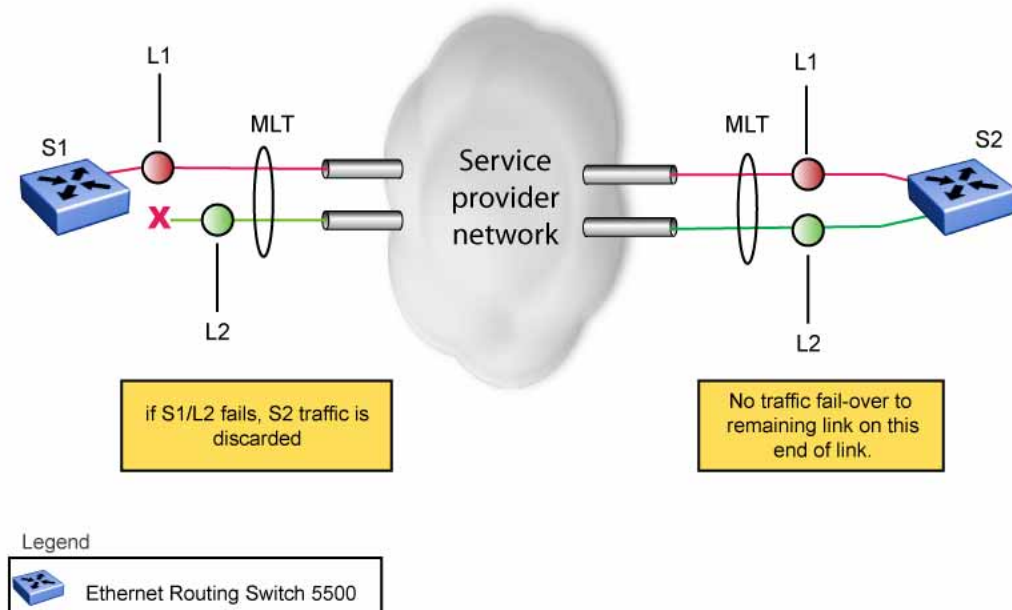
In ["Problem description \(1 of 2\)" \(page 90\)](#), the MLT (between Enterprise switches S1 and S2) extends through the service provider (SP) network.

Problem description (1 of 2)



As shown in "Problem description (2 of 2)" (page 91), 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.

Problem description (2 of 2)



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

Nortel has developed an extension to LACP, which is called *Virtual LACP (VLACP)*. This extension can provide an end-to-end failure detection mechanism. With VLACP, far-end failures can be detected allowing an MLT to fail over properly when end-to-end connectivity is not guaranteed for certain links in an aggregation group. VLACP prevents the failure scenario shown in "Problem description (2 of 2)" (page 91).

VLACP features

This section provides a summary of some of the key features of VLACP as implemented in Release 5.0 software:

- 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 when the port is unblocked)

Auto-Detection and Auto-Configuration of Nortel IP Phones

Ethernet Routing Switch 5500 Series Release 5.0 and higher software supports the Auto-Detection and Auto-Configuration (ADAC) of Nortel IP Phones. With ADAC, you can automatically configure the switch to support and prioritize IP Phone traffic.

When ADAC is enabled and a Nortel 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 Nortel 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).

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 Nortel IP Phones

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

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

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

The detection mechanism can be selected

- 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 Nortel IP phone. For more information and the list of defined MAC address ranges, see "[Auto-Detection by MAC address](#)" (page 95).

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 \(IEEE 802.1ab\)](#)" (page 96).

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 Nortel IP Phone MAC addresses, ADAC determines that the specified port is connected to a Nortel IP Phone and initiates the required configuration. ADAC is supported for a maximum of 32 devices per port, but in most cases, there will be only one IP phone and one PC on each port.

The 5500 Series switch has a default range of MAC addresses configured to be recognized as Nortel IP Phones by ADAC.

"Default ADAC MAC address ranges" (page 95) shows a list of the default MAC address ranges.

Default ADAC MAC address ranges

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

00-15-9B-FE-A4-66	00-15-9B-FF-24-B5
00-16-CA-00-00-00	00-16-CA-01-FF-FF
00-16-CA-F2-74-20	00-16-CA-F4-BE-0F
00-17-65-F6-94-C0	00-17-65-F7-38-CF
00-17-65-FD-00-00	00-17-65-FF-FF-FF
00-18-B0-33-90-00	00-18-B0-35-DF-FF
00-19-69-83-25-40	00-19-69-85-5F-FF

You can change these default MAC address ranges using the CLI, JDM, or Web-based management.

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

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

The maximum number of ranges that ADAC supports is 128.

Auto-Detection by LLDP (IEEE 802.1ab)

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

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

Detailed configuration example

The following commands provide a detailed configuration example.

- Default a DUT with 5.1 software image.
- Disable on port 5 MAC detection.

```

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

```

- Enable ADAC on port 5 and globally.

```

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

```

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

```

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

```

- Verify that above settings were applied.

```

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

```

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

```

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

```

Auto-Configuration of Nortel IP Phones

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

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

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

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

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

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

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

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

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

Initial user settings

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

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

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

— Uplink port, if used

Note: To properly enable the ADAC feature, the VLAN ID for the Voice-VLAN must not be a preexisting VLAN.

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

Port Restrictions

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

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

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

The **Uplink port** must not be:

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

The **Telephony port** must not be:

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

Operating modes

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

- ["QoS settings used by ADAC" \(page 100\)](#)

- "Untagged-Frames-Basic operating mode" (page 100)
- "Untagged-Frames-Advanced operating mode" (page 101)
- "Tagged-Frames operating mode" (page 102)

QoS settings used by ADAC

ADAC QoS configuration is applied to:

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

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

- **all-IP-traffic**

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

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

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

Untagged-Frames-Basic operating mode

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

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

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

QoS configuration

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

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

VLAN configuration

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

- Tagging of Telephony ports is set to Untagged.

Untagged-Frames-Advanced operating mode

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

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

QoS configuration

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

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

VLAN configuration

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

- Telephony port:

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

Tagged-Frames operating mode

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

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

QoS configuration

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

- For traffic coming from the telephony ports:

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

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

VLAN configuration

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

- Telephony port:
 - Membership = adds to Voice-VLAN; not removed from other VLANs
 - Tagging = UntagPVIDOnly
 - PVID = no change or changed to Default-VLAN(1) if the current value equals the Voice-VLAN (must be different from the Voice-VLAN ID)
- Call Server port (if any):
 - Membership = adds to Voice-VLAN; not removed from other VLANs
 - Tagging = Untagged
 - PVID = Voice-VLAN
- Uplink port (if any):
 - Membership = adds to Voice-VLAN; not removed from other VLANs
 - Tagging = Tagged
 - PVID = no change (All VLAN changes made by ADAC are as if VCC =flexible, so the Auto-PVID setting is ignored.)

Dynamic VLAN auto-configuration

The following describes the details of the ADAC VLAN configuration:

- The ADAC Voice VLAN is created and removed automatically.

- All membership to the ADAC Voice VLAN is dynamic, meaning that the settings are not saved to NVRAM. The dynamic settings will be lost on reboot or when ADAC is disabled.
- From the moment ADAC is enabled on a port set as a telephony port or a call server port, (but not an uplink port), all VLAN configuration is dynamic (including user configuration). When removing the configuration for a port (for example, when changing a port so that it is no longer a call server port or a telephony port), the configuration from NVRAM is restored. After that, the user configuration will be permanent again. For an uplink port, any user configuration made while ADAC was enabled on the port is saved.
- For telephony ports, the NVRAM VLAN configuration is restored in two cases: when the ADAC configuration is removed due to the removal of the IP Phone, or when ADAC is disabled for that port.
- The VLAN Configuration Control (VCC) rules, other than those for the Flexible mode, are skipped internally by ADAC configuring VLANs. Any VLAN settings made automatically by ADAC follow the rules of the Flexible mode, regardless of the current value of VCC. Any settings that you make manually on ADAC ports follow the current VCC mode, as for a non-ADAC port.
- If you change the preset values of Tagging and PVID when ADAC is running in Tagged-Frames mode, future auto-configurations will apply the new values. Changing the preset has no effect on current configured Tagging and PVID values.

ADAC and stacking

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

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

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

This same scenario also occurs for the Uplink port.

Lost Call Server Port or Uplink Port

If ADAC is operating in either the Untagged-Frames-Advanced or Tagged-Frames operating mode and you reset the unit on which the Call Server or Uplink port is located, the feature loses the valid Call Server or Uplink port. In this case, the feature is temporarily disabled until the unit

with the Call Server or Uplink port rejoins the stack and the configuration becomes valid again. While the unit is in a temporarily disabled state, the Voice-VLAN is not deleted if it was created first.

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

Uplink port as part of MLT in a stack

To set the Uplink port to be part of a distributed MLT in a stack, you must first configure and enable the MLT, and then you can set one of the MLT members as the Uplink port.

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

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

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

ADAC and LACP enabled on an Uplink port

To set the Uplink port as LACP-enabled, you must first configure and enable LACP on the port, and then you can set the port as the Uplink port.

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

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

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

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

Uplink port as part of LACP in a stack

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

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

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

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

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

ADAC and EAP configuration

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

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

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

To enable ADAC on an EAP port, follow these steps.

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

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

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

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

ADAC user Restrictions

After ADAC is enabled, you cannot:

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

You can:

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

Disabling ADAC

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

ADAC management

For details on configuring ADAC using the CLI, see "[Configuring ADAC for Nortel IP Phones using the CLI](#)" (page 122); using Web-based management, see "[Configuring ADAC for Nortel IP Phones using Web-based management](#)" (page 147); and, using Device Manager, see "[Configuration of ADAC for Nortel IP Phones using Device Manager](#)" (page 171).

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

Creating and Managing VLANs

Virtual Local Area Networks (VLAN) can be configured in the Nortel Ethernet Routing Switch 5500 Series through the Command Line Interface (CLI), Web-based Management Interface, or the Java Device Manager (JDM). This chapter outlines the creation and management of VLANs using these switch interfaces.

VLAN Support

The Nortel Ethernet Routing Switch 5500 Series supports up to 256 VLANs with up to 255 VLANs configurable with up to seven different PIDs.

Creating and Managing VLANs using the CLI

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

This section contains information about the following topics:

- ["show vlan command" \(page 110\)](#)
- ["show vlan interface info command" \(page 111\)](#)
- ["show vlan interface vids command" \(page 111\)](#)
- ["vlan mgmt command" \(page 111\)](#)
- ["default vlan mgmt command" \(page 112\)](#)
- ["vlan delete command" \(page 113\)](#)
- ["no vlan command" \(page 113\)](#)
- ["vlan name command" \(page 114\)](#)
- ["auto-pvid command" \(page 114\)](#)
- ["no auto-pvid command" \(page 114\)](#)
- ["vlan ports command" \(page 114\)](#)
- ["vlan members command" \(page 115\)](#)

- "Configuring VLAN Configuration Control" (page 116)
- "Managing the MAC address forwarding database table" (page 117)
- "IP Directed Broadcasting" (page 121)

show vlan command

The `show vlan` command displays the number, name, type, protocol, user PID, state of a VLAN and whether it is a management VLAN.

The syntax for the `show vlan` command is:

```
show vlan [configcontrol] [dhcp-relay <1-4094>]
[igmp { <1-4094> | unknown-mcast-allow-flood |
unknown-mcast-no-flood}] [interface { info | vids}] [ip
<vid>] [mgmt] [multicast < membership>] [type {port |
protocol-ipEther2| protocol-ipx802.3 | protocol-ipx802.2 |
protocol-ipxSnap | protocol-ipxEther2 | protocol-decEther2 |
protocol-snaEther2 | protocol-Netbios | protocol-xnsEther2 |
protocol-vinesEther2 | protocol-ipv6Ether2 | protocol-Userdef
|protocol-RarpEther2} [vid <1-4094>]
```

The `show vlan` command is executed in the Privileged EXEC command mode.

" `show vlan parameters`" (page 110) outlines the parameters for this command.

show vlan parameters

Parameter	Description
vid <1-4094>	Enter the number of the VLAN to display.
type	Enter the type of VLAN to display: <ul style="list-style-type: none"> • port - port-based • protocol - protocol-based (see following list)
protocol-ipEther2	Specifies an ipEther2 protocol-based VLAN.
protocol-ipx802.3	Specifies an ipx802.3 protocol-based VLAN.
protocol-ipx802.2	Specifies an ipx802.2 protocol-based VLAN.
protocol-ipxSnap	Specifies an ipxSnap protocol-based VLAN.
protocol-ipxEther2	Specifies an ipxEther2 protocol-based VLAN.
protocol-decEther2	Specifies a decEther2 protocol-based VLAN.
protocol-snaEther2	Specifies an snaEther2 protocol-based VLAN.
protocol-Netbios	Specifies a NetBIOS protocol-based VLAN.

Parameter	Description
protocol-xnsEther2	Specifies an xnsEther2 protocol-based VLAN.
protocol-vinesEther2	Specifies a vinesEther2 protocol-based VLAN.
protocol-ipv6Ether2	Specifies an ipv6Ether2 protocol-based VLAN.
protocol-Userdef	Specifies a user-defined protocol-based VLAN.
protocol-RarpEther2	Specifies a RarpEther2 protocol-based VLAN.

show vlan interface info command

The `show vlan interface info` command displays VLAN settings associated with a port, including tagging information, PVID number, priority, and filtering information for tagged, untagged, and unregistered frames.

The syntax for the `show vlan interface info` command is:

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

Substitute `<portlist>` with a list of the ports for which VLAN information is required or ALL for all ports.

The `show vlan interface info` command is executed in the Privileged EXEC command mode.

show vlan interface vids command

The `show vlan interface vids` command displays port memberships in VLANs.

The syntax for the `show vlan interface vids` command is:

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

Substitute `<portlist>` with a list of the ports for which VLAN information is required or ALL for all ports.

The `show vlan interface vids` command is executed in the Privileged EXEC command mode.

vlan mgmt command

You can use the `vlan mgmt` command to set a VLAN as the management VLAN.

The syntax for the `vlan mgmt` command is:

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

Substitute `<1-4094>` with the number of the port to be set as the management VLAN.

The `vlan mgmt` command is executed in the Global Configuration command mode.

default vlan mgmt command

The `default vlan mgmt` command resets the management VLAN to VLAN1.

The syntax for the `default vlan mgmt` command is:

```
default vlan mgmt
```

The `default vlan mgmt` command is executed in the Global Configuration command mode.

The `default vlan mgmt` command has no variables or parameters.

vlan create command

The `vlan create` command allows for the creation of a VLAN. A VLAN is created by setting the state of a previously nonexistent VLAN.

The syntax for the `vlan create` command is:

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

The `vlan create` command is executed in the Global Configuration command mode.

"[vlan create parameters](#)" (page 112) outlines the parameters for this command.

vlan create parameters

Parameter	Description
<1-4094>	Enter the number of the VLAN to create.
name <line>	Enter the name of the VLAN to create.
type	Enter the type of VLAN to create: <ul style="list-style-type: none"> port - port-based protocol - protocol-based (see following list)
protocol-ipEther2	Specifies an ipEther2 protocol-based VLAN.

Parameter	Description
protocol-ipx802.3	Specifies an ipx802.3 protocol-based VLAN.
protocol-ipx802.2	Specifies an ipx802.2 protocol-based VLAN.
protocol-ipxSnap	Specifies an ipxSnap protocol-based VLAN.
protocol-ipxEther2	Specifies an ipxEther2 protocol-based VLAN.
protocol-decEther2	Specifies a decEther2 protocol-based VLAN.
protocol-snaEther2	Specifies an snaEther2 protocol-based VLAN.
protocol-Netbios	Specifies a NetBIOS protocol-based VLAN.
protocol-xnsEther2	Specifies an xnsEther2 protocol-based VLAN.
protocol-vinesEther2	Specifies a vinesEther2 protocol-based VLAN.
protocol-Userdef <4096-65534>	Specifies a user-defined protocol-based VLAN.
protocol-ipv6Ether2	Specifies an ipv6Ether2 protocol-based VLAN.

vlan delete command

The `vlan delete` command allows for the deletion of a VLAN.

The syntax for the `vlan delete` command is:

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

Substitute the `<2-4094>` with the number of the VLAN to be deleted. VLAN1 cannot be deleted.

The `vlan delete` command is executed in the Global Configuration command mode.

no vlan command

The `no vlan` command is another method to delete a VLAN. You can also use this command to remove MAC addresses from the list of addresses for which flooding is allowed.

The syntax for the `no vlan` command is:

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

Substitute `<2-4094>` with the number of the VLAN to be deleted. (VLAN1 cannot be deleted.) Substitute `<H.H.H>` with the MAC addresses to remove from the list of addresses for which flooding is allowed.

The `no vlan` command is executed in the Global Configuration command mode.

vlan name command

The `vlan name` command allows the name of an existing VLAN to be changed.

The syntax for the `vlan name` command is:

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

Substitute `<1-4094>` with the number of the VLAN and `<line>` with the new VLAN name.

The `vlan name` command is executed in the Global Configuration command mode.

auto-pvid command

The `auto-pvid` command enables the automatic PVID feature.

The syntax for the `auto-pvid` command is:

```
auto-pvid
```

The `auto-pvid` command is executed in the Global Configuration command mode.

no auto-pvid command

The `no auto-pvid` command disables the automatic PVID feature.

The syntax for the `no auto-pvid` command is:

```
no auto-pvid
```

The `no auto-pvid` command is executed in the Global Configuration command mode.

vlan ports command

The `vlan ports` command configures the VLAN-related settings for a port.

The syntax for the `vlan ports` command is:

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

The `vlan ports` command is executed in the Global Configuration command mode.

" [vlan ports parameters](#)" (page 115) outlines the parameters for this command.

vlan ports parameters

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

vlan members command

The `vlan members` command adds or deletes a port from a VLAN.

The syntax for the `vlan members` command is:

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

The `vlan members` command is executed in the Global Configuration command mode.

" [vlan members parameters](#)" (page 116) outlines the parameters for this command.

vlan members parameters

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

Configuring VLAN Configuration Control

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

VLAN Configuration Control offers four options for controlling VLAN modification:

- Strict
- Automatic
- AutoPVID
- Flexible

Note: The factory default setting is Strict.

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

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

- ["show vlan configcontrol command" \(page 116\)](#)
- ["vlan configcontrol command" \(page 117\)](#)

show vlan configcontrol command

The `show vlan configcontrol` command is used to display the current VLAN Configuration Control setting.

The syntax for this command is:

```
show vlan configcontrol
```


The `show vlan configcontrol` command is executed in the Global Configuration command mode. This command has no parameters.

vlan configcontrol command

The `vlan configcontrol` command is used to modify the current VLAN Configuration Control setting. This command applies the selected option to all VLANs on the switch.

The syntax for this command is:

```
vlan configcontrol <vcc_option>
```

"[vlan configcontrol parameters](#)" (page 117) outlines the parameters for this command.

vlan configcontrol parameters

Parameter	Description
<vcc_option>	<p>This parameter denotes the VCC option to use on the switch. The valid values are:</p> <ul style="list-style-type: none"> • <code>automatic</code> -- Changes the VCC option to Automatic. • <code>autopvid</code> -- Changes the VCC option to AutoPVID. • <code>flexible</code> -- Changes the VCC option to Flexible. • <code>strict</code> -- Changes the VCC option to Strict. This is the default VCC value. <p>For more information about these options, refer to "Configuring VLAN Configuration Control" (page 116).</p>

The `vlan configcontrol` command is executed in the Global Configuration command mode.

Managing the MAC address forwarding database table

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

- "[show mac-address-table command](#)" (page 118)
- "[mac-address-table aging-time command](#)" (page 119)

- "default mac-address-table aging-time command" (page 120)

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

- a single MAC address (see "clear mac-address-table address command" (page 121))
- all addresses from the MAC address table (see "clear mac-address-table command" (page 120))
- a port or list of ports (see "clear mac-address-table interface FastEthernet command" (page 120))
- a trunk (see "clear mac-address-table interface mlt command" (page 121))
- a VLAN (see "clear mac-address-table interface vlan command" (page 120))

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

The MAC flush commands are supported in NNCLI, SNMP, JDM, and the Web-based management interface.

show mac-address-table command

The `show mac-address-table` command displays the current contents of the MAC address forwarding database table. You can now filter the MAC Address table by port number. The MAC address table can store up to 16000 addresses.

The syntax for the `show mac-address-table` command is:

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

The `show mac-address-table` command is in the `privExec` command mode.

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

show mac-address-table command parameters

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

The following figure displays sample output from the `show mac-address-table` command.

show mac-address-table command output

```

5530-24IFD(config)#show mac-address-table
Mac Address Table Aging Time: 300
Number of addresses: 21

```

MAC Address	Source	MAC Address	Source
00-04-38-D5-9A-81	Port: 1	00-06-29-77-4E-23	Port: 1
00-06-29-8F-CF-0D	Port: 1	00-07-E9-40-7A-2A	Port: 1
00-08-02-37-FD-E4	Port: 1	00-08-02-A4-3F-DF	Port: 1
00-08-02-C2-8D-50	Port: 1	00-09-97-29-19-80	Port: 1
00-11-85-C1-45-BF	Port: 1	00-11-85-C1-77-85	Port: 1
00-11-85-C1-77-A2	Port: 1	00-11-85-C3-2F-F9	Port: 1
00-11-85-C3-DE-95	Port: 1	00-11-85-D3-17-72	Port: 1
00-11-F9-35-D0-00	Port: 1	00-12-79-8F-4B-6B	Port: 1
00-12-79-8F-CD-4E	Port: 1	00-12-79-8F-ED-3C	Port: 1
00-50-04-E1-3D-EB	Port: 1	00-E0-81-5A-4D-E5	Port: 1
00-E0-81-5A-4F-19	Port: 1	08-00-87-80-B0-7A	Port: 1

mac-address-table aging-time command

The `mac-address-table aging-time` command sets the time during which the switch retains unseen MAC addresses.

The syntax for the `mac-address-table aging-time` command is:

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

The `mac-address-table aging-time` command is in the config command mode.

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

mac-address-table aging-time command parameters

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

default mac-address-table aging-time command

The `default mac-address-table aging-time` command sets the aging for MAC addresses to 300 seconds.

The syntax for the `default mac-address-table aging-time` command is:

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

The `default mac-address-table aging-time` command is in the config command mode.

clear mac-address-table command

The `clear mac-address-table` command flushes the MAC address table.

The syntax for the `clear mac-address-table` command is:

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

The `clear mac-address-table` command is in the privExec command mode.

clear mac-address-table interface vlan command

The `clear mac-address-table interface vlan` command flushes the MAC addresses for the specified vlan.

The syntax for the `clear mac-address-table interface vlan` command is:

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

where `<vlan #>` is the number of the vlan to flush from the MAC address table.

The `clear mac-address-table vlan` command is in the privExec command mode.

clear mac-address-table interface FastEthernet command

The `clear mac-address-table interface FastEthernet` command flushes the MAC addresses for the specified ports. This command does not flush the addresses learned on the trunk.

The syntax for the `clear mac-address-table interface FastEthernet` command is:

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

where `<port-list>` is the list of ports to flush from the MAC address table.

Flushing out ports 1 and 2 on a standalone unit example

```
clear mac-address-table interface FastEthernet 1,2
```

Flushing out ports 1-10 on unit 2 and 1-7 on unit 3 of a stack example

```
clear mac-address-table interface FastEthernet
2/1-10,3/1-7
```

Flushing out all ports example

```
clear mac-address-table interface FastEthernet All
```

The `clear mac-address-table FastEthernet` command is in the `privExec` command mode.

clear mac-address-table interface mlt command

The `clear mac-address-table interface mlt` command flushes the MAC addresses for the specified trunk. This command flushes only addresses that are learned on the trunk.

The syntax for the `clear mac-address-table interface trunk` command is:

```
clear mac-address-table interface mlt <trunk #>
```

where `<trunk #>` is the number of the trunk to flush from the MAC address table.

The `clear mac-address-table mlt` command is in the `privExec` command mode.

clear mac-address-table address command

The `clear mac-address-table address` command flushes one MAC address from the MAC address table.

The syntax for the `clear mac-address-table address` command is:

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

where `<H.H.H>` is the MAC address to flush from the MAC address table.

Clearing address 00-AB-C2-F9-A1-02 example

```
clear mac-address-table address AB.C2F9.A102
```

The `clear mac-address-table address` command is in the `privExec` command mode.

IP Directed Broadcasting

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

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

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

By default, this feature is disabled.

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

- ["ip directed-broadcast enable command" \(page 122\)](#)
- ["no ip directed-broadcast enable command" \(page 122\)](#)

ip directed-broadcast enable command

The `ip directed-broadcast enable` command is used to enable IP directed broadcast.

The syntax for this command is:

```
ip directed-broadcast enable
```

The `ip directed-broadcast enable` command is executed in the Global Configuration command mode.

no ip directed-broadcast enable command

The `no ip directed-broadcast enable` command is used to disable IP directed broadcast.

The syntax for this command is:

```
no ip directed-broadcast enable
```

The `no ip directed-broadcast enable` command is available in the Global Configuration command mode.

Configuring ADAC for Nortel IP Phones using the CLI

You can configure ADAC-related settings using the CLI. For more information about the ADAC feature, see ["Auto-Detection and Auto-Configuration of Nortel IP Phones" \(page 93\)](#).

This section covers the following commands:

- ["adac command \(global\)" \(page 123\)](#)
- ["no adac command \(global\)" \(page 124\)](#)
- ["default adac" \(page 124\)](#)
- ["adac detection command" \(page 127\)](#)
- ["no adac detection command" \(page 127\)](#)

- "default adac detection command" (page 128)
- "adac port enable command" (page 128)
- "no adac port enable command" (page 128)
- "default adac port enable" (page 129)
- "adac mac-range-table command" (page 129)
- "no adac mac-range-table command" (page 129)
- "default adac mac-range-table command" (page 130)
- "show adac mac-range-table command" (page 131)
- "show adac interface command" (page 130)
- "show adac mac-range-table command" (page 131)

adac command (global)

The `adac` command sets the global ADAC settings for the device.

The syntax for the `adac` command is:

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

The `adac` command is in the config command mode.

"[adac command \(global\) parameters and variables](#)" (page 123) describes the parameters and variables for the `adac` command.

adac command (global) parameters and variables

Parameters and variables	Description
enable	Enables ADAC on the device.
op-mode <untagged-frames-basic/ untagged-frames-advanced / tagged-frames >	Sets the ADAC operation mode to one of the following: <ul style="list-style-type: none"> • untagged-frames-basic: IP Phones send untagged frames, and the Voice VLAN is not created. • untagged-frames-advanced: IP Phones send untagged frames, and the Voice VLAN is created. • tagged-frames: IP Phones send tagged frames.

Parameters and variables	Description
traps enable	Enables ADAC trap notifications.
voice-vlan <1-4094>	Sets the Voice VLAN ID. The assigned VLAN ID must not previously exist.
uplink-port <portlist>	Sets the Uplink ports.
call-server-port <ports>	Sets the Call Server ports.

no adac command (global)

The `no adac` command disables ADAC on the device or clears the ADAC settings for the device. The syntax for the `no adac` command is:

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

The `no adac` command is in the config command mode.

"[no adac command parameters and variables](#)" (page 124) describes the parameters and variables for the `no adac` command.

Note: If you do not specify any of the following parameters in the `no adac` command, the command performs all of the actions described for all of these parameters.

no adac command parameters and variables

Parameters and variables	Description
enable	Disables ADAC on the device.
traps enable	Disables ADAC trap notifications.
voice-vlan	Clears the Voice VLAN ID.
uplink-port	Clears the Uplink ports.
call-server-port	Clears Call Server ports.

default adac

The `default adac` command restores the default ADAC settings on the device. The syntax for the `default adac` command is:

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

The `default adac` command is in the config command mode.

"[default adac command parameters and variables](#)" (page 125) describes the parameters and variables for the `default adac` command.

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

default adac command parameters and variables

Parameters and variables	Description
enable	Restores the default ADAC administrative state (disabled).
call-server-port	Restores the default Call Server port (none).
op-mode	Restores the default ADAC operation mode (Untagged Frames Basic).
traps enable	Restores the default state for ADAC notifications (enabled).
uplink-port	Restores the default Uplink port (none).
voice-vlan	Restores the default Voice-VLAN ID (none).

adac command (per port settings)

The `adac` command sets the per port ADAC settings for the device.

The syntax for the `adac` command is:

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

The `adac` command is in the interface configuration command mode.

"[adac command \(per port\) parameters and variables](#)" (page 125) describes the parameters and variables for the `adac` command.

adac command (per port) parameters and variables

Parameters and variables	Description
port <portlist>	Ports to which to apply the ADAC configuration.
enable	Enables ADAC on the port or ports listed.

tagged-frames-pvid <1-4094> <i>no-change</i>	Sets Tagged-Frames PVID on the port or ports listed. Use <i>no-change</i> to keep the current setting.
tagged-frames-tagging <i>tagAll</i> <i>tagPvidOnly</i> <i>untagPvidOnly</i> <i>no-change</i>	Sets Tagged-Frames Tagging to <ul style="list-style-type: none"> • <i>tagAll</i> • <i>tagPvidOnly</i> • <i>untagPvidOnly</i> Use <i>no-change</i> to keep the current setting.

no adac command (per port settings)

The `no adac` command disables ADAC on the port.

The syntax for the `no adac` command is:

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

The `no adac` command is in the interface configuration command mode.

"[no adac command \(per port\) parameters and variables](#)" (page 126) describes the parameters and variables for the `no adac` command.

no adac command (per port) parameters and variables

Parameters and variables	Description
port <portlist>	Ports for which to disable ADAC.
enable	Disables ADAC on the port or ports listed.

default adac command (per port settings)

The `default adac` command sets the per port ADAC defaults for the specified ports.

The syntax for the `default adac` command is:

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

The `default adac` command is in the interface configuration command mode.

"[default adac command \(per port\) parameters and variables](#)" (page 127) describes the parameters and variables for the `default adac` command.

default adac command (per port) parameters and variables

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

adac detection command

The `adac detection` command sets the auto-detection method, by MAC address or using LLDP (IEEE 802.1ab). The syntax for the `adac detection` command is:

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

The `adac detection` command is in the config-if command mode.

"[adac detection command parameters and variables](#)" (page 127) describes the parameters and variables for the `adac detection` command.

adac detection command parameters and variables

Parameters and variables	Description
port <portlist>	Specifies the port or ports for which to set the detection mode.
mac	Enables MAC-based detection. The default setting is MAC enabled.
lldp	Enables LLDP (802.1ab) detection. The default setting is LLDP enabled.

no adac detection command

The `no adac detection` command turns off the auto-detection method for either MAC address or LLDP. The syntax for the `no adac detection` command is:

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

The `no adac detection` command is in the config-if command mode.

"[no adac detection command parameters and variables](#)" (page 128) describes the parameters and variables for the `no adac detection` command.

no adac detection command parameters and variables

Parameters and variables	Description
port <portlist>	Specifies the port or ports for which to disable the detection mode.
mac	Disables the MAC address detection mode.
lldp	Disables the LLDP detection mode.

default adac detection command

The `default adac detection` command returns the auto-detection method to its defaults. The default is to have both MAC and LLDP enabled. The syntax for the `default adac detection` command is:

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

The `default adac detection` command is in the config-if command mode.

["default adac detection command parameters and variables" \(page 128\)](#) describes the parameters and variables for the `default adac detection` command.

default adac detection command parameters and variables

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

adac port enable command

The `adac port enable` command enables Auto-Detection on specified ports.

The syntax for the `adac port enable` command is:

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

where <port-list> specifies the ports to enable with ADAC.

The `adac port enable` command is in the config-if command mode.

no adac port enable command

The `no adac port enable` command disables Auto-Detection on the specified ports.

The syntax for the `no adac port enable` command is:

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

where `<port-list>` specifies the adac ports to disable.

The `no adac port enable` command is in the config-if command mode.

default adac port enable

The `default adac port enable` command restores the default ADAC setting (disabled) for the specified ports. The syntax for the `default adac port enable` command is:

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

where `<port-list>` identifies the port to configure with default values.

The `default adac port enable` command is in the config command mode.

adac mac-range-table command

The `adac mac-range-table` command adds a specified range to the table of MAC addresses recognized as Nortel IP Phones by the Auto-Detection process.

The syntax for the `adac mac-range-table` command is:

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

where `<MACaddress>` specifies the low-end and high-end MAC addresses in the range.

The `adac mac-range-table` command is in the config command mode.

no adac mac-range-table command

The `no adac mac-range-table` command deletes an existing MAC address range used by the Auto-Detection process.

The syntax for the `no adac mac-range-table` command is:

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

where `<MACaddress>` specifies the low-end and high-end MAC addresses of the range to delete.

Note: If the low-end and high-end MAC address values are not provided, the switch deletes all existing MAC address ranges from the switch.

The `no adac mac-range-table` command is in the config command mode.

default adac mac-range-table command

The `default adac mac-range-table` command restores all supported MAC address ranges on the switch to their default values.

The syntax for the `default adac mac-range-table` command is:

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

The `default adac mac-range-table` command is in the config command mode.

show adac command

The `show adac` command displays the global ADAC settings for the device.

The syntax for the `show adac` command is:

```
show adac
```

The `show adac` command is in the exec command mode.

"[show adac command output](#)" (page 130) displays sample output from the `show adac` command.

show adac command output

```
5530-24TFD(config)#show adac
      ADAC Global Configuration
-----
ADAC Admin State:  Enabled
ADAC Oper State:  Enabled
Operating Mode:   Untagged Frames Basic
Traps Control Status:  Enabled
Voice-VLAN ID:   None
Call Server Port:  None
Uplink Port:     None
```

show adac interface command

The `show adac interface` command displays the ADAC settings for a particular port.

The syntax for the `show adac interface` command is:

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

where `<interface-type>` is the interface type, and `<slot/port>` specifies the port.

The `show adac interface` command is in the `privExec` command mode.

"[show adac interface command output](#)" (page 131) displays sample output from the `show adac interface` command.

show adac interface command output

```
5530-24TFD(config)#show adac interface 1/1
      Auto      Oper      Auto
Port Type Detection State Configuration T-F PVID T-F Tagging
-----
1    T    Enabled  Enabled  Applied      No Change Untag PVID Only
```

show adac mac-range-table command

The `show adac mac-range-table` command displays the ADAC MAC ranges configured on the switch.

The syntax for the `show adac mac-range-table` command is:

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

The `show adac mac-range-table` command is in the `privExec` command mode.

show adac detection interface command

The `show adac detection interface` command displays the detection mechanism configured per port.

The syntax for the `show adac detection interface` command is:

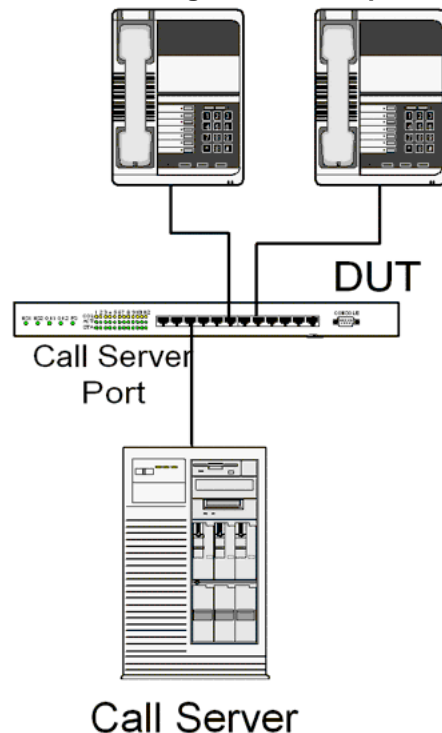
```
show adac detection interface [<interface-type>] [<interface-id>]
```

where `<interface-type>` is the interface type, and `<interface-id>` specifies the interface ID.

The `show adac detection interface` command is in the `privExec` command mode.

ADAC UFA configuration example

"[ADAC UFA configuration example](#)" (page 132) shows an example of ADAC configured in Untagged-Frames-Advanced (UFA) op-mode. (Call-server-port is used in this example, because the server is directly connected to the 5500 series switch.)

ADAC UFA configuration example

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

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

To configure the example shown in "[ADAC UFA configuration example](#)" ([page 132](#)), you must perform the following tasks:

Step	Action
1	Configure the call-server port.
2	Configure voice-VLAN.
3	Configure Untagged-Frames-Advanced (UFA) op-mode.
4	Enable ADAC on all ports to which IP phones connect.
5	Configure IP phones to send untagged traffic.
6	Enable the LLDP-MED Capabilities TLV on the ports used by IP phones.
7	Enable the LLDP-MED Network Policy TLV for transmission. This prevents configuration mismatches by enabling the IP Phone to obtain its policy settings directly from the switch.

—End—

ADAC configuration commands

The following section describes the detailed CLI commands required to carry out the configuration shown in ["ADAC UFA configuration example" \(page 132\)](#).

```
(config)#adac call-server-port 7
(config)#adac voice-vlan 2
(config)#adac enable op-mode untagged-frames-advanced
(config)#interface fastEthernet all
(config)#interface fastEthernet 16,24 enable
(config-if)#lldp tx-tlv port 16,24 med med-capabilities
(config-if)#lldp tx-tlv port 16,24 med network-policy
```

Verifying new ADAC settings

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

Auto configuration settings

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

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

VLAN settings**(config)#show vlan**

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

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

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

ADAC settings**(config)#show running-config**

```
!...
! *** ADAC *** Note information in this section.
!
no adac enable
no adac mac-range-table
interface FastEthernet ALL
adac port 24 enable
no adac port 1-23 enable
exit
adac mac-range-table low-end 00-0A-E4-01-10-20 high-end
00-0A-E4-01-23-A7
adac mac-range-table low-end 00-0A-E4-01-70-EC high-end
00-0A-E4-01-84-73
adac mac-range-table low-end 00-0A-E4-01-A1-C8 high-end
00-0A-E4-01-AD-7F
adac mac-range-table low-end 00-0A-E4-01-DA-4E high-end
00-0A-E4-01-ED-D5
adac mac-range-table low-end 00-0A-E4-02-1E-D4 high-end
00-0A-E4-02-32-5B
adac mac-range-table low-end 00-0A-E4-02-5D-22 high-end
00-0A-E4-02-70-A9
adac mac-range-table low-end 00-0A-E4-02-D8-AE high-end
00-0A-E4-02-FF-BD
adac mac-range-table low-end 00-0A-E4-03-87-E4 high-end
00-0A-E4-03-89-0F
adac mac-range-table low-end 00-0A-E4-03-90-E0 high-end
00-0A-E4-03-B7-EF
```

```
adac mac-range-table low-end 00-0A-E4-04-1A-56 high-end
00-0A-E4-04-41-65
adac mac-range-table low-end 00-0A-E4-04-80-E8 high-end
00-0A-E4-04-A7-F7
adac mac-range-table low-end 00-0A-E4-04-D2-FC high-end
00-0A-E4-05-48-2B
adac mac-range-table low-end 00-0A-E4-05-B7-DF high-end
00-0A-E4-06-05-FE
adac mac-range-table low-end 00-0A-E4-06-55-EC high-end
00-0A-E4-07-19-3B
adac mac-range-table low-end 00-0A-E4-08-0A-02 high-end
00-0A-E4-08-7F-31
adac mac-range-table low-end 00-0A-E4-08-B2-89 high-end
00-0A-E4-09-75-D8
adac mac-range-table low-end 00-0A-E4-09-BB-9D high-end
00-0A-E4-09-CF-24
adac mac-range-table low-end 00-0A-E4-09-FC-2B high-end
00-0A-E4-0A-71-5A
adac mac-range-table low-end 00-0A-E4-0A-9D-DA high-end
00-0A-E4-0B-61-29
adac mac-range-table low-end 00-0A-E4-0B-BB-FC high-end
00-0A-E4-0B-BC-0F
adac mac-range-table low-end 00-0A-E4-0B-D9-BE high-end
00-0A-E4-0C-9D-0D
adac traps enable
adac voice-vlan 2
adac call-server-port 7
no adac uplink-port
adac op-mode untagged-frames-advanced
adac enable
!
```

Creating and Managing VLANs using the Web-based Management Interface

The following sections detail how to create and manage a VLAN using the Web-based Management Interface. VLAN creation and management is performed in the VLAN Configuration screen illustrated in "[VLAN Configuration screen](#)" (page 136).

VLAN Configuration screen

Application > VLAN > VLAN Configuration

VLAN Table							
Action	VLAN	VLAN Name	VLAN Type	Protocol	User Defined Protocol	Learning Constraint	State
		1	VLAN #1	Port	None	0x0	IVL Active

VLAN Creation
 VLAN Type: Port
 Create VLAN

VLAN Setting
 Management VLAN:
 Submit

VLAN ConfigControl Setting
 VLAN ConfigControl: Strict
 Submit

For details, refer to the following sections:

- "Creating a Port-based VLAN" (page 136)
- "Creating a Protocol-based VLAN" (page 137)
- "Modifying a Port-based VLAN" (page 141)
- "Modifying a Protocol-based VLAN" (page 142)
- "Selecting a Management VLAN" (page 144)
- "Deleting a VLAN configuration" (page 144)

Creating a Port-based VLAN

To create a port-based VLAN, perform the following tasks:

Step	Action
1	Select Application > VLAN > VLAN Configuration . The VLAN Configuration page appears.
2	In the VLAN Creation section, select Port .
3	Click Create VLAN .

- 4 In the **Port Based Settings** screen, type a number for the VLAN between 2 and 4094 in the **VLAN Number** field and, optionally, a name for the VLAN in the **VLAN Name** field.
- 5 Click **Submit**.

—End—

The new VLAN is displayed in the VLAN Configuration page.

When a new VLAN has been created, it must be modified to add ports. Consult "[Modifying a Port-based VLAN](#)" (page 141) for information about performing this task.

Creating a Protocol-based VLAN

To create a protocol-based VLAN, perform the following tasks:

- | Step | Action |
|------|---|
| 1 | Select Application > VLAN > VLAN Configuration .
The VLAN Configuration page appears. |
| 2 | In the VLAN Creation section, select Protocol . |
| 3 | Click Create VLAN . |
| 4 | In the Protocol Based Settings screen, fill in the required information to create the VLAN. The following table describes the fields on this screen. |

Protocol Based Settings fields

Field	Description
VLAN	The unique number between 2 and 4094 that identifies the VLAN.
VLAN Name	The name of the VLAN.

Field	Description
Protocol	The protocol that this VLAN will use. Consult " Standard protocol-based VLANs and PID types " (page 138) for an explanation of these protocols.
User Defined Protocol	<p>If ProtocolUser Defined was selected from the list, specify the protocol identifier for the VLAN.</p> <p>Note: Any frames that match the specified PID in any of the following ways are assigned to that user-defined VLAN:</p> <ul style="list-style-type: none"> • The ethertype for Ethernet type 2 frames • The PID in Ethernet SNAP frames • The DSAP or SSAP value in Ethernet 802.2 frames <p>For a list of reserved PIDs that are unavailable for user-defined PIDs, see "Predefined Protocol Identifiers" (page 140).</p>

5 Click **Submit**.

—End—

The new VLAN is displayed in the VLAN Configuration page.

When a new VLAN is created, it must be modified to add ports. Consult "[Modifying a Protocol-based VLAN](#)" (page 142) for information about performing this task.

"[Standard protocol-based VLANs and PID types](#)" (page 138) outlines the standard protocol-based VLAN and PID types supported by the Nortel Ethernet Routing Switch 5500 Series.

Standard protocol-based VLANs and PID types

PID Name	Encapsulation	PID Value (Hex)	VLAN Type
IP Ether2	Ethernet type 2	0800, 0806	Standard IP on Ethernet Type 2 frames
IPX 802.3	Ethernet 802.3	FFFF	Novell IPX on Ethernet 802.3 frames

PID Name	Encapsulation	PID Value (Hex)	VLAN Type
IPX 802.2	Ethernet 802.2	E0 E0	Novell IPX on Ethernet 802.2 frames
IPX Snap	Ethernet Snap	8137, 8138	Novell IPX on Ethernet SNAP frames
IPX Ethernet II	Ethernet type 2	8137, 8138	Novell IPX on Ethernet Type 2 frames
DEC Lat	Ethernet type 2	6004	DEC LAT protocol
SNA Ethernet II	Ethernet type 2	80D5	IBM SNA on Ethernet Type 2 frames
NetBios	Ethernet type 2	F0**, **F0	NetBIOS protocol
XNS	Ethernet type 2	0600, 0807	Xerox XNS
Vines	Ethernet type 2	0BAD	Banyan VINES
IPv6	Ethernet type 2	86DD	IP version 6
RARP	Ethernet type 2	8035	<p>Reverse Address Resolution Protocol (RARP):</p> <p>RARP is a protocol used by some old diskless devices to obtain IP addresses by providing the MAC layer address. When you create a VLAN based on RARP, you can limit the RARP broadcasts to the ports that lead to the RARP server.</p>
User-Defined	Ethernet type 2, Ethernet 802.2, or Ethernet Snap	User-defined 16 bit value	<p>If you select User Defined from the Protocol list, specify the protocol identifier for the VLAN.</p> <p>Note: Any frames that match the specified PID, in any of the following ways are assigned to that user defined VLAN:</p>

PID Name	Encapsulation	PID Value (Hex)	VLAN Type
			<ul style="list-style-type: none"> The ethertype for Ethernet type 2 frames The PID in Ethernet SNAP frames The DSAP or SSAP value in Ethernet 802.2 frames. <p>For a list of reserved PIDs that are unavailable for user-defined PIDs, see "Predefined Protocol Identifiers" (page 140).</p>

"[Predefined Protocol Identifiers](#)" (page 140) outlines reserved PIDs that are not available in user-defined PIDs.

Predefined Protocol Identifiers

PID Name	Encapsulation	PID Value (Hex)	VLAN Type
IPX 802.3	Ethernet 802.3	FF FF	Novell IPX on Ethernet 802.3 frames
IPX 802.2	Ethernet 802.2	E0 E0	Novell IPX on Ethernet 802.2 frames
IPX Snap	Ethernet Snap	8137, 8138	Novell IPX on Ethernet SNAP frames
IP Ether2	Ethernet type 2	0800, 0806	Standard IP on Ethernet Type 2 frames
IPX Ethernet II	Ethernet type 2	8137, 8138	Novell IPX on Ethernet Type 2 frames
ApITk Ether2 Snap	Ethernet type 2 or Ethernet Snap	809B, 80F3	AppleTalk on Ethernet Type 2 and Ethernet Snap frames
Declat Ether2	Ethernet type 2	6004	DEC LAT protocol
Sna Ether2	Ethernet type 2	80D5	IBM SNA on Ethernet Type 2 frames
NetBios 802.2	Ethernet type 2	F0**, **F0	NetBIOS protocol

PID Name	Encapsulation	PID Value (Hex)	VLAN Type
Xns Ether2	Ethernet type 2	0600, 0807	Xerox XNS
Vines Ether2	Ethernet type 2	0BAD	Banyan VINES
Ipv6 Ether2	Ethernet type 2	86DD	IP version 6
User-Defined	Ethernet type 2, Ethernet 802.2, or Ethernet Snap	User-defined 16 bit value	User-defined protocol-based VLAN
IPX 802.3	Ethernet 802.3	FF FF	Novell IPX on Ethernet 802.3 frames

Modifying a Port-based VLAN

To modify an existing port-based VLAN, perform the following procedure:

Step	Action
------	--------

- From the menu, select **Applications > VLAN > VLAN Configuration**.
The VLAN Configuration page appears.
- In the **VLAN Table** section, select the VLAN to be modified by clicking the **Modify** icon in the appropriate VLAN row.
"VLAN Table section" (page 144) illustrates an example of the VLAN Table section.
- The VLAN Configuration: Port Based screen appears ("VLAN Configuration: Port Based screen" (page 142)). On this screen, modify port membership for the VLAN by selecting check boxes to add a port to the VLAN or clearing check boxes to remove a port.
"VLAN Configuration: Port Based fields" (page 141) describes the fields present on the VLAN Configuration: Port Based screen.

VLAN Configuration: Port Based fields

Field	Description
VLAN	The number assigned to the VLAN when it was created. This field is noneditable.
VLAN Name	The name assigned to the VLAN when it was created.

Field	Description
Learning Constraint	All Nortel Ethernet Routing Switch 5500 Series switches have a learning constraint of IVL. This means that the VLAN uses a filtering database that is independent of all other VLANs.
Unit/Port Membership	Select the check boxes of stand-alone or stacked unit ports to associate them with the VLAN. If the port is already a member, clear the check box to remove it as a member of the VLAN.

4 Click **Submit**.

—End—

The modified VLAN is now displayed in the VLAN Table section ("[VLAN Table section](#)" (page 144)) of the VLAN Configuration screen.

VLAN Configuration: Port Based screen

Modifying a Protocol-based VLAN

To modify a protocol-based VLAN, follow this procedure:

Step	Action
------	--------

1	From the menu, select Applications > VLAN > VLAN Configuration .
---	---

The VLAN Configuration page appears.

2	In the VLAN Table section, select the VLAN to be modified by clicking the Modify icon in the appropriate VLAN row.
---	--

"[VLAN Table section](#)" (page 144) illustrates an example of the VLAN Table section.

- 3 The **VLAN Configuration: Protocol Based** screen appears ("VLAN Configuration: Protocol Based screen" (page 143)). On this screen, modify port membership for the VLAN by selecting check boxes to add a port to the VLAN or clearing check boxes to remove a port.

"VLAN Configuration: Protocol based fields" (page 143) outlines the fields present on the VLAN Configuration: Protocol Based screen.

VLAN Configuration: Protocol based fields

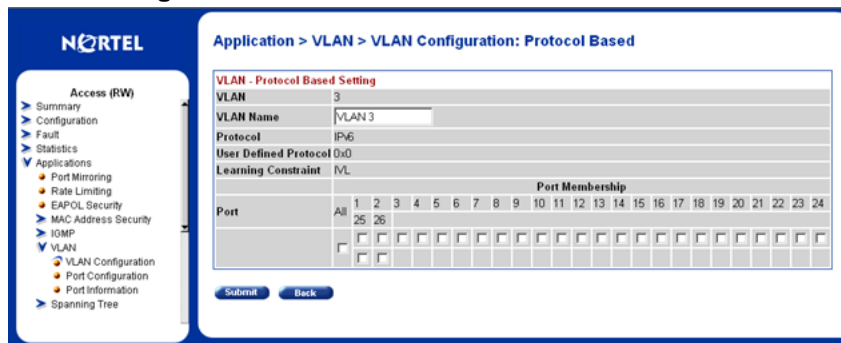
Field	Description
VLAN	The number assigned to the VLAN when it was created. This field is noneditable.
VLAN Name	The name assigned to the VLAN when it was created.
Learning Constraint	All Nortel Ethernet Routing Switch 5500 Series switches have a learning constraint of IVL. This means that the VLAN uses a filtering database that is independent of all other VLANs.
Unit/Port Membership	Select the check boxes of stand-alone or stacked unit ports to associate them with the VLAN. If the port is already a member, clear the check box to remove it as a member of the VLAN.

- 4 Click **Submit**.



—End—

The modified VLAN is now displayed in the **VLAN Table** section ("VLAN Table section" (page 144)) of the **VLAN Configuration** screen.

VLAN Configuration: Protocol Based screen



VLAN Table section

VLAN Table							
Action	VLAN	VLAN Name	VLAN Type	Protocol	User Defined Protocol	Learning Constraint	State
		1	VLAN #1	Port	None	0x0	IVL Active

Modify

Delete

Selecting a Management VLAN

Any VLAN can be selected to perform as the management VLAN. VLAN 1 is the default management VLAN for the switch. To set this field, the **VLAN State** field value must be **Active**.

To select a VLAN as the management VLAN:

Step	Action
1	From the main menu, choose Application > VLAN > VLAN Configuration . The VLAN Configuration page appears (" VLAN Configuration screen " (page 136)).
2	In the VLAN Setting section, choose the VLAN to assign as your management VLAN.
3	Click Submit .

—End—

Deleting a VLAN configuration

To delete a VLAN configuration:

Step	Action
1	From the main menu, choose Application > VLAN > VLAN Configuration . The VLAN Configuration page appears (" VLAN Configuration screen " (page 136)).
2	In the VLAN Table section, click the Delete icon for the entry you want to delete. This section is illustrated in " VLAN Table section " (page 144).
3	A dialog box appears asking for confirmation of the delete action.

Do one of the following:

- Click **Yes** to delete the VLAN configuration.
- Click **Cancel** to return to the **VLAN Configuration** page without making changes.

—End—

Flushing the MAC address table using Web-based management

You can flush the MAC address table of dynamically-learned MAC addresses. The MAC flush functionality allows you to flush:

- one MAC address
- all MAC addresses
- one VLAN
- one port or a list of ports
- one trunk

To flush MAC addresses from the MAC address table:

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the main menu, choose Configuration > MAC Address Table . |
|---|--|

The MAC Address Table configuration screen appears.

MAC Address Table Configuration

Configuration > MAC Address Table

MAC Address Setting

Aging Time seconds

Select VLAN

MAC Flush

Address

MAC Address Table
(Number of addresses: 11)

MAC Address	Source
00-03-BA-5B-DB-E6	Port: 35
00-04-38-D5-70-C1	Port: 35
00-04-DC-80-56-A1	Port: 35

MAC Flush field description

Field	Description
MAC Flush	<p>The type of addresses to flush from the MAC address table. Choose from the following:</p> <ul style="list-style-type: none"> Address, enter the MAC address to flush VLAN, enter the VLAN number Port, enter the port number or the port range Trunk, enter the trunk number All

- 2 Select the type of **MAC Flush**.
- 3 Type the MAC address, the VLAN or trunk number, or the port number or range. These examples illustrate how to enter port ranges for the Flush Port command.

Flushing out ports 1 and 2 on a standalone unit example
Flush Port 1,2

Flushing out ports 1-10 on unit 2 and 1-7 on unit 3 of a stack example

Flush Port 2/1-10,3/1-7

- 4 Click **Submit**.

—End—

Configuring ADAC for Nortel IP Phones using Web-based management

You can configure the settings for Auto-Detection and Auto-Configuration (ADAC) of Nortel IP Phones using Web-based management. For more information about the ADAC feature, see ["Auto-Detection and Auto-Configuration of Nortel IP Phones"](#) (page 93).

This section contains the following topics:

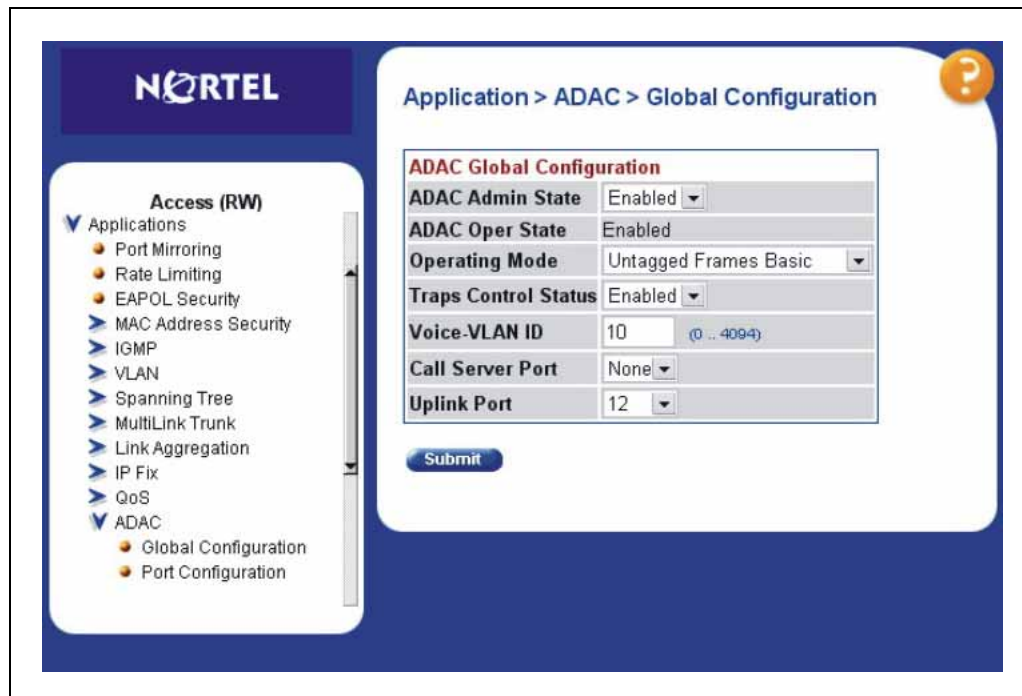
- ["Configuring global ADAC properties"](#) (page 147)
- ["Configuring ADAC port properties"](#) (page 149)
- ["Configuring ADAC MAC address ranges"](#) (page 151)
- ["Configuring ADAC Port Detection"](#) (page 153)

Configuring global ADAC properties

To configure the global ADAC settings:

Step	Action
1	From the main menu, choose Application > ADAC > Global Configuration . The Global Configuration page appears (" ADAC Global Configuration " (page 148)).

ADAC Global Configuration



"ADAC Global Configuration field description" (page 148) describes the fields in the Global Configuration page.

ADAC Global Configuration field description

Field	Description
ADAC Admin State	Enables and disables ADAC (sets the admin state).
ADAC Oper State	Read-only: Displays the ADAC operating state, either Enabled or Disabled
Operating Mode	Sets the ADAC operation mode: <ul style="list-style-type: none"> Tagged Frames: IP Phones send tagged frames. Untagged Frames Advanced: IP Phones send untagged frames, and the Voice VLAN is created. Untagged Frames Basic: IP Phones send untagged frames, and the Voice VLAN is not created.
Traps Control Status	Enables and disables ADAC trap notifications.
Voice VLAN ID	Sets the Voice VLAN ID.

Field	Description
Call Server Port	Sets the Call Server port.
Uplink Port	Sets the Uplink port.

- 2 From the ADAC list, select **Enabled**.
- 3 Choose the Operating Mode.
- 4 In the **Traps Control Status** field, enable or disable trap notifications.
- 5 Enter the Voice VLAN ID.
- 6 Choose the Call Server port and unit and the Uplink port and unit from the lists.
- 7 Click **Submit**.

—End—

Configuring ADAC port properties

To configure the ADAC port settings:

Step	Action
1	<p>From the main menu, choose Application > ADAC > Port Configuration.</p> <p>The Port Configuration page ("ADAC Port Configuration" (page 150)) appears.</p>

ADAC Port Configuration

Application > ADAC > Port Configuration

ADAC Port Configuration

Unit **1** 2 3 4 5

Port	Type	Auto Detection	Oper State	Auto Configuration	Tagged-Frames PVID	Tagged-Frames Tagging
1	T	Enabled	Enabled	Not Applied	0	Untag PVID Only
2	T	Enabled	Enabled	Not Applied	0	Untag PVID Only
3	T	Enabled	Enabled	Not Applied	0	Untag PVID Only
4	T	Enabled	Enabled	Not Applied	0	Untag PVID Only
5	T	Enabled	Enabled	Not Applied	0	Untag PVID Only
6	T	Enabled	Enabled	Not Applied	0	Untag PVID Only
7	T	Enabled	Disabled	Not Applied	0	Untag PVID Only
8	T	Enabled	Enabled	Not Applied	0	Untag PVID Only
9	T	Enabled	Enabled	Not Applied	0	Untag PVID Only
10	T	Enabled	Enabled	Not Applied	0	Untag PVID Only
11		Disabled	Disabled	Not Applied	0	Untag PVID Only
12		Disabled	Disabled	Not Applied	0	Untag PVID Only
Switch		Disabled			0	Untag PVID Only
Stack		Disabled			0	Untag PVID Only

Unit **1** 2 3 4 5

Submit

[Ports 13 - 24](#) [Ports 25 - 36](#) [Ports 37 - 48](#)

- 2 Choose the **Auto-Detection** setting for each port from the lists as required.
- 3 Type the Tagged-Frames Port VLAN ID (PVID) into the **Tagged-Frames PVID** box for each port. A value of 0 means the PVID remains unchanged.

- 4 Choose the **Tagged-Frames Tagging** mode setting for each port from the list.
- 5 Click **Submit**.

—End—

Configuring ADAC MAC address ranges

Configure the ADAC MAC address ranges.

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the main menu, choose Applications > ADAC > MAC Range Table .

The MAC Range Table page appears. |
|---|--|

ADAC MAC Range Table

The screenshot shows the web interface for an Ethernet Routing Switch 5520. The browser window title is "Ethernet Routing Switch 5520 - 24T - PWR - 10.3.2.39 - Mozilla Firefox". The address bar shows "http://10.3.2.39/". The page title is "Application > ADAC > MAC Range Table".

ADAC MAC Range Table Control

Operation: Reset To Defaults

Low End MAC Address: (XX-XX-XX-XX-XX-XX)

High End MAC Address: (XX-XX-XX-XX-XX-XX)

Submit

ADAC MAC Range Table

Action	Lowest MAC Address	Highest MAC Address
X	00-0A-E4-01-10-20	00-0A-E4-01-23-A7
X	00-0A-E4-09-BB-9D	00-0A-E4-09-CF-24
X	00-0A-E4-0A-9D-DA	00-0A-E4-0B-61-29
X	00-0A-E4-0B-BB-FC	00-0A-E4-0B-BC-0F

Total Ranges 4

Done

"MAC Range Table page items" (page 153) describes the fields in the MAC Range Table page.

MAC Range Table page items

Section	Field	Description
ADAC MAC Range Table Control	Operation	<p>From this field, you can choose to perform one of the following actions:</p> <ul style="list-style-type: none"> Reset To Defaults: resets the MAC address range to default values. Delete All Ranges: deletes all existing MAC address ranges. Add Range: adds a range specified by the Low End and High End MAC Address fields. Delete Range: deletes a range specified by the Low End and High End MAC Address fields. <p>To complete the chosen action, click Submit.</p>
	Low End MAC Address	Specifies the low-end address of the range to add or delete.
	High End MAC Address	Specifies the high-end address of the range to add or delete.
ADAC MAC Range Table	Action	Deletes the specified MAC address range.
	Lowest MAC Address	Specifies the low-end of the MAC address range.
	Highest MAC Address	Specifies the high-end of the MAC address range.

- 2 Type the Low End and High End MAC addresses for the new range you want to add.
- 3 Click Submit.

—End—

Configuring ADAC Port Detection

Configure the ADAC port detection settings.

Step Action

- 1 From the main menu, choose **Applications > ADAC > Port Detection**.

ADAC Port Detection

The screenshot shows the web interface for an Ethernet Routing Switch 5510. The browser address bar shows `http://10.100.7.70/`. The page title is "Application > ADAC > Port Detection". On the left, a navigation menu under "Access (RW)" includes "ADAC" with sub-items: "Global Configuration", "Port Configuration", "Port Detection", and "MAC Range Table".

The main content area is titled "ADAC Port Detection" and features a unit selector (Unit 1, 2, 3, 4, 5) and a table with the following data:

Port	MAC Detection	LLDP Detection
1	Enabled	Enabled
2	Enabled	Enabled
3	Enabled	Enabled
4	Enabled	Enabled
5	Enabled	Enabled
6	Enabled	Enabled
7	Enabled	Enabled
8	Enabled	Enabled
9	Enabled	Enabled
10	Enabled	Enabled
11	Enabled	Enabled
12	Enabled	Enabled
Switch	Enabled	Enabled
Stack	Enabled	Enabled

Below the table is another unit selector (Unit 1, 2, 3, 4, 5) and a "Submit" button. At the bottom, there are links for "Ports 13 - 24", "Ports 25 - 36", and "Ports 37 - 48".

"ADAC port detection field description" (page 155) describes the fields in the ADAC Port Detection page.

ADAC port detection field description

Field	Description
MAC Detection	Enables or disables MAC detection by port, switch or stack. The default setting is Enabled .
LLDP Detection	Enables or disables LLDP detection by port, switch or stack. The default setting is Enabled .

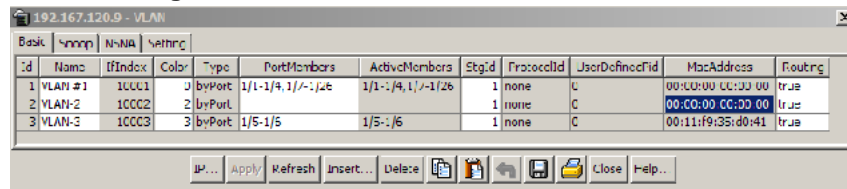
- 2 Enable or disable the **MAC Detection** and the **LLDP Detection** setting for each port.
- 3 Click **Submit**

—End—

Creating and Managing VLANs using the Java Device Manager

The following sections detail how to create and manage a VLAN using the Java Device Manager (JDM). VLAN creation and management is performed in the VLANs dialog box illustrated in "VLANs dialog box" (page 155).

VLANs dialog box



The VLAN Basic tab fields are described in the following table.

VLAN Basic tab

Field	Description
Id	The VLAN ID for the VLAN.
Name	Name of the VLAN.
Ifindex	Displays port numbers.
Color	An administratively assigned color code for the VLAN. The value of this object is used by the VLAN Manager GUI tool to select a color when it draws this VLAN on the screen.
Type	Indicates the type of VLAN: byPort or byProtocolId.
PortMembers	Ports that are members of the VLAN.

Field	Description
ActiveMembers	Set of ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met.
StgId	Identifies the spanning tree group to which the VLAN belongs. This field is only available when the switch is running in Nortel STPG mode.
MstpInstance	This field is only available when the switch is running in MSTP mode.
ProtocolId	Protocol for protocol-based VLANs. This value is taken from the Assigned Numbers RFC. For port-based VLANs, None is the displayed value.
UserDefinedPid	When rcVlanProtocolId is set to usrDefined(15) in a protocol-based VLAN, this field represents the 16-bit user-defined protocol identifier.
MacAddress	The unique hardware address of the device.
Routing	Specifies whether routing is enabled (true) or disabled (false) on the VLAN.

This section contains information about the following topics:

- ["Setting VLAN Configuration Control" \(page 156\)](#)
- ["Enabling AutoPVID" \(page 157\)](#)
- ["Creating a VLAN" \(page 158\)](#)
- [" Modifying a VLAN" \(page 160\)](#)
- ["Deleting VLANs" \(page 161\)](#)
- ["Configuring VLAN port properties" \(page 161\)](#)
- ["Configuring IGMP snooping" \(page 162\)](#)
- ["Assigning an IP address to a VLAN" \(page 163\)](#)
- ["Configuring VLAN DHCP" \(page 164\)](#)
- ["Configuration of ADAC for Nortel IP Phones using Device Manager " \(page 171\)](#)

Setting VLAN Configuration Control

To access VLAN Configuration Control, use the following procedure.

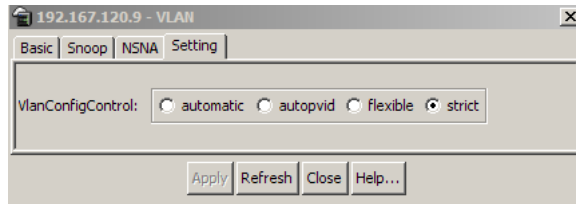
Step	Action
------	--------

- | | |
|---|---|
| 1 | From the Device Manager, click VLAN . |
| 2 | Select VLANs . The VLAN dialog box opens. |

3 Click the **Setting** tab. The **VLAN Setting** tab appears.

—End—

VLAN Setting tab



The following table describes the selections available on the VLAN Setting tab.

VLAN Setting tab field

Field	Description
VlanConfigControl	<p>VlanConfigControl presents four selections:</p> <ul style="list-style-type: none"> <p>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</p> <p>autopvid: When an untagged port is added to a new VLAN, the port is added to the new VLAN and the PVID assigned to the new VID without removing it from any previous VLAN memberships. Using this option, an untagged port can have membership in multiple VLANs.</p> <p>flexible: This selections 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.</p> <p>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.</p>

Enabling AutoPVID

A Port VLAN ID can be automatically assigned to any port by enabling the AutoPVID functionality on the switch. To enable this functionality through the JDM, follow this procedure:

Step	Action
1	From the menu, select Edit > Chassis . The Chassis dialog box appears with the System tab selected.
2	On the System tab, select enabled in the AutoPVID field.
3	Click Apply .

—End—

Creating a VLAN

To create a VLAN, follow this procedure:

Step	Action
1	From the JDM menu, select VLAN > VLANs . The VLANs dialog box appears.
2	Click Insert . The Insert Basic dialog box for creating VLANs appears (" VLANs Insert Basic dialog box " (page 159)). This dialog box appears with the Type field set to byPort.

VLANs Insert Basic dialog box

- 3 Enter the identifier for the VLAN in the **Id** field. This value must be a unique number between 2 and 4094.
- 4 Optionally, enter a name for the VLAN in the **Name** field.
- 5 Optionally, assign a color identifier to the VLAN in the **Color** field.
- 6 Enter the value of the Spanning Tree Group to which the VLAN will belong in the **StgId** field.
- 7 When in Nortel STPG mode, use the **StgId** menu to choose the spanning tree group to which the VLAN is to belong. When in MSTP mode, use the **MstpInstance** list to select the CIST or MSTI instance to which the VLAN is to belong.
- 8 Select the type of VLAN in the **Type** field.
 - a. If the VLAN is to be port-based, select the **byPort** option button.
 - b. If the VLAN is to be protocol-based, select the **byProtocolId** option button. This selection enables the **ProtocolId** field. From this field select the protocol on which this VLAN will be based. If it is to be based on a user-defined protocol, select the **usrDefined** option button and enter the custom PID in the **UserDefinedPid** field.
- 9 Click **Insert**.

—End—

The new VLAN is created and displayed in the VLANs Basic tab. To add or remove ports from the VLAN, the VLAN must be modified. Consult "[Modifying a VLAN](#)" (page 160) for details.

Modifying a VLAN

After a VLAN is created, four types of information can be modified without the need to recreate the VLAN:

1. VLAN Name
2. Color Identifier
3. Member Ports
4. Routing status

To change the VLAN name, color identifier, or routing status, click in the appropriate fields in the VLANs Basic tab and then click **Apply**.

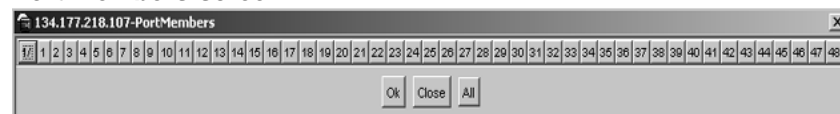
To change the VLAN member ports, follow this procedure:

Step	Action
------	--------

- 1 In the row that represents the VLAN that is to be modified, double-click in the **PortMembers** field.

The Port Members screen ("[Port Members screen](#)" (page 160)) appears.

Port Members screen



- 2 Click the buttons that correspond to the ports that are to be added or deleted from the VLAN. Click **All** to select all switch ports.
- 3 Click **OK**.
- 4 Click **Apply**.

—End—

The VLANs Basic tab refreshes with the correct port numbers listed in the PortMembers field.

Deleting VLANs

To delete a VLAN:

Step	Action
1	From the JDM menu, select VLAN > VLANs . The VLANs dialog box appears with the Basic tab selected.
2	Select the VLAN to be deleted.
3	Click Delete .

—End—

The JDM deletes the selected VLAN.

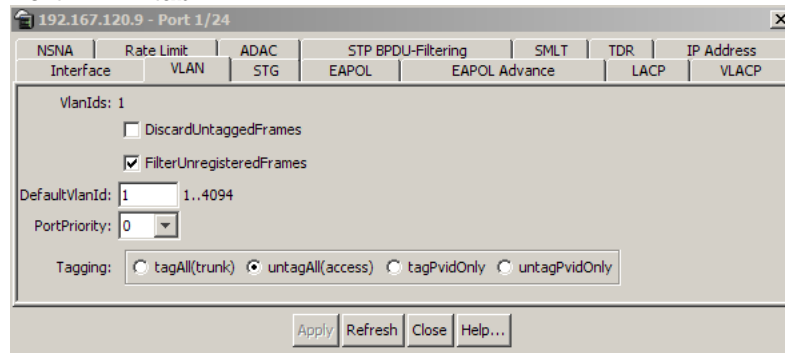
Configuring VLAN port properties

The Port - VLAN tab displays the VLAN membership for a port.

To view the Port - VLAN tab:

Step	Action
1	From the Device View, select the port to edit.
2	From the menu, choose Edit > Port . The Port dialog box appears.
3	Select the VLAN tab. The following illustration shows the Port -- VLAN tab.

Port VLAN tab



VLAN tab items for a single port

Field	Description
VlanIds	The VLANIDs of which this port is a member.

Field	Description
DiscardUntaggedFrames	This field only applies to trunk ports. It acts as a flag used to determine how to process untagged frames received on this port. When the flag is set, the frames are discarded by the forwarding process. When the flag is reset, the frames are assigned to the VLAN specified by rcVlanPortDefaultVlanId.
FilterUnregisteredFrames	This field only applies to access ports. It acts as a flag used to determine how to process unregistered frames received on this port. When the flag is set, the frames are discarded by the forwarding process. When the flag is reset, the frames are processed normally.
DefaultVlanId	The VLAN ID assigned to untagged frames received on a trunk port.
PortPriority	Set the port priority value from the list as a value between 0 and 7.
Tagging	Indicates the type of VLAN port. A trunk port can be a member of more than one VLAN. An access port can be a member of only VLAN, if no membership conflict exists. There are four types of VLAN port: <ul style="list-style-type: none"> • tagAll(trunk) • untagAll(access) • tagPvidOnly • untagPvidOnly

4 Click **Apply** after making any changes.

—End—

Configuring IGMP snooping

Use the Snoop tab on the VLANs dialog box to enable or disable IGMP snooping on a switch.

For information on this tab and on the IGMP snooping feature, refer to *Nortel Ethernet Routing Switch 5500 Series Configuration — IP Routing Protocols* (NN47200-503).

Assigning an IP address to a VLAN

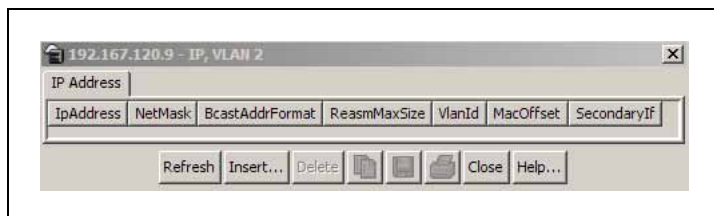
Note: Before assigning an IP address to a VLAN, ensure that IP forwarding is turned on. For information about configuring IP forwarding, refer to *Nortel Ethernet Routing Switch 5500 Series Configuration — IP Routing Protocols* (NN47200-503).

The first IP address assigned to a VLAN is the primary IP address. You can assign up to eight subsequent IP addresses to the VLAN, for a total of eight secondary IP interfaces.

To assign an IP address to a VLAN, follow this procedure:

Step	Action
1	From the JDM menu, select VLAN > VLANs . The VLANs dialog box appears.
2	Highlight the VLAN to which an IP address is to be assigned.
3	Click IP . The IP VLAN dialog box appears with the IP Address tab selected. The following illustration shows the IP Address tab.

IP Address tab



IP Address tab fields

Field	Description
IpAddress	The device IP address.
NetMask	The subnet mask address.
BcastAddrFormat	The IP broadcast address format used on this interface.
ReasmMaxSize	The size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface
VlanId	The VLAN number. A value of -1 indicates that the VLAN ID is ignored.

Field	Description
MacOffset	Used to translate the IP address into a MAC address. You can either mention a MAC offset while configuring an IP on the VLAN or it can be allotted by the system within the above range.
SecondaryIf	The SecondaryIf field is set to True if the VLAN IP address is a secondary IP address and False if the IP address for the VLAN is the primary IP address.

- 4 Click **Insert**. The Insert IP Address dialog box appears ("Insert IP Address screen" (page 164)).

Insert IP Address screen



- 5 Type the **IP Address**, **Subnet Mask**, and **Mac Address Offset** in the fields provided.
- 6 Click **Insert**.

—End—

Configuring VLAN DHCP

Note: Before you can view the DHCP tab, you must first enable routing on the switch. For more information about IP routing configuration, refer to *Nortel Ethernet Routing Switch 5500 Series Configuration - IP Routing Protocols*, part number NN47200-503.

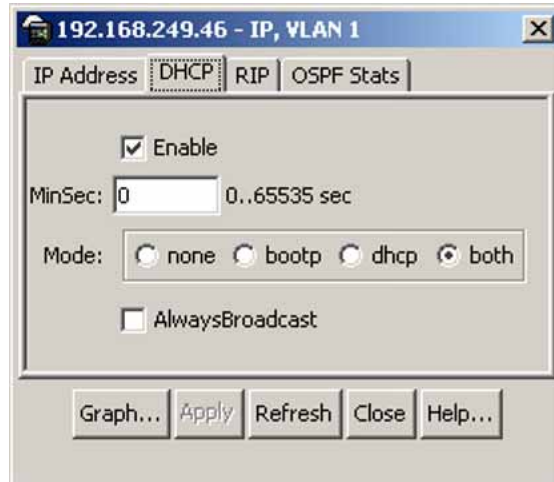
To configure DHCP for a VLAN, follow this procedure:

Step Action

- From the JDM menu, select **VLAN > VLANs**.
The VLANs dialog box appears.
- Highlight the VLAN for which DHCP is to be configured.

- 3 Click **IP**.
The IP VLAN screen appears.
- 4 Select the **DHCP** tab. This tab is illustrated in "DHCP tab fields" (page 165).

DHCP tab fields



DHCP tab fields

Field	Description
Enable	Specifies whether DHCP is enabled or disabled.
MinSec	Indicates the minimum number of seconds to wait between receiving a DHCP packet and actually forwarding the DHCP packet to the destination device. A value of zero (0) indicates forwarding is done immediately without any delay.
Mode	Indicates what type of DHCP packets this interface supports. A value of none (1) results in all incoming DHCP and BOOTP packets being dropped.
AlwaysBroadcast	Indicates if DHCP Reply packets are broadcast to the DHCP client on this interface.

- 5 Make changes as necessary in the fields provided.
- 6 Click **Apply**.

—End—

Graphing DHCP statistics

To graph DHCP statistics:

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the DHCP tab, click Graph . |
|---|--|

The DHCP tab for graphing appears.

DHCP tab for graphing

	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
NumRequests	0	0	0	0	0	0
NumReplies	0	0	0	0	0	0

DHCP graphing tab fields

Field	Description
NumRequests	The total number of DHCP requests seen on this interface.
NumReplies	The total number of DHCP replies seen on this interface.

—End—

Configuring NSNA per VLAN

To configure NSNA for a VLAN, use the procedure in this section.

ATTENTION

VLANs that you plan to configure as Nortel SNA VLANs must be empty (that is, they have no port members assigned). Nortel SNA VLANs cannot be associated with non-Nortel SNA ports; therefore you cannot assign non-NSNA ports manually to enabled NSNA VLANs.

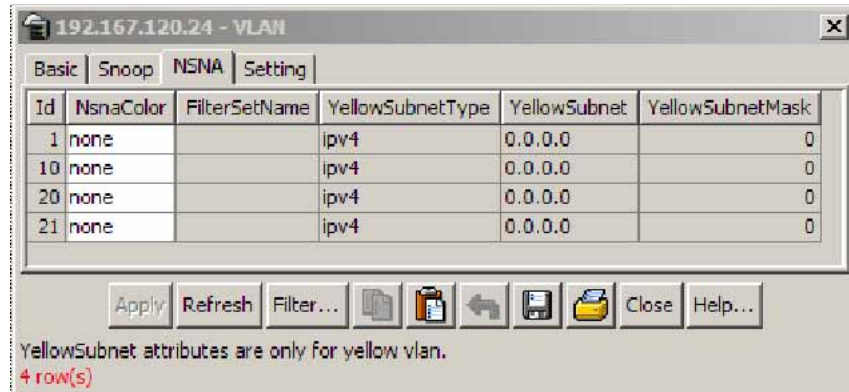
Dumb and static devices that cannot authenticate through tunnel guard can be connected to NSNA dynamic ports. To ensure network access for these devices, add the MAC addresses to the SNAS MAC database.

Configuring NSNA per VLAN

Step	Action
------	--------

- 1 From the Device Manager main menu, select **VLAN**. The VLAN menu opens.
- 2 Select **VLAN**. The VLAN dialog appears with the Basic tab open.
- 3 Select the **NSNA** tab.

VLAN NSNA tab



VLAN NSNA tab fields

Field	Description
Id	Specifies the VLAN identification number.
NsnaColor	Specifies the NSNA VLAN color.
FilterSetName	Specifies the filter set name. Note: NsnaColor field must be only red, yellow, or green.
YellowSubnetType	Specifies the Ethernet type for the Yelooow VLAN subnet. Note: NsnaColor field must be set to yellow.
YellowSubnet	Specifies the Yellow VLAN subnet. Note: NsnaColor field must be set to yellow.
YellowSubnetMask	Specifies the Yellow VLAN subnet mask. Note: NsnaColor field must be set to yellow..

- 4 Select a VLAN to modify.
- 5 Double click the **NsnaColor** field. A menu appears.
- 6 Select one of the following options from the menu:

- none
- red
- green
- yellow
- voip

ATTENTION

Although each switch can have multiple Yellow, Green, and VoIP VLANs, each switch must have only one Red VLAN.

- 7 In the other columns, enter parameters compatible with the NsnaColor selection.
- 8 Click **Apply**.

—End—

For more information about Nortel SNA, refer to *Nortel Ethernet Routing Switch 5500 Series Configuration - Security*, NN47200-501.

Deleting an NSNA VLAN

To remove an NSNA VLAN, use the procedure in this section.

Note: NSNA must be globally disabled before you can delete an NSNA VLAN.

Deleting an NSNA VLAN

Step	Action
1	To globally disable NSNA, from the Device Manager menu, select Edit .
2	Select Security .
3	Select NSNA . The NSNA dialog appears with the NSNAS tab open.
4	Select the Globals tab.
5	Clear the Enabled check box.

NSNA Globals tab



- 6 From the Device Manager menu, select **VLAN**. The VLAN dialog appears with the Basic tab open.
- 7 Select the **NSNA** tab.
- 8 Select the VLAN to delete and double click the **NsnasColor** field.
- 9 From the list, select **none**.
- 10 Click **Apply**.
- 11 Select the **Basic** tab.
- 12 Select the VLAN to delete (the VLAN for which the NsnasColor was changed to none).
- 13 Click **Delete**.

—End—

Filtering an NSNA VLAN

To filter an NSNA VLAN, use the following procedure.

Filtering an NSNA VLAN

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the Device Manager main menu, select VLAN . The VLAN menu appears. |
| 2 | From the VLAN menu, select VLANs . The VLAN dialog appears with the Basic tab open. |
| 3 | Select NSNA . |

- 4 Click **Filter**. The **VLAN, NSNA - Filter** dialog opens.
- 5 Set the filter parameters.
- 6 Click **Filter**.

—End—

MAC address table maintenance using the Device Manager

You can flush the MAC address table using Device Manager. For more information about the MAC address table, see ["Managing the MAC address forwarding database table"](#) (page 117).

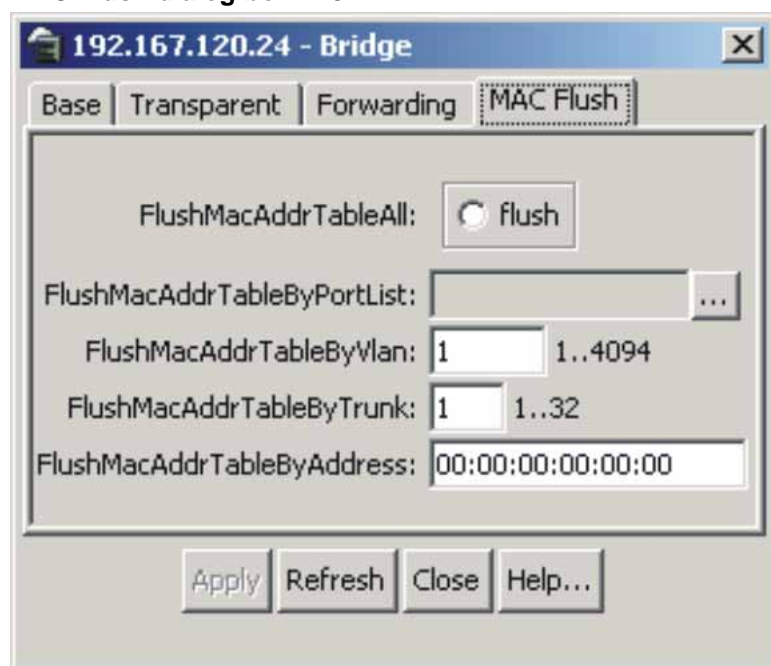
Flushing the MAC address table

Flush dynamically learned MAC addresses from the MAC address forwarding table.

Step	Action
------	--------

- 1 Go to the MAC flush commands by choosing **Edit > Bridge > MAC Flush**. The MAC Flush dialog box appears.

MAC Flush dialog box in JDM



MAC flush fields

Field	Description
FlushMacAddrTableAll	Flushes all MAC addresses from MAC address table.
FlushMacAddrTableByPortlist	Flushes the MAC addresses for port(s) specified from the MAC address table.
FlushMacAddrTableByVlan	Flushes the MAC addresses for the VLAN specified from the MAC address table.
FlushMacAddrTableByTrunk	Flushes the MAC addresses for the MultiLink Trunk specified from the MAC address table.
FlushMacAddrTableByAddress	Flushes the specified MAC addresses from MAC address table.

- 2 Click **flush** or type the MAC address, VLAN, trunk, port, or portlist in the corresponding box.
- 3 Click **Apply**.

—End—

Configuration of ADAC for Nortel IP Phones using Device Manager

You can configure ADAC-related settings using Device Manager. For more information about the ADAC feature, see "[Auto-Detection and Auto-Configuration of Nortel IP Phones](#)" (page 93) .

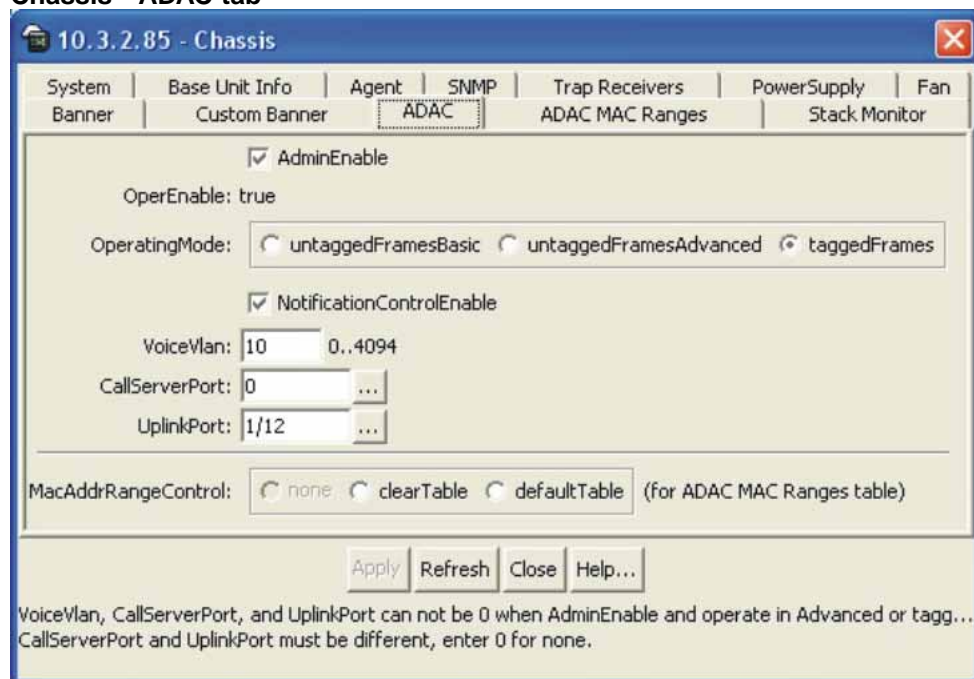
Configuring global ADAC settings

Configure the global ADAC settings.

Step Action

- 1 From the Device Manager menu bar, choose **Edit > Chassis**.
The Chassis dialog box appears.
- 2 Choose the **ADAC** tab.
The ADAC tab appears.

Chassis - ADAC tab



VoiceVlan, CallServerPort, and UplinkPort can not be 0 when AdminEnable and operate in Advanced or tagg...
CallServerPort and UplinkPort must be different, enter 0 for none.

Chassis - ADAC tab field description

Field	Description
AdminEnable	Enables and disables ADAC.
OperEnable	Indicates ADAC operational state: true is enabled and false is disabled. Note: If AdminEnable is True and OperEnable is False, this indicates an error condition such as missing Uplink and Call Server ports.
OperatingMode	Sets the ADAC operation mode: <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 and disables ADAC trap notifications.
VoiceVLAN	Sets the Voice VLAN ID.

Field	Description
CallServerPort	Sets the Call Server port.
UplinkPort	Sets the Uplink port.
MacAddrRangeControl	Provides two options for configuring the MAC address range table: <ul style="list-style-type: none"> clearTable: clears the MAC address range table. defaultTable: sets the MAC address range table to its default values.

- 3 Select the **AdminEnable** field to enable ADAC.
- 4 Choose the Operating Mode.
- 5 In the **NotificationControlEnable** field, enable or disable trap notifications.
- 6 Enter the Voice VLAN ID, Call Server port, and Uplink port.
- 7 Click **Apply**.

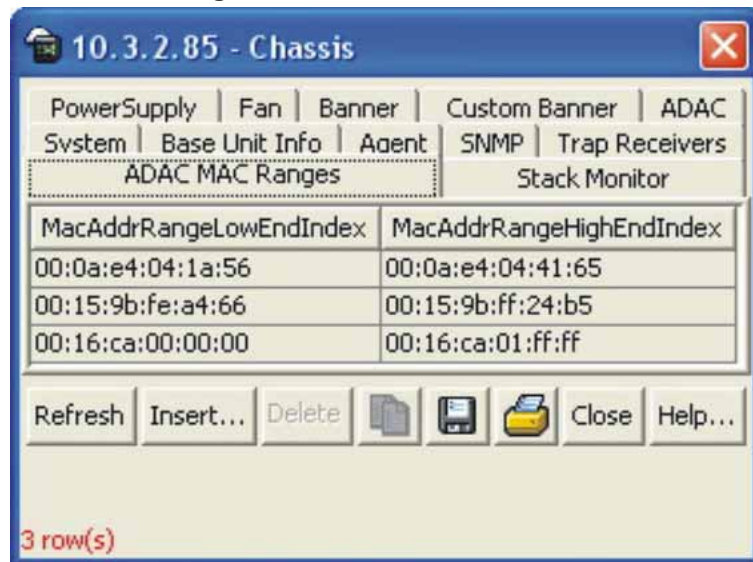
—End—

Configuring ADAC MAC address ranges using Device Manager

Add MAC address ranges to the ADAC MAC address range table.

Step	Action
------	--------

- 1 From the Device Manager menu bar, choose **Edit > Chassis**.
The Chassis dialog box appears, with the System tab displayed.
- 2 Choose the **ADAC MAC Ranges** tab.
The ADAC MAC Ranges tab appears.

ADAC MAC Ranges tab

- 3 Click **Insert**.
The Chassis, Insert ADAC MAC Ranges window appears.
- 4 In the **MacAddrRangeLowEndIndex** field, enter the low-end of the MAC address range to add.
- 5 In the **MacAddrRangeHighEndIndex** field, enter the high-end of the MAC address range to add.
- 6 Click **Insert**.

—End—

Deleting MAC address ranges using Device Manager

Delete MAC address ranges from the ADAC MAC address range table.

Step Action

- 1 From the Device Manager menu bar, choose **Edit > Chassis**.
The Chassis dialog box appears, with the System tab displayed.
- 2 Choose the **ADAC MAC Ranges** tab.
The ADAC MAC Ranges tab appears.
- 3 Select the desired range to delete.
- 4 Click **Delete**.

—End—

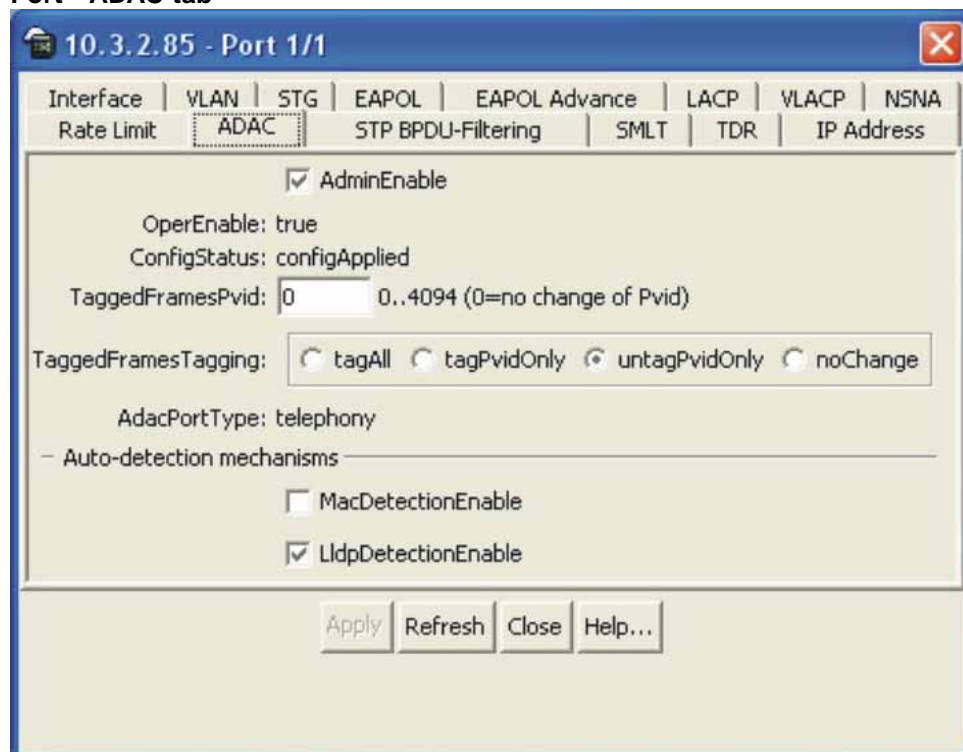
Configuring ADAC settings on a port

Configure ADAC settings on a port.

Step	Action
------	--------

- | | |
|---|--|
| 1 | <p>Highlight a port, and from the Device Manager menu bar, choose Edit > Port.</p> <p>The Port dialog box appears, with the Interface tab displayed.</p> |
| 2 | <p>Click the ADAC tab.</p> <p>The ADAC tab appears.</p> |

Port - ADAC tab



Port - ADAC tab field description

Field	Description
AdminEnable	Enables or disables ADAC for the port.

Field	Description
OperEnable	Indicates ADAC operational state: true is enabled and false is disabled. Note: If OperEnable is False and AdminEnable is True, then Auto-Detection/Auto-Configuration is disabled. This can occur due to a condition such as reaching the maximum number of devices supported per port.
ConfigStatus	(Read only) Describes the ADAC status for the port: <ul style="list-style-type: none"> • configApplied means that the ADAC configuration is applied to this port. • configNotApplied means that the ADAC configuration is not applied to this port.
TaggedFramesPVID	Unique PVID between 1 and 4094. A value of 0 indicates that Auto-Configuration cannot change the PVID for the respective port.
TaggedFramesTagging	Choose <ul style="list-style-type: none"> • tagAll to tag all frames • tagPvidOnly to tag frames by the unique PVID • untagPvidOnly to untag frames by the unique PVID • noChange to accept frames without change
AdacPortType	Describes how ADAC classifies the port: <ul style="list-style-type: none"> • telephony (when Auto-Detection is enabled for the port) • callServer • uplink • none

Field	Description
MacDetectionEnable	True indicates that Auto-Detection of Nortel IP Phones, based on MAC address, is enabled on the interface. False indicates that Auto-Detection of Nortel IP Phones, based on MAC address, is disabled on the interface. NOTE: MacDetectionEnable cannot be set to false if no other supported detection mechanism is enabled on the port.
LldpDetectionEnable	True indicates that Auto-Detection of Nortel IP Phones, based on 802.1ab is enabled on the interface. False indicates that Auto-Detection of Nortel IP Phones, based on 802.1ab, is disabled on the interface. NOTE: LldpDetectionEnable cannot be set to False if no other supported detection mechanism is enabled on the port.

- 3 To enable ADAC for the port, select the **AdminEnable** check box. To disable ADAC for the port, clear the **AdminEnable** check box.
- 4 In the **TaggedFramesPvid** box, type a number between 0 and 4094, where 0 means "no change."
- 5 Click on the **TaggedFramesTagging** setting required.
- 6 Select **MacDetectionEnable** or **LldpDetectionEnable** or select them both to enable the detection methods on the port.
- 7 Click **Apply**.

—End—

Configuring Spanning Tree Protocol

Spanning Tree Protocol (STP) can be configured in the Nortel Ethernet Routing Switch 5500 Series through the Console Interface, Command Line Interface, Web-based Management Interface, or the Java Device Manager. This chapter outlines the configuration and management of STP using these switch interfaces.

This chapter contains the following topics:

- "Configuring Spanning Tree using the Console Interface" (page 179)
- "Setting the STP mode using the CLI" (page 209)
- "Creating and Managing STGs using the CLI" (page 210)
- "Managing RSTP using the CLI" (page 218)
- "Managing MSTP using the CLI" (page 221)
- "Setting the STP mode using the Web-based Management Interface" (page 227)
- "Creating and Managing STGs using the Web-based Management Interface" (page 228)
- "Configuring RSTP using Web-based management" (page 238)
- "Configuring MSTP using Web-based management" (page 241)
- "Setting the STP mode using Device Manager" (page 252)
- "Configuring STP BPDU Filtering using Device Manager" (page 252)
- "Creating and Managing STGs using Device Manager" (page 253)
- "Configuring RSTP using Device Manager" (page 263)
- "Configuring MSTP using Device Manager" (page 271)

Configuring Spanning Tree using the Console Interface

The following sections provide instructions for configuring Spanning Tree in the three modes.

- "Spanning Tree configuration in STPG mode" (page 180)

- "Spanning Tree configuration in RSTP mode" (page 190)
- "Spanning Tree configuration in MSTP mode" (page 198)

Spanning Tree configuration in STPG mode

From the Spanning Tree Configuration Menu screen ("Spanning Tree Configuration menu screen in STPG mode" (page 180)) in the STPG mode (IEEE 802.1d), you can view Spanning Tree parameters and configure individual switch ports to participate in the Spanning Tree Algorithm.

To open the Spanning Tree Configuration Menu screen:

- Choose **Spanning Tree Configuration** (or press **p**) from the main menu.

Spanning Tree Configuration menu screen in STPG mode

```

Spanning Tree Configuration Menu

Spanning Tree Group Configuration...
Spanning Tree Port Configuration...
Display Spanning Tree Switch Settings...
Display Spanning Tree VLAN Membership...
Return to Main Menu

Use arrow keys to highlight option, press <Return> or <Enter> to select option.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

```

"Spanning Tree Configuration Menu options in STPG mode." (page 180) describes the **Spanning Tree Configuration Menu** options.

Spanning Tree Configuration Menu options in STPG mode.

Option	Description
Spanning Tree Group Configuration	Displays the Spanning Tree Group Configuration screen. (See "Spanning Tree Group Configuration screen in STPG mode" (page 181).)
Spanning Tree Port Configuration	Displays the Spanning Tree Port Configuration screen. (See "Spanning Tree Port Configuration screen in STPG mode" (page 183).)
Display Spanning Tree Switch Settings	Displays the Spanning Tree Switch Settings screen. (See "Spanning Tree Switch Settings screen in STPG mode" (page 186).)
Display Spanning Tree VLAN Membership	Displays the Spanning Tree VLAN Membership screen.

Spanning Tree Group Configuration screen in STPG mode

To open the Spanning Tree Group Configuration screen

Step	Action
------	--------

- | | |
|---|---|
| 1 | Choose Spanning Tree Group Configuration (or press g) from the Spanning Tree Configuration Menu screen. |
|---|---|

Spanning Tree Group Configuration screen in STPG mode

```

Spanning Tree Group Configuration

STP Mode:                               STPG (Nortel MSTP)
Create STP Group:                        [ 1 ]
Delete STP Group:                        [   ]
Bridge Priority (in Hex):                 [ 8000 ]
Bridge Hello Time:                       [ 2 seconds ]
Bridge Max. Age Time:                    [ 20 seconds ]
Bridge Forward Delay Time:               [ 15 seconds ]
Add VLAN Membership:                     [ 1 ]
Delete VLAN Membership:                  [   ]
Tagged BPDU on tagged port:              [ No ]
UID used for Tagged BPDU:                [ 4001 ]
STP Multicast Address:                   [ 01-80-C2-00-00-00 ]
STP Group State:                         [ Active ]

Enter number, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

```

Spanning Tree Group Configuration parameters in STPG mode

Parameter	Description
STP Mode	Shows the current STP operational mode for switch/stack. The modes available are: <ul style="list-style-type: none"> STPG (Nortel MSTP) RSTP (IEEE 802.1w) MSTP (IEEE 802.1s)
Create STP Group	Creates a spanning tree group. Default value 1 Range 1 to 8
Delete STP Group	Deletes a spanning tree group. Default value Blank Range Configured STP groups from 1 to 8

Parameter	Description
Bridge Priority (in Hex)	<p>For the STP Group, configures the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values.</p> <p>Default value 0x8000</p> <p>Range 0x0000 to 0xF000</p>
Bridge Hello Time	<p>Configures the Hello Interval (the amount of time between transmissions of BPDUs) for the STP Group. This parameter takes effect only when this bridge becomes the root bridge.</p> <p>Note: Although you can set the Hello Interval for a bridge using bridge management software, after the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network.</p> <p>Default value 2 seconds</p> <p>Range 1 to 10 seconds</p>
Bridge Max. Age Time	<p>For the STP Group, configures the maximum age (in seconds) that a Hello message can attain before being discarded. This parameter takes effect only when the bridge becomes the root bridge.</p> <p>Note: If this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network.</p> <p>Default value 20 seconds</p> <p>Range 6 to 40 seconds</p>
Bridge Forward Delay Time	<p>For the STP Group, configures the Forward Delay parameter value for this bridge. This parameter takes effect only when this bridge becomes the root bridge.</p> <p>The Forward Delay parameter value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state.</p> <p>Note: All bridges participating in the spanning tree network use the root bridge Forward Delay parameter value.</p>

Parameter	Description
	Default value 15 seconds Range 4 to 30 seconds
Add VLAN Membership	Adds a VLAN to the specified spanning tree group. Default value 1 Range 1 to 4094.
Delete VLAN Membership	Deletes a VLAN from the specified spanning tree group. Default value Blank Range Configured VLANs from 1 to 4094
Tagged BPDU on tagged port	Specifies whether to send tagged or untagged BPDUs from a tagged port. Default value STP Group 1: No; Other STP Groups: Yes Range No or Yes
VID used for tagged BPDU	Specifies the VLAN ID (VID) for tagged BPDU for the specified spanning tree group. Default value 4001 to 4008 for STGs 1 through 8, respectively Range 1 to 4094
STP Multicast Address	Specifies the STP Multicast Address. Default value 01-80-C2-00-00-00
STP Group State	Sets the STP Group to active or inactive. Note: You cannot set the default STG (STG 1) to Inactive. Default value Active for STG 1; Inactive for STGs 2 to 8 Range Active or Inactive

—End—

Spanning Tree Port Configuration screen in STPG mode

With the Spanning Tree Port Configuration screen ("[Spanning Tree Port Configuration screen in STPG mode](#)" (page 184)), you can configure individual switch ports or all switch ports to participate in the Spanning Tree.

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

Field	Description
Participation	<p>Configures any (or all) of ports on the switch for Spanning tree participation.</p> <p>When an individual port is a trunk member, changing this setting for one trunk member changes the setting for all members of that trunk. Consider how this can change your network topology before you change this setting.</p> <p>The Fast Learning parameter is the same as Normal Learning, except that the state transition timer is shortened to 2 seconds.</p> <p>Default value Normal Learning</p> <p>Range Normal Learning, Fast Learning, Disabled</p>
Priority	<p>This read-only field is a bridge spanning tree parameter that prioritizes the lowest port path cost to the root. When one or more ports have the same path cost, STP selects the path with the highest priority (lowest numerical value).</p> <p>Default value 128</p> <p>Range 0 to 255</p>
Path Cost	<p>This read-only field is a bridge spanning tree parameter that determines the lowest path cost to the root.</p> <p>Default value in 802.1d mode:</p> <ul style="list-style-type: none"> • Path cost = 1000 / LAN speed in Mbyte/s • 1 for 1 Gigabit port <p>in 802.1t mode:</p> <ul style="list-style-type: none"> • Path cost = $2 \cdot 10^{10} / \text{LAN speed in Kbyte/s}$ • 20 000 for 1 Gigabit port (default on ERS5500) <p>•</p> <p>The higher the LAN speed, the lower the path cost.</p> <p>Range in 802.1d mode: 1 to 65535 in 802.1t mode: 1 to 200 000 000</p>

Field	Description				
State	<p>This read-only field indicates the current port state within the spanning tree network. Each port can transition to various states, as determined by the Participation field setting. For example, when the Participation field is set to Disabled, the port does not participate in the spanning tree and transitions to the Forwarding state (the default). When the Participation field is set to Enabled, the port transitions from the Disabled state through the Blocking, Listening, and Learning states before entering the Forwarding state.</p> <table data-bbox="568 541 1377 653"> <tr> <td data-bbox="568 541 981 583">Default value</td> <td data-bbox="981 541 1377 583">Topology dependent</td> </tr> <tr> <td data-bbox="568 583 981 653">Range</td> <td data-bbox="981 583 1377 653">Disabled, Blocking, Listening, Learning, Forwarding</td> </tr> </table>	Default value	Topology dependent	Range	Disabled, Blocking, Listening, Learning, Forwarding
Default value	Topology dependent				
Range	Disabled, Blocking, Listening, Learning, Forwarding				

Spanning Tree Switch Settings screen in STPG mode

With the Spanning Tree Switch Settings screen ("[Spanning Tree Switch Settings screen in STPG mode](#)" (page 186)), you can view spanning tree parameter values for the Ethernet Routing Switch 5500 Series.

To open the Spanning Tree Switch Settings screen:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Choose Display Spanning Tree Switch Settings (or press d) from the Spanning Tree Configuration Menu screen. |
|---|---|

Spanning Tree Switch Settings screen in STPG mode

```

Spanning Tree Switch Settings
STP Group: 1

STP Mode:              STPG (Nortel MSTP)
Bridge Priority:       8000
Designated Root:      8000001F9343401
Root Port:             0
Root Path Cost:        0
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

Enter number, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

```

Spanning Tree Switch Settings parameters in STPG mode

Parameter	Description
STP Group	<p>Specifies the number of the spanning tree group (STG) to view. To view another STG, type that STG ID number and press Enter, or press the spacebar on your keyboard to toggle the STP Group numbers.</p> <p>Default value 1</p> <p>Range Configured STP Groups from 1 to 8</p>
STP Mode	<p>Shows the current STP operational mode for switch/stack:</p> <ul style="list-style-type: none"> • Nortel MSTP (STPG) • IEEE 802.1w (RSTP) • IEEE 802.1s (MSTP)
Bridge Priority	<p>Indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values compared first, followed by the hardware addresses.</p> <p>Default value 0x8000</p> <p>Range HEX: 0x0000 - 0xF000</p>
Designated Root	Indicates the bridge ID of the root bridge, as determined by spanning tree.
Root Port	Indicates the switch port number that offers the lowest path cost to the root bridge.
Root Path Cost	<p>Indicates the path cost from this switch port to the root bridge.</p> <p>Default value 0</p> <p>Range Unit 1-8 Port 1-50 (in stack mode) Port 1-50 (in standalone mode)</p>
Hello Time	<p>Defines the amount of time between transmissions of BPDUs.</p> <p>Range 1 to 10 seconds</p>

Parameter	Description				
Bridge Forward Delay	<p>Indicates the Forward Delay parameter value specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge.</p> <p>The Forward Delay parameter value specifies the amount of time that the bridge ports remain in each of the Listening and Learning states before entering the Forwarding state.</p> <p>Note: All bridges participating in the spanning tree network use the root bridge Forward Delay parameter value.</p> <table> <tr> <td>Default value</td> <td>15 seconds</td> </tr> <tr> <td>Range</td> <td>4 to 30 seconds</td> </tr> </table>	Default value	15 seconds	Range	4 to 30 seconds
Default value	15 seconds				
Range	4 to 30 seconds				

—End—

Spanning Tree VLAN Membership screen in STPG mode

With the Spanning Tree VLAN Membership screen ("[Spanning Tree VLAN Membership screen in STPG mode](#)" (page 189)), you can view which VLANs belong to the selected STP Group. (STP Group 1 is the default STP group.)

To open the Spanning Tree VLAN Membership screen:

Step Action

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

Spanning Tree VLAN Membership screen in STPG mode

```

                                Spanning Tree VLAN Membership
                                STP Group: 1
Total VLAN Membership: 1
 1 ;

Enter number, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.
```

Spanning Tree VLAN Membership parameters

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

—End—

Spanning Tree configuration in RSTP mode

With the Spanning Tree Configuration Menu screen ("[Spanning Tree Configuration main menu in RSTP mode](#)" (page 190)), you can view spanning tree parameters and configure individual switch ports to participate in the Spanning Tree Algorithm (STA).

To open the Spanning Tree Configuration Menu screen:

Step	Action
------	--------

- | | |
|---|--|
| 1 | Choose Spanning Tree Configuration (or press p) from the main menu. |
|---|--|

Spanning Tree Configuration main menu in RSTP mode

```

Spanning Tree Configuration Menu

Spanning Tree Group Configuration...
Spanning Tree Port Configuration...
Display Spanning Tree Switch Settings...
Return to Main Menu

Use arrow keys to highlight option, press <Return> or <Enter> to select option.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.
```

Spanning Tree Configuration main menu options

Menu option	Description
Spanning Tree Group Configuration	Displays the Spanning Tree Group Configuration screen. (See "Spanning Tree Group Configuration screen in RSTP mode" (page 191).)
Spanning Tree Port Configuration	Displays the Spanning Tree Port Configuration screen. (See "Spanning Tree Port Configuration screen in RSTP mode" (page 193).)
Display Spanning Tree Switch Settings	Displays the Spanning Tree Switch Settings screen. (See "Spanning Tree Switch Settings screen in RSTP mode" (page 195).)

—End—

Spanning Tree Group Configuration screen in RSTP mode

With the Spanning Tree Group Configuration screen ("Spanning Tree Group Configuration screen in RSTP mode" (page 191)), you can create and configure spanning tree groups (STGs).

To open the Spanning Tree Group Configuration screen:

Step Action

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

Spanning Tree Group Configuration screen in RSTP mode

```

Spanning Tree Group Configuration

STP Mode: IEEE 802.1w
Bridge Priority (in Hex): 8000
Bridge Hello Time: [ 2 seconds ]
Bridge Max. Age Time: [ 20 seconds ]
Bridge Forward Delay Time: [ 15 seconds ]
Bridge Tx Hold Count: [ 3 ]
Default Path Cost Type: [ 32 Bits ]

Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

```

Spanning Tree Group Configuration parameters in RSTP mode

Parameter	Description
STP Mode	Shows the current STP operational mode for switch/stack: <ul style="list-style-type: none">• Nortel MSTP (STPG)• IEEE 802.1w (RSTP)• IEEE 802.1s (MSTP)
Bridge Priority (in Hex)	For the STP Group, configures the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values. Default value 0x8000 Range 0x0000 to 0xF000
Bridge Hello Time	For the STP Group, configures the Hello Interval (the amount of time between transmissions of BPDUs). This parameter takes effect only when this bridge becomes the root bridge. Although you can set the Hello Interval for a bridge using bridge management software, after the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network. Default value 2 seconds Range 1 to 10 seconds
Bridge Max. Age Time	For the STP Group, configures the maximum age (in seconds) that a Hello message can attain before being discarded. This parameter takes effect only when the bridge becomes the root bridge. If this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. Default value 20 seconds Range 6 to 40 seconds

Spanning Tree Port Configuration screen in RSTP mode

Spanning Tree Port Configuration							
Port	STP Group: Trunk	CIST Learning	Edge	Priority	STP Mode: Path Cost	IEEE 802.1w Role	State
1		[Enabled]	No	128	20000	Disabled	Discarding
2		[Enabled]	No	128	20000	Disabled	Discarding
3		[Enabled]	No	128	200000	Designated	Forwarding
4		[Enabled]	No	128	20000	Disabled	Discarding
5		[Enabled]	No	128	20000	Disabled	Discarding
6		[Enabled]	No	128	20000	Disabled	Discarding
7		[Enabled]	No	128	2000000	Disabled	Discarding
8		[Enabled]	No	128	20000	Disabled	Discarding
9		[Enabled]	No	128	20000	Disabled	Discarding
10		[Enabled]	No	128	20000	Disabled	Discarding
11		[Enabled]	No	128	20000	Disabled	Discarding
12		[Enabled]	No	128	20000	Disabled	Discarding
13		[Enabled]	No	128	20000	Disabled	Discarding
14		[Enabled]	No	128	20000	Disabled	Discarding
More...							

Press Ctrl-N to display next screen.
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

Spanning Tree Port Configuration parameters in RSTP mode

Field	Description
Unit	This field appears only if the switch is participating in a stack configuration. The field specifies the number of the unit to view. To view another unit, type its unit number and press Enter, or press the spacebar on your keyboard to toggle the unit numbers.
Port	Indicates the switch port numbers that correspond to the field values in that row (for example, the field values in row 2 apply to switch port 2). The values in the Switch row affect all switch ports, and when the switch is part of a stack, the values in the Stack row affect all ports in the entire stack.
Trunk	The read-only data displayed in this column indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen.
Learning	Indicates the port states of Spanning Tree. Range: Enabled, Disabled
Edge	Indicates if a port is an Edge port. When a port is connected to a non-switch device such as a PC or a workstation, configure it as an Edge port. An active Edge port goes directly to Forwarding state without any delay.
Priority	This read-only field is a bridge spanning tree parameter that prioritizes the lowest port path cost to the root. When one or more ports have the same path cost, STP selects the path with the highest priority (lowest numerical value). Default value: 128 Range: 0 to 255

Field	Description
Path Cost	This read-only field is a bridge spanning tree parameter that determines the lowest path cost to the root. Default value 20000 for 1 Gigabit port Path cost = $2 \cdot 10^{10} / \text{LAN speed (in Kbits/s)}$ The higher the LAN speed, the lower the path cost. Range 1 to 200 000 000
Role	A role represents a functionality characteristic or capability of a resource to which policies are applied. The role of a port can be Root, Designated, Alternate, or Backup.
State	Indicates the current state of the Port as defined by the Rapid Spanning Tree Protocol. The state of a Port can be Forwarding in one instance and Discarding (Blocking) in another.

—End—

Spanning Tree Switch Settings screen in RSTP mode

With the Spanning Tree Switch Settings screen ("[Spanning Tree Switch Settings screen in RSTP mode](#)" (page 195)), you can view spanning tree parameter values for the Ethernet Routing Switch 5500 Series.

To open the Spanning Tree Switch Settings screen:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Choose Display Spanning Tree Switch Settings (or press d) from the Spanning Tree Configuration Menu screen. |
|---|---|

Spanning Tree Switch Settings screen in RSTP mode

```

Spanning Tree Switch Settings
STP Group: CIST

STP Mode: IEEE 802.1w
Bridge Priority: 8000
Designated Root: 80000011F9343400
Root Port: 0
Root Path Cost: 0
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
Tx Hold Count: 3
Default Path Cost Type: 32 Bits

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

```

Spanning Tree Switch Settings parameters in RSTP mode

Field	Description
STP Mode	Indicates the mode of the STP operation for the switch. The possible values for the STP mode are: <ul style="list-style-type: none">• STPG (Nortel MSTP)• RSTP (IEEE 802.1w)• MSTP (IEEE 802.1s)
Bridge Priority	Indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values compared first, followed by the hardware addresses. Default value 0x8000 Range HEX: 0x0000 - 0xF000
Designated Root	This field specifies the unique Bridge Identifier of the bridge. It is recorded as the CIST Root in the configuration BPDUs that are transmitted.
Root Port	Indicates the switch port number that offers the lowest path cost to the root bridge. The local switch is the root bridge when this value is 0 (path cost). Default value 0 Range Unit: 1-8, Port 1-50 (in stack mode) Port: 1-50 (in standalone mode)
Root Path Cost	Indicates the path cost from this switch port to the root bridge. Default value 0 Range Not applicable
Hello Time	Defines the amount of time between transmissions of BPDUs. Range 1 to 10 seconds

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

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

—End—

Spanning Tree configuration in MSTP mode

With the Spanning Tree Configuration Menu screen ("[Spanning Tree Configuration Menu in MSTP mode](#)" (page 199)), you can view spanning tree parameters and configure individual switch ports to participate in the spanning tree algorithm (STA).

To open the Spanning Tree Configuration Menu screen:

Step	Action
------	--------

- | | |
|----------|--|
| 1 | Choose Spanning Tree Configuration (or press p) from the main menu. |
|----------|--|

Spanning Tree Configuration Menu in MSTP mode

```

Spanning Tree Configuration Menu

Spanning Tree Group Configuration...
Spanning Tree Port Configuration...
Display Spanning Tree Switch Settings...
Display Spanning Tree VLAN Membership...
Return to Main Menu

Use arrow keys to highlight option, press <Return> or <Enter> to select option.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

```

Spanning Tree Configuration Menu options in MSTP mode

Option	Description
Spanning Tree Group Configuration	Displays the Spanning Tree Group Configuration screen (see "Spanning Tree Group Configuration screen in MSTP mode" (page 199)).
Spanning Tree Port Configuration	Displays the Spanning Tree Port Configuration screen (see "Spanning Tree Port Configuration screen in MSTP mode" (page 202)).
Display Spanning Tree Switch Settings	Displays the Spanning Tree Switch Settings screen (see "Spanning Tree Switch Settings screen in MSTP mode" (page 204)).
Display Spanning Tree VLAN Membership	Displays the Spanning Tree VLAN Membership screen (see "Spanning Tree VLAN Membership screen in MSTP mode" (page 208)).

—End—

Spanning Tree Group Configuration screen in MSTP mode

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

To open the Spanning Tree Group Configuration screen:

Step	Action
1	Choose Spanning Tree Group Configuration (or press g) from the Spanning Tree Configuration Menu screen.

Spanning Tree Group Configuration screen in MSTP mode

```

Spanning Tree Group Configuration

STP Mode: IEEE 802.1s
Create STP Group: [ CIST ]
Delete STP Group: [ ]
Bridge Priority (in Hex): [ 8000 ]
Bridge Max. Age Time: [ 20 seconds ]
Bridge Forward Delay Time: [ 15 seconds ]
Bridge Tx Hold Count: [ 3 ]
Max. Hop Count: [ 2000 ]
Default Path Cost Type: [ 32 Bits ]
Add VLAN Membership: [ 1 ]
Delete VLAN Membership: [ ]
STP Group State: Active

Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

```

Spanning Tree Group Configuration parameters in MSTP mode

Parameter	Description
STP mode	Indicates the STP mode in which the switch is operating. The available modes are: <ul style="list-style-type: none"> • STPG (Nortel MSTP) • RSTP (IEEE 802.1w) • MSTP (IEEE 802.1s)
Create STP Group	Creates a spanning Tree group. You can also use this parameter to select the STP Group information to display. Default value CIST Range 1 to 7 (MSTIs)
Delete STP Group	Deletes a spanning tree group. You cannot delete the CIST STP Group, and you can delete only nonactive STP Groups (that is, MSTIs). Default Value Blank Range 1 to 8; only created STP Groups are available
Bridge Priority	For the STP Group, configures the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. STP uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values. Default value 0x8000 Range 0x0000 -0xF000

Spanning Tree Port Configuration screen in MSTP mode

Spanning Tree Port Configuration								
Port	STP Group: Trunk	Group: CIST Learning	Edge	Priority	STP Mode: Path Cost	IEEE 802.1s Role	State	
1		[Enabled]	No	128	20000	Disabled	Discarding	
2		[Enabled]	No	128	20000	Disabled	Discarding	
3		[Enabled]	No	128	200000	Designated	Forwarding	
4		[Enabled]	No	128	20000	Disabled	Discarding	
5		[Enabled]	No	128	20000	Disabled	Discarding	
6		[Enabled]	No	128	20000	Disabled	Discarding	
7		[Enabled]	No	128	2000000	Disabled	Discarding	
8		[Enabled]	No	128	20000	Disabled	Discarding	
9		[Enabled]	No	128	20000	Disabled	Discarding	
10		[Enabled]	No	128	20000	Disabled	Discarding	
11		[Enabled]	No	128	20000	Disabled	Discarding	
12		[Enabled]	No	128	20000	Disabled	Discarding	
13		[Enabled]	No	128	20000	Disabled	Discarding	
14		[Enabled]	No	128	20000	Disabled	Discarding	
More...								

Press Ctrl-N to display next screen.
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

Spanning Tree Port Configuration screen fields in MSTP mode

Field	Description
STP Group	Specifies the MSTP instance for which to display the port properties. Press the spacebar to toggle between the CIST and the configured MSTI instances.
Port	Indicates the switch port numbers that correspond to the field values in that row (for example, the field values in row 2 apply to switch port 2). The values in the Switch row affect all switch ports, and when the switch is part of a stack, the values in the Stack row affect all ports in the entire stack.
Trunk	The read-only data displayed in this column indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen.
Learning	Configures any (or all) of the switch ports for Spanning tree participation. When an individual port is a trunk member (see Trunk field), changing this setting for one of the trunk members changes the setting for all members of that trunk. Consider how this will change your network topology before you change this setting. Default value Enabled
Edge	A value of Yes indicates that this port is to be assumed as an edge-port and a value of No indicates that this port is to be assumed as a non-edge port. Default value No Range No, Yes

Field	Description
Priority	<p>This read-only field is a bridge spanning tree parameter that prioritizes the lowest port path cost to the root. When one or more ports have the same path cost, STP selects the path with the highest priority (lowest numerical value).</p> <p>Default value 128</p> <p>Range 0 to 255</p>
Path Cost	<p>This read-only field is a bridge spanning tree parameter that determines the lowest path cost to the root.</p> <p>Default value Default value is 20000 for 1 Gigabit port</p> <p style="text-align: center;">Path Cost = $2 \times 10^{10} / \text{LAN speed (in Kbit/s)}$</p> <p style="text-align: center;">The higher the LAN speed, the lower the path cost.</p> <p>Range 1 to 200 000 000</p>
Role	<p>The current role of the port as defined by Multiple Spanning Tree Protocol.</p> <p>Default Disabled</p> <p>Range Disabled, Root, Designated, Alternate, Backup</p>
State	<p>This read-only field indicates the current port state within the spanning tree network. Each port can transition to various states, as determined by the Participation field setting. For example, when the Participation field is set to Disabled, the port does not participate in the spanning tree and transitions to the Forwarding state (the default). When the Participation field is set to Enabled, the port transitions from the Disabled state through the Blocking, Listening, and Learning states before entering the Forwarding state.</p> <p>Default value Topology dependent</p> <p>Range Discarding, Learning, Forwarding</p>

—End—

Spanning Tree Switch Settings screen in MSTP mode

With the Spanning Tree Switch Settings screen ("[Spanning Tree Switch Settings screen in MSTP mode](#)" (page 205)), you can view spanning tree parameter values for the Ethernet Routing Switch 5500 Series.

To open the Spanning Tree Switch Settings screen:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Choose Display Spanning Tree Switch Settings (or press d) from the Spanning Tree Configuration Menu screen. |
|---|---|

Spanning Tree Switch Settings screen in MSTP mode

```

Spanning Tree Switch Settings
STP Group: CIST

STP Mode: IEEE 802.1s
Bridge Priority: 8000
CIST Root: 80000011F9343400
Regional Root: 80000011F9343400
Root Port: 0
Root Path Cost: 0
Regional Root Path Cost: 0
Maximum Age Time: 20 seconds
Forward Delay: 15 seconds
Bridge Hold Time: 1 second
Bridge Maximum Age Time: 20 seconds
Bridge Forward Delay: 15 seconds
Tx Hold Count: 3
Hop Count: 2000
Default Path Cost Type: 32 Bits
Region Name:

Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

```

Spanning Tree Switch Settings parameters in MSTP mode

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

Parameter	Description
Root Port	<p>Indicates the switch port number that offers the lowest path cost to the root bridge. The local switch is the root bridge when this value is 0 (path cost).</p> <p>Range Unit: 1-8, Port 1-50 (in stack mode)</p> <p style="text-align: right;">Port: 1-50 (in standalone mode)</p>
Root Path Cost	<p>Indicates the path cost from this switch port to the root bridge.</p> <p>Default value 0</p> <p>Range Not applicable</p>
Regional Root Path Cost	<p>Indicates the Path Cost to CIST Regional Root seen from this device.</p>
Maximum Age Time	<p>Indicates the Maximum Age Time parameter value that the root bridge is currently using. This value specifies the maximum age that a Hello message can attain before being discarded.</p> <p>The root bridge Maximum Age Time parameter value becomes the actual Maximum Age Time parameter value for all bridges participating in the spanning tree network.</p> <p>Default value 20 seconds</p> <p>Range 6 to 40 seconds</p>
Forward Delay	<p>Indicates the Forward Delay parameter value that the root bridge is currently using. This value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state.</p> <p>The root bridge Forward Delay parameter value becomes the actual Forward Delay parameter value for all bridges participating in the spanning tree network.</p> <p>Default value 15 seconds</p> <p>Range 4 to 30 seconds</p>
Bridge Hold Time	<p>This value determines the time interval during which no more than two configuration BPDUs can be transmitted by this node.</p> <p>Default value 1 second</p>

Parameter	Description	
Region Name	Name of the Region. CIST External Root interprets devices from the same region as a single switch.	
	Default value	The MAC address of the device
	Range	1 to 32 chars (string)

—End—

Spanning Tree VLAN Membership screen in MSTP mode

With the Spanning Tree VLAN Membership screen ("[Spanning Tree VLAN Membership screen in MSTP mode](#)" (page 208)), you can view which VLANs belong to the selected STP Group. (The CIST is displayed by default.)

To open the Spanning Tree VLAN Membership screen:

Step Action

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

Spanning Tree VLAN Membership screen in MSTP mode

```

                                     Spanning Tree VLAN Membership
                                     STP Group: CIST
Total VLAN Membership: 1
  1  |

```

Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

Spanning Tree VLAN Membership parameters

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

—End—

Setting the STP mode using the CLI

You can set the STP operational mode with the following command:

spanning-tree op-mode

The `spanning-tree op-mode` command sets the STP operational mode to STPG (Nortel Multiple Spanning Tree Protocol), RSTP (802.1w Rapid Spanning Tree Protocol), or MSTP (802.1s Multiple Spanning Tree Protocol).

The syntax for the `spanning-tree op-mode` command is:

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

After you configure a change in STP protocols, you must initiate a manual reboot for the change to take effect.

The `spanning-tree op-mode` command is in the config command mode.

Configuring STP BPDU Filtering using the CLI

You can use the `spanning-tree bpdu-filtering` command to configure STP BPDU Filtering on a port. This command is available in all STP modes (STPG, RSTP, and MSTP).

The syntax for the `spanning-tree bpdu-filtering` command is:

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

The `spanning-tree bpdu-filtering` command is in the Interface Configuration command mode.

The following table describes the parameters for this command.

spanning-tree bpdu-filtering command parameters

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

To set the STP BPDU Filtering properties on a port to their default values, use the following command from the Interface Configuration command mode:

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

To disable STP BPDU Filtering on a port, use the following command from the Interface Configuration command mode:

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

To show the current status of the BPDU Filtering parameters, use the following command from the Privileged EXEC mode:

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

Creating and Managing STGs using the CLI

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

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

To configure STGs using the CLI, refer to the following:

- "spanning-tree cost-calc-mode command" (page 211)
- "spanning-tree port mode command" (page 211)
- "show spanning-tree command" (page 211)
- "spanning-tree stp create command" (page 212)

- "spanning-tree stp delete command" (page 212)
- "spanning-tree stp enable command" (page 213)
- "spanning-tree stp disable command" (page 213)
- "spanning-tree command" (page 213)
- "default spanning-tree command" (page 214)
- "spanning-tree add-vlan command" (page 215)
- "spanning-tree remove-vlan command" (page 215)
- "spanning-tree command by port" (page 216)
- "default spanning-tree command by port" (page 217)
- "no spanning-tree command by port" (page 218)

spanning-tree cost-calc-mode command

The `spanning-tree cost-calc-mode` command sets the path cost calculation mode for all Spanning Tree Groups on the switch.

The syntax for the `spanning-tree cost-calc-mode` command is:

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

where `dot1d` specifies IEEE 802.1d path cost, and `dot1t` specifies IEEE 802.1t path cost.

The `spanning-tree cost-calc-mode` command is in the Privileged EXEC command mode.

spanning-tree port mode command

The `spanning-tree port-mode` command sets the STG port membership mode for all Spanning Tree Groups on the switch. For details on the port membership mode, refer to "[STG port membership mode](#)" (page 35).

The syntax for the `spanning-tree port-mode` command is:

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

The `spanning-tree port-mode` command is in the Privileged EXEC command mode.

show spanning-tree command

The `show spanning-tree` command displays spanning tree configuration information that is specific to either the Spanning Tree Group or to the port.

The syntax for the `show spanning-tree` command is:

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

The `show spanning-tree` command is executed in the Privileged EXEC command mode.

The following table outlines the parameters for this command.

show spanning-tree parameters

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

spanning-tree stp create command

The `spanning-tree stp create` command creates a Spanning Tree Group.

The syntax for the `spanning-tree stp create` command is:

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

Substitute the <1-8> with the number of the Spanning Tree Group to create. By default, Spanning Tree Group 1 is already created.

The `spanning-tree stp create` command is executed in the Global Configuration command mode.

spanning-tree stp delete command

The `spanning-tree stp delete` command deletes a Spanning Tree Group.

The syntax for the `spanning-tree stp delete` command is:

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

Substitute the <1-8> with the number of the Spanning Tree Group to delete. Spanning Tree Group 1 cannot be deleted.

The `spanning-tree stp delete` command is executed in the Global Configuration command mode.

spanning-tree stp enable command

The `spanning-tree stp enable` command enables a Spanning Tree Group.

The syntax for the `spanning-tree stp enable` command is:

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

Substitute <1-8> with the number of the Spanning Tree Group to be enabled. Spanning Tree Group 1 is enabled always because it cannot be disabled.

The `spanning-tree stp enable` command is executed in the Global Configuration command mode.

spanning-tree stp disable command

The `spanning-tree stp disable` command disables a Spanning Tree Group.

The syntax for the `spanning-tree stp disable` command is:

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

Substitute <1-8> with the number of the Spanning Tree Group to be disabled. Spanning Tree Group 1 cannot be disabled.

The `spanning-tree stp disable` command is executed in the Global Configuration command mode.

spanning-tree command

The `spanning-tree` command sets STP values by STG.

The syntax for the `spanning-tree` command by STG is:

```
spanning-tree [stp <1-8>] [forward-time <4-30>] [hello-time <1-10>] [max-age <6-40>] [priority {0*0000 | 0*1000 | 0*2000 | 0*3000 | ... | 0*E000 | 0*F000}] [tagged-bpdu {enable | disable}] [tagged-bpdu-vid <1-4094>] [multicast-address <H.H.H>] [add-vlan] [remove-vlan]
```

The `spanning-tree` command is executed in the Global Configuration command mode.

The following table outlines the parameters for this command.

spanning-tree parameters

Parameters	Description
stp <1-8>	Specifies the Spanning Tree Group; enter the STG ID.
forward-time <4-30>	Enter the forward time of the STG in seconds; the range is 4 -- 30, and the default value is 15.
hello-time <1-10>	Enter the hello time of the STG in seconds; the range is 1 --10, and the default value is 2.
max-age <6-40>	Enter the max-age of the STG in seconds; the range is 6 -- 40, and the default value is 20.
priority {0x000 0x1000 0x2000 0x3000 0xE000 0xF000}	Sets the spanning tree priority (in Hex); if 802.1T compliant, this value must be a multiple of 0x1000.
tagged-bpdu {enable disable}	Sets the BPDU as tagged or untagged. The default value for Spanning Tree Group 1 (default group) is untagged; the default for the other groups is tagged.
tagged-bpdu-vid <1-4094>	Sets the VLAN ID (VID) for the tagged BPDU. The default value is 4001 -- 4008 for STG 1 -- 8, respectively.
multicast-address <H.H.H>	Sets the spanning tree multicast address.
add-vlan	Adds a VLAN to the Spanning Tree Group.
remove-vlan	Removes a VLAN from the Spanning Tree Group.

default spanning-tree command

The `default spanning-tree` command restores the default spanning tree values for the Spanning Tree Group.

The syntax for the `default spanning-tree` command is:

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

The `default spanning-tree` command is executed in the Global Configuration command mode.

The following table outlines the parameters for this command.

default spanning-tree parameters

Parameter	Description
stp <1-8>	Disables the Spanning Tree Group; enter the STG ID.
forward-time	Sets the forward time to the default value of 15 seconds.
hello-time	Sets the hello time to the default value of 2 seconds.
max-age	Sets the maximum age time to the default value of 20 seconds.
priority	Sets spanning tree priority (in Hex); if 802.1T compliant, this value must be a multiple of 0x1000.
tagged-bpdu	Sets the tagging to the default value. The default value for Spanning Tree Group 1 (default group) is untagged; the default for the other groups is tagged.
multicast address	Sets the spanning tree multicast MAC address to the default.

spanning-tree add-vlan command

The `spanning-tree add-vlan` command adds a VLAN to a specified Spanning Tree Group.

The syntax for the `spanning-tree add-vlan` command is:

```
spanning-tree [stp <1-8>] add-vlan <1-4094>
```

Substitute <1-8> with the number of the Spanning Tree Group and <1-4094> with the number of the VLAN to add. VLAN 1 is always part of STG 1.

The `spanning-tree add-vlan` command is executed in the Global Configuration command mode.

spanning-tree remove-vlan command

The `spanning-tree remove-vlan` command removes a VLAN from a specified Spanning Tree Group.

The syntax for the `spanning-tree remove-vlan` command is:

```
spanning-tree [stp <1-8>] remove-vlan <1-4094>
```

Substitute <1-8> with the number of the Spanning Tree Group and <1-4094> with the number of the VLAN to remove. VLAN 1 is always part of STG 1.

The `spanning-tree remove-vlan` command by port is executed in the Global Configuration command mode.

spanning-tree command by port

The `spanning-tree` (by port) command sets the Spanning Tree Protocol (STP) and multiple Spanning Tree Group (STG) participation for the ports within the specified Spanning Tree Group.

The syntax for the `spanning-tree` command by port is:

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

The `spanning-tree` command by port is executed in the Interface Configuration command mode.

The following table outlines the parameters for this command.

spanning-tree parameters

Parameter	Description
port <portlist>	Enables the spanning tree for the specified port or ports; enter port or ports you want enabled for the spanning tree. Note: If you omit this parameter, the system uses the port number you specified when you issued the interface command to enter the Interface Configuration mode.
stp <1-8>	Specifies the spanning tree group; enter the STG ID.
learning {disable normal fast}	Specifies the STP learning mode: <ul style="list-style-type: none"> • disable -- disables FastLearn mode • normal -- changes to normal learning mode • fast -- enables FastLearn mode

Parameter	Description
cost <1-65535>	Enter the path cost of the spanning tree; range is 1 -- 65535.
priority	Sets the spanning tree priority for a port as a hexadecimal value. If the Spanning Tree Group is 802.1T compliant, this value must be a multiple of 0x10.

default spanning-tree command by port

The `default spanning-tree` (by port) command sets the spanning tree values for the ports within the specified Spanning Tree Group to the factory default settings.

The syntax for the `default spanning-tree` command by port is:

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

The `default spanning-tree` command by port is executed in the Interface Configuration command mode.

The following table outlines the parameters for this command.

default spanning-tree parameters

Parameter	Description
port <portlist>	Enables spanning tree for the specified port or ports; enter port or ports to be set to factory spanning tree default values. Note: If this parameter is omitted, the system uses the port number specified when the interface command was used to enter Interface Configuration mode.
stp <1-8>	Specifies the Spanning Tree Group to set to factory default values; enter the STG ID. This command places the port into the default STG. The default value for STG is 1.
learning	Sets the spanning tree learning mode to the factory default value. The default value for learning is Normal mode.

Parameter	Description
cost	Sets the path cost to the factory default value. The default value for path cost depends on the type of port.
priority	Sets the priority to the factory default value. The default value for the priority is 0x8000.

no spanning-tree command by port

The `no spanning-tree` (by port) command disables spanning tree for a port in a specific Spanning Tree Group.

The syntax for the `no spanning-tree` command by port is:

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

The `no spanning-tree` command by port is executed in the Interface Configuration command mode.

The following table outlines the parameters for this command.

no spanning-tree parameters

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

Managing RSTP using the CLI

Use the following command to configure RSTP:

- "spanning-tree rstp command" (page 219)
- "spanning-tree rstp port command" (page 219)
- "show spanning-tree rstp command" (page 220)
- "show spanning-tree rstp port command" (page 221)

spanning-tree rstp command

The `spanning-tree rstp` command sets the RSTP parameters which include forward delay, hello time, maximum age time, default path cost version, bridge priority, transmit holdcount, and version for the bridge. The syntax for the `spanning-tree rstp` command is:

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

The `spanning-tree rstp` command is in the CLI Global configuration mode.

The following table describes the parameters and variables for the `spanning-tree rstp` command.

spanning-tree rstp command parameters

Parameters and variables	Description
forward-time <4- 30>	Sets the RSTP forward delay for the bridge in seconds; the default is 15.
hello-time <1- 10>	Sets the RSTP hello time delay for the bridge in seconds; the default is 2.
max-age <6 - 40>	Sets the RSTP maximum age time for the bridge in seconds; the default is 20.
pathcost-type {bits16 bits32}	Sets the RSTP default path cost version; the default is bits32.
priority {0000 1000 ... F000}	Sets the RSTP bridge priority (in hex); the default is 8000.
tx-hold count	Sets the RSTP Transmit Hold Count; the default is 3.
version {stp-compatible rstp}	Sets the RSTP version; the default is rstp.

spanning-tree rstp port command

The `spanning-tree rstp port` command sets the RSTP parameters, which include path cost, edge-port indicator, learning mode, point-to-point indicator, priority, and protocol migration indicator on the single or multiple port.

The syntax for the `spanning-tree rstp port` command is:

```
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}]
```

The `spanning-tree rstp port` command is in the CLI Interface configuration mode.

The following table describes the parameters and variables for the `spanning-tree rstp port` command.

spanning-tree rstp port command parameters

Parameters and variables	Description
port <portlist>	Filter on list of ports.
cost <1 - 200000000>	Sets the RSTP path cost on the single or multiple ports; the default is 200000.
edge-port {false true}	Indicates whether the single or multiple ports are assumed to be edge ports. This parameter sets the Admin value of edge port status; the default is false.
learning {disable enable}	Enables or disables RSTP on the single or multiple ports; the default is enable.
p2p {auto force-false force-true}	Indicates whether the single or multiple ports are to be treated as point-to-point links. This command sets the Admin value of P2P Status; the default is force-true.
priority {00 10 ... F0}	Sets the RSTP port priority on the single or multiple ports; the default is 80.
protocol-migration {false true}	Forces the single or multiple port to transmit RSTP BPDUs when set to true, while operating in RSTP mode; the default is false.

show spanning-tree rstp command

The `show spanning-tree rstp` command displays the Rapid Spanning Tree Protocol (RSTP) related bridge-level configuration details. The syntax for the `show spanning-tree rstp` command is:

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

The `show spanning-tree rstp` command is in the `privExec` command mode.

show spanning-tree rstp command

Parameters and variables	Description
config	Displays RSTP bridge-level configuration.
status	Displays RSTP bridge-level role information.
statistics	Displays RSTP bridge-level statistics.

show spanning-tree rstp port command

The `show spanning-tree rstp port` command displays the Rapid Spanning Tree Protocol (RSTP) related port-level configuration details. The syntax for the `show spanning-tree rstp port` command is:

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

The `show spanning-tree rstp port config` command is in the `privExec` command mode.

show spanning-tree rstp port command

Parameters and variables	Description
config	Displays RSTP port-level configuration.
status	Displays RSTP port-level role information.
statistics	Displays RSTP port-level statistics.
role	Displays RSTP port-level status.

Managing MSTP using the CLI

- ["spanning-tree mstp command" \(page 222\)](#)
- ["spanning-tree mstp port command" \(page 223\)](#)
- ["spanning-tree mstp region command" \(page 224\)](#)
- ["spanning-tree mstp msti command" \(page 224\)](#)
- ["no spanning-tree mstp msti enable command" \(page 225\)](#)
- ["no spanning-tree mstp msti command" \(page 225\)](#)
- ["show spanning-tree mstp command" \(page 225\)](#)
- ["show spanning-tree mstp port command" \(page 226\)](#)
- ["show spanning-tree mstp msti command" \(page 226\)](#)

spanning-tree mstp command

The `spanning-tree mstp` command sets the MSTP parameters, which include maximum hop count, maximum number of instances allowed, forward delay time, hello time, maximum age time, default path cost version, priority, transmit hold count, and version for the Cist Bridge. The syntax for the `spanning-tree mstp` command is:

```
spanning-tree mstp [max-hop <600 - 4000>]
[forward-time <4 - 30>]
[max-age <6 - 40>]
[pathcost-type {bits16 | bits32}]
[priority {0000 | 1000 | 2000 | ... | F000}]
[tx-hold count <1 - 10>]
[version {stp-compatible | rstp | mstp}]
[add-vlan <1 - 4094>] [remove-vlan <1 - 4094>]
```

The `spanning-tree mstp` command is in the Global configuration mode.

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

spanning-tree mstp command parameters

Parameters and variables	Description
max-hop <600 - 4000>	Sets the MSTP maximum hop count for the CIST bridge; the default is 2000.
forward-time <4 - 30>	Sets the MSTP forward delay for the CIST bridge in seconds; the default is 15.
max-age <6 - 40>	Sets the MSTP maximum age time for the CIST bridge in seconds; the default is 20.
pathcost-type {bits16 bits32}	Sets the MSTP default path cost version; the default is bits32.
priority {0000 1000 2000 ... F000}	Sets the MSTP bridge priority for the CIST Bridge; the default is 8000.
tx-holdcount<1 - 10>	Sets the MSTP Transmit Hold Count; the default is 3.
version {stp-compatible rstp mstp}	Sets the MSTP version for the Cist Bridge; the default is mstp.
add-vlan <1 - 4094>	Adds a VLAN to the CIST bridge.
remove-vlan <1 - 4094>	Removes the specified VLAN from the CIST bridge.

spanning-tree mstp port command

The `spanning-tree mstp port` command sets the MSTP parameters, which include path cost, hello time, edge-port indicator, learning mode, point-to-point indicator, priority, and protocol migration indicator on the single or multiple ports for the Common Spanning Tree.

The syntax for the `spanning-tree mstp port` command is:

```
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}]
```

The `spanning-tree mstp port` command is in the Interface configuration mode.

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

spanning-tree mstp port command parameters

Parameters and variables	Description
port <portlist>	Enter a list or range of port numbers.
cost <1 - 200000000>	Sets the MSTP path cost on the single or multiple ports for the CIST; the default is 200000.
hello-time <1 - 10>	Sets the MSTP hello time on the single or multiple ports for the CIST; the default is 2.
edge-port {false true}	Indicates whether the single or multiple ports are assumed to be edge ports. This parameter sets the Admin value of edge port status; the default is false.
learning {disable enable}	Enables or disables MSTP on the single or multiple ports; the default is enable.
p2p {auto force-false force-true}	Indicates whether the single or multiple ports are treated as point-to-point links. This command sets the Admin value of P2P Status; the default is force-true.
priority {00 10 ... F0}	Sets the MSTP port priority on the single or multiple ports; the default is 80.
protocol-migration {false true}	Forces the single or multiple ports to transmit MSTP BPDUs when set to true, while operating in MSTP mode; the default is false.

spanning-tree mstp region command

The `spanning-tree mstp region` command sets the MSTP parameters, which include config ID selector, region name, and region version. The syntax for the `spanning-tree mstp region` command is:

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

The `spanning-tree mstp region` command is in the Global configuration mode.

spanning-tree mstp region command parameters

Parameters and variables	Description
[config-id-sel <0 - 255>]	Sets the MSTP config ID selector; the default is 0.
[region-name <1 - 32 chars>]	Sets the MSTP region name; the default is the bridge MAC address.
[region-version <0 - 65535>]	Sets the MSTP region version; the default is 0.

spanning-tree mstp msti command

The `spanning-tree mstp msti` command sets the MSTP parameters, which include forward delay time, hello-time, maximum hop count, priority, and VLAN mapping for the bridge instance. The syntax for the `spanning-tree mstp msti` command is:

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

The `spanning-tree mstp msti` command is in the Global configuration mode.

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

spanning-tree mstp msti command parameters

Parameters and variables	Description
<1 - 7>	Filter on MSTP instance.
priority {0000 1000 ... F000}	Sets the MSTP priority for the bridge instance; the default is 8000.

Parameters and variables	Description
<code>add-vlan <1 - 4094></code>	Maps the specified Vlan and MSTP bridge instance.
<code>remove-vlan <1 - 4094></code>	Unmaps the specified Vlan and MSTP bridge instance.
<code>enable</code>	Enables the MSTP bridge instances.

no spanning-tree mstp msti enable command

This command disables an MSTP bridge-instance.

This command can be executed in the config command mode, and the syntax is:

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

no spanning-tree mstp msti command

This command deletes an MSTP bridge-instance.

This command can be executed in the config command mode, and the syntax is:

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

show spanning-tree mstp command

The `show spanning-tree mstp` command displays Multi Spanning Tree Protocol (MSTP) related status information known by the selected bridge. The syntax for the `show spanning-tree mstp` command is:

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

The `show spanning-tree mstp` command is in the privExec command mode.

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

show spanning-tree mstp command parameters

Parameters and variables	Description
<code>config</code>	Displays the MSTP-related bridge-level VLAN and region information.
<code>status</code>	Displays the MSTP-related bridge-level status information known by the selected bridge.
<code>statistics</code>	Displays the MSTP-related bridge-level statistics.

show spanning-tree mstp port command

The `show spanning-tree mstp port` command displays the Multi Spanning Tree Protocol (MSTP) Cist Port information maintained by every port of the Common Spanning Tree. The syntax for the `show spanning-tree mstp port` command is:

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

The `show spanning-tree mstp port config` command is in the `privExec` command mode.

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

show spanning-tree mstp port command parameters

Parameters and variables	Description
<portlist>	Enter a list or range of port numbers.
config	Displays the MSTP CIST port information maintained by every port of the Common Spanning Tree.
role	Displays MSTP CIST related port role information maintained by every port.
statistics	Displays the MSTP CIST Port statistics maintained by every port.

show spanning-tree mstp msti command

The `show spanning-tree mstp msti` command displays the MSTP MSTI settings. The syntax for the `show spanning-tree mstp msti` command is:

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

The `show spanning-tree mstp msti` command is in the CLI Global configuration mode.

show spanning-tree mstp msti command parameters

Parameters and variables	Description
config	Displays the MSTP instance-specific configuration and the VLAN mapping port.
statistics	Displays MSTP instance-specific statistics.

Parameters and variables	Description
port {config role statistics}	Displays MSTP instance-specific port information: <ul style="list-style-type: none"> config: displays MSTI port configuration role: displays MSTI port role information statistics: displays MSTI port statistics
<1 - 7>	Specifies the MSTI instance for which to display the statistics.

Setting the STP mode using the Web-based Management Interface

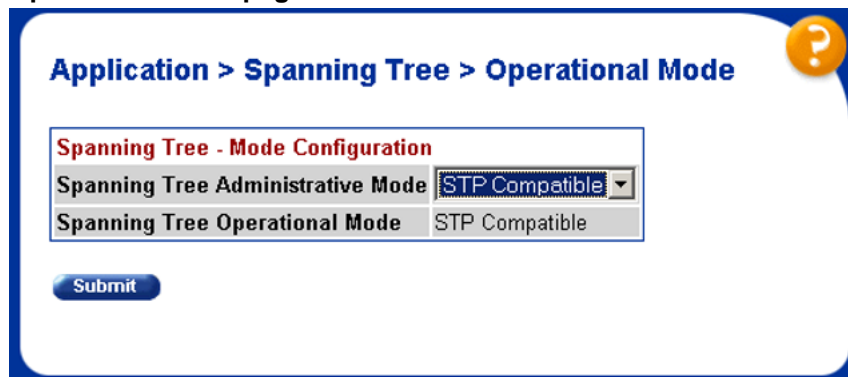
To set the STP operational mode using the Web-based Management Interface:

Step	Action
------	--------

- From the menu, select **Applications > Spanning Tree > Operational Mode**.

The Operational Mode page appears.

Operational Mode page



- Select the **Spanning Tree Administrative Mode** from the list.

The available options are:

- STP Compatible
- RSTP
- MSTP

- Click **Submit**.

A warning appears reminding you that a switch reset is required for the change to take effect.

- 4 Click **OK**.
- 5 To reset the switch, choose **Administration > Reset**.

—End—

Creating and Managing STGs using the Web-based Management Interface

The Web-based Management Interface screens detailed in this section allow for the creation and management of Spanning Tree Groups.

To configure STGs using the Web-based Management Interface, refer to the following:

- ["Creating a Spanning Tree Group" \(page 228\)](#)
- ["Modifying a Spanning Tree Group" \(page 230\)](#)
- ["Deleting a Spanning Tree Group" \(page 231\)](#)
- ["Associating an STG with VLAN Membership" \(page 231\)](#)
- ["Spanning Tree Port Configuration" \(page 233\)](#)
- ["Modifying STG Bridge Information" \(page 235\)](#)

Creating a Spanning Tree Group

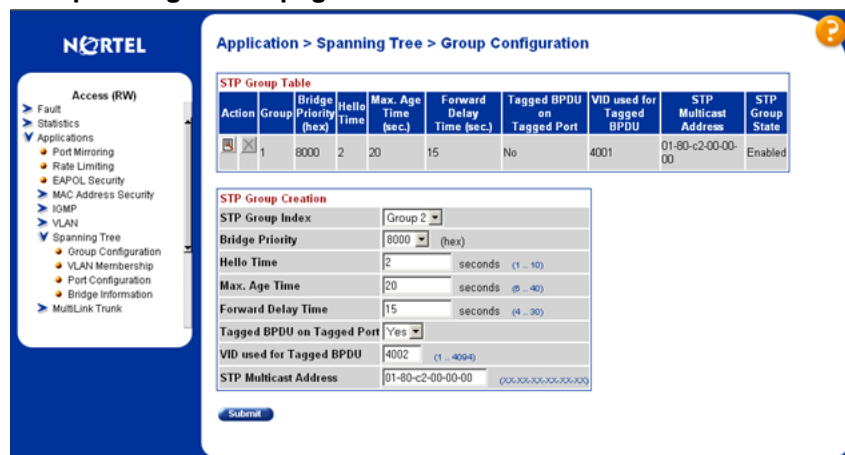
To create a Spanning Tree Group, follow this procedure:

Step	Action
------	--------

- | | |
|---|---|
| 1 | From the menu, select Applications > Spanning Tree > Group Configuration . |
|---|---|

The Group Configuration page appears ("[Group Configuration page](#)" [\(page 229\)](#)).

Group Configuration page



- 2 In the **STG Group Creation** section, enter the information to create the new Spanning Tree Group. "STG Group Creation fields" (page 229) outlines the fields in this section.





STG Group Creation fields

Field	Description
STP Group Index	Choose the group number to be created.
Bridge Priority	Select the desired priority from the list.
Hello Time	Enter the desired hello time for this STG in seconds; the range is 1 to 10.
Max. Age time	Enter the desired maximum age time for this STG in seconds; the range is 6 to 40.
Forward Delay Time	Enter the desired forward delay time for this STG in seconds; the range is 4 to 30.
Tagged BPDU on Tagged Port	Set the frames as tagged (Yes) or untagged (No) on tagged ports.
VID used for Tagged BPDU	Enter the VLAN ID for tagged BPDUs for the specified STG. Note: The default VIDs are 4001 through 4008 for STGs 1 through 8, respectively.
STP Multicast Address	Enter the STP multicast MAC address.

- 3 Click **Submit**.

The new Spanning Tree Group is created and displayed in the STG Group Table section ("STG Group Table section" (page 230)) of the Group Configuration page.

STG Group Table section

STP Group Table									
Action	Group	Bridge Priority (hex)	Hello Time	Max. Age Time (sec.)	Forward Delay Time (sec.)	Tagged BPDU on Tagged Port	VID used for Tagged BPDU	STP Multicast Address	STP Group State
	 1	8001	2	20	15	Nc	4001	01-80-c2-00-00-00	Enabled
	 2	8002	2	20	15	Nc	4002	01-80-c2-00-00-00	Disabled

Modify (points to the Modify icon in the first row)

Delete (points to the Delete icon in the second row)

The new Spanning Tree Group is disabled until you modify it by clicking the Modify button on the STG Group Table section.

—End—

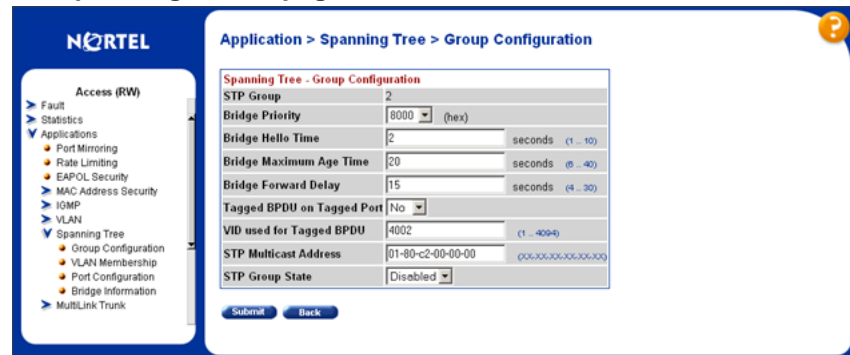
Modifying a Spanning Tree Group

To modify an existing Spanning Tree Group, follow this procedure:

Step	Action
------	--------

- From the menu, select **Applications > Spanning Tree > Group Configuration**.
The Group Configuration page appears.
- In the **STG Group Table** section ("[STG Group Table section](#)" (page 230)), click the **Modify** button for the STG to be modified.
The Group Configuration page ("[Group Configuration page](#)" (page 231)) appears and allows the Spanning Tree Group information to be edited.
- Use the **STG Group State** field to enable or disable the selected Spanning Tree Group.
- Make any additional changes to the Spanning Tree Group using the fields provided.

Group Configuration page



- 5 Click **Submit**.

—End—

Deleting a Spanning Tree Group

To delete a Spanning Tree Group, follow this procedure:

Step	Action
------	--------

- | | |
|---|---|
| 1 | From the menu, select Applications > Spanning Tree > Group Configuration .

The Group Configuration page appears. |
| 2 | In the STG Group Table section, click the Delete button (" STG Group Table section " (page 230)) for the STG to be deleted. (STG 1 can never be deleted.)

A message appears asking for confirmation of the deletion. |
| 3 | Click Yes . |

—End—

Associating an STG with VLAN Membership

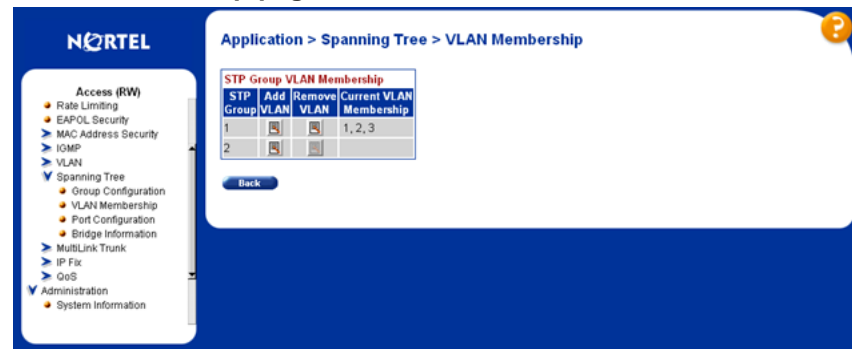
To modify the association of a VLAN with an STG, follow this procedure:

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the menu, select Applications > Spanning Tree > VLAN Membership .

The VLAN Membership page appears (" VLAN Membership page " (page 232)). |
|---|--|

VLAN Membership page



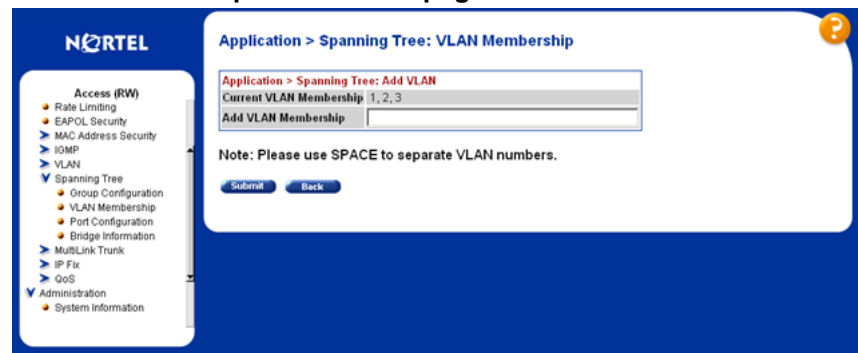
2 Refer to the following to add or delete a VLAN.

a. To add a VLAN to an STG:

- Click the **Modify** button that appears in the **Add VLAN** column of the STG to be modified.

The VLAN Membership modification page appears ("VLAN Membership modification page" (page 232)).

VLAN Membership modification page



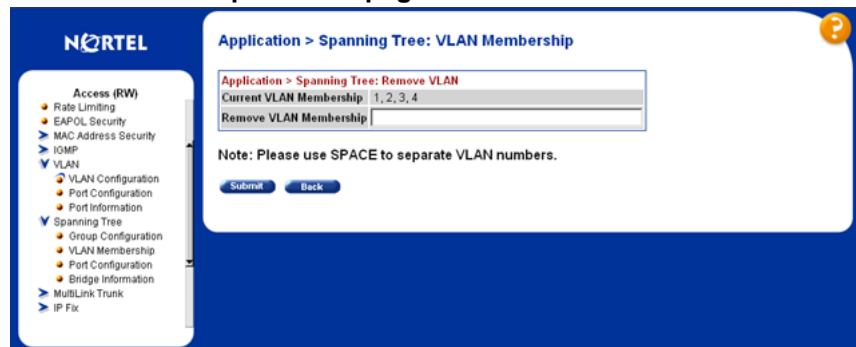
- In the **Add VLAN Membership** field, type the numbers of the VLANs to be added, separated by spaces.
- Click **Submit**.

b. To remove a VLAN from an STG:

- Click the **Modify** button that appears in the **Remove VLAN** column of the STG to be modified.

The VLAN Membership deletion page appears ("VLAN Membership deletion page" (page 233)).

VLAN Membership deletion page



- In the **Remove VLAN Membership** field, type the numbers of the VLANs to be removed, separated by spaces.
- Click **Submit**.

—End—

Spanning Tree Port Configuration

To configure ports for participation in a Spanning Tree Group, follow this procedure:

Step	Action
------	--------

- | | |
|---|---|
| 1 | <p>From the menu, select Applications > Spanning Tree > Port Configuration .</p> <p>The Port Configuration page appears ("Port Configuration page" (page 234)).</p> |
|---|---|

Port Configuration page

Application > Spanning Tree > Port Configuration

STP Group
Group: Group 1

Submit

Spanning Tree - Port Setting

Port	Trunk	Tagging	Participation	Priority (hex)	Path Cost	State
1		Untag All	Disabled	80	1	Disabled
2		Untag All	Disabled	80	1	Disabled
3		Untag All	Disabled	80	1	Disabled
4		Untag All	Disabled	80	1	Disabled
5		Untag All	Disabled	80	1	Disabled
6		Untag All	Disabled	80	1	Disabled
7		Untag All	Disabled	80	1	Disabled
8		Untag All	Disabled	80	1	Disabled
9		Untag All	Disabled	80	1	Disabled
10		Untag All	Disabled	80	1	Disabled
11		Untag All	Disabled	80	1	Disabled
12		Untag All	Disabled	80	1	Disabled
Switch			Normal Learning	80		

Submit

- 2 From the **STG Group** section **Group** list, select the STG to configure.
- 3 Immediately under the **STG Group** section, click **Submit**.
- 4 With the desired STG selected, use the fields in the **Spanning Tree -- Port Setting** section to denote which ports will participate in the STG.

The fields for this section are outlined in "[Spanning Tree -- Port Setting fields](#)" (page 234).

Spanning Tree -- Port Setting fields

Field	Description
Participation	<p>This list is used to select the STG participation for the port. The options are:</p> <ul style="list-style-type: none"> • Normal Learning • Fast Learning • Disabled <p>Note: When an individual port is a trunk member, changing this setting for one of the trunk members changes the setting for all members of that trunk. Consider the effect that changing this value will have on the network topology before making changes.</p> <p>The default setting is Normal Learning.</p>

Field	Description
Priority	The bridge spanning tree parameter that prioritizes the lowest port path cost to the root. When one or more ports have the same path cost, STP selects the path with the highest priority (lowest numerical value).
Path Cost	The bridge spanning tree parameter that determines the lowest path cost to the root.

- 5 Immediately under the **Spanning Tree -- Port Setting** section, click **Submit**.

—End—

The Spanning Tree -- Port Setting section does not list all ports on a switch at one time. Click the links that appear at the bottom of the page to view the designated ports.

Modifying STG Bridge Information

To modify the Spanning Tree Group Bridge information, follow this procedure:

Step	Action
------	--------

- | | |
|---|---|
| 1 | <p>From the menu, select Applications > Spanning Tree > Bridge Information .</p> <p>The Bridge Information page appears ("Bridge Information page" (page 236)).</p> |
|---|---|

Bridge Information page

The screenshot shows the 'Spanning Tree - Bridge Information' configuration page. The left sidebar contains a navigation tree with 'Spanning Tree' expanded to 'Bridge Information'. The main content area has a breadcrumb trail 'Application > Spanning Tree > Bridge Information'. Below this is a section for 'STP Group' with a dropdown menu set to 'Group 2' and a 'Submit' button. The main configuration area is titled 'Spanning Tree - Bridge Information' and contains the following fields:

Bridge Priority	8000	(hex)
Designated Root	00-00-00-00-00-00	
Root Port	Port 0	
Root Path Cost	0	
Hello Time	0	seconds
Maximum Age Time	0	seconds
Forward Delay	0	seconds
Bridge Hello Time	2	seconds (1 - 10)
Bridge Maximum Age Time	20	seconds (6 - 40)
Bridge Forward Delay	15	seconds (4 - 30)
Tagged BPDU on Tagged Port	Yes	
VID used for Tagged BPDU	4002	(1 - 4094)
STP Multicast Address	01-80-c2-00-00-00	(00-xx-xx-xx-xx-xx)

- 2 From the **Group** list in the **STG Group** section, select the STG to modify.
- 3 Immediately underneath the STG Group section, click the **Submit** button.
- 4 In the fields provided, edit the information pertaining to the selected STG.

"Spanning Tree -- Bridge Information fields" (page 236) describes the fields that can be edited in the Spanning Tree -- Bridge Information section.

Spanning Tree -- Bridge Information fields

Field	Description
Bridge Priority	Select the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. The Spanning Tree Algorithm uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values compared first, followed by the hardware addresses. The default setting is 8000.

Field	Description
Bridge Hello Time	<p>The Hello Interval (the amount of time between transmissions of BPDUs) specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge.</p> <p>Note: Although you can set the Hello Interval for a bridge using bridge management software, after the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network.</p> <p>The default is 2 seconds.</p>
Bridge Maximum Age Time	<p>The Maximum Age Time parameter value that the root bridge uses. This value specifies the maximum age that a Hello message can attain before being discarded.</p> <p>Note: The root bridge Maximum Age Time parameter value becomes the actual Maximum Age Time parameter value for all bridges participating in the spanning tree network.</p>
Bridge Forward Delay	<p>The Forward Delay parameter value that the root bridge uses. This value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state.</p> <p>Note: The root bridge Forward Delay parameter value becomes the actual Forward Delay parameter value for all bridges participating in the spanning tree network.</p>
Tagged BPDU on Tagged Port	<p>This parameter determines whether tagged or untagged BPDUs are sent from a tagged port.</p>
VID used for Tagged BPDU	<p>This parameter determines the VLAN ID sent with the tagged BPDUs for the specified STG.</p>
STP Multicast Address	<p>The STP multicast address to be used.</p>

5 Click **Submit**.

—End—

Configuring RSTP using Web-based management

The Rapid Spanning Tree protocol (RSTP or IEEE 802.1w) reduces the recovery time after a network breakdown. It also maintains a backward compatibility with the IEEE 802.1d which was the Spanning Tree implementation prior to RSTP. In certain configurations the recovery time of RSTP can be reduced to less than 1 second.

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

To configure RSTP using Web-based management, refer to the following sections:

- ["Configuring RSTP bridge settings" \(page 238\)](#)
- ["Configuring RSTP port settings" \(page 240\)](#)

Configuring RSTP bridge settings

You can view and configure the existing Spanning Tree (RSTP) bridge switch settings.

To configure the Spanning Tree (RSTP) bridge switch settings:

Step	Action
------	--------

1	From the main menu, choose Application > Spanning Tree > Bridge Configuration .
---	--

The Spanning Tree (RSTP) - Bridge Configuration page appears.

Spanning Tree (RSTP) - Bridge Configuration page

Spanning Tree - Bridge Configuration	
STP Priority	8000 (hex)
Designated Root	80-00-00-04-38-d5-9a-b1
Stp Root Cost	200000
Stp Root Port	Port 1
Bridge Max Age	20 seconds (0..40)
Bridge Hello Time	2 seconds (1..10)
Bridge Forward Delay Time	15 seconds (4..30)
Tx Hold Count	3 (1..10)
PathCost Default Type	32-bit

Submit

Spanning Tree (RSTP) - Bridge Configuration page items

Item	Description
STP Priority	The value of the writable portion of the Bridge ID. That is, the first two octets of the (8 octet long) Bridge ID. The other (last) 6 octets of the Bridge ID are given by the value of dot1dBaseBridgeAddress. On bridges supporting IEEE 802.1t or IEEE 802.1w permissible values are 0-61440, in steps of 4096.
Designated Root	The bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol as executed by this node. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
Stp Root Cost	The cost of the path to the root as seen from this bridge.
Stp Root Port	The port number of the port which offers the lowest cost path from this bridge to the root bridge.
Bridge Max Age	The value that all bridges use for MaxAge when this bridge acts as the root. Note: 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.
Bridge Hello Time	The value that all bridges use for HelloTime when this bridge acts as the root. Note: 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.
Bridge Forward Delay Time	The value that all bridges use for ForwardDelay when this bridge acts as the root. Note: 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.
Tx Hold Count	The value used by the Port Transmit state machine to limit the maximum transmission rate.
PathCost Default Type	The version of the Spanning Tree default Path Costs that are used by this Bridge.

—End—

Configuring RSTP port settings

To open the **Spanning Tree (RSTP) - Port Configuration** page:

Step Action

- 1 From the main menu, choose **Application > Spanning Tree > Port Configuration**.

The Spanning Tree (RSTP) - Port Configuration page appears.

Spanning Tree (RSTP) - Port Configuration page

Application > Spanning Tree (RSTP) > Port Configuration

Port	STP Participation	Priority (hex)	Path Cost	Admin Edge Status	Oper Edge Status	Admin P2P Status	Oper P2P Status	Oper Protocol Version	Role	State
1	Enabled	80	200000	False	False	Auto	True	StpCompatible Mode	Root	Forwarding
2	Enabled	80	20000	False	False	Auto	True	Rstp Mode	Disabled	Discarding
3	Enabled	80	20000	False	False	Auto	True	Rstp Mode	Disabled	Discarding
4	Enabled	80	20000	False	False	Auto	True	Rstp Mode	Disabled	Discarding
5	Enabled	80	20000	False	False	Auto	True	Rstp Mode	Disabled	Discarding
6	Enabled	80	200000	False	False	Auto	True	Rstp Mode	Disabled	Discarding
7	Disabled								Disabled	
8	Disabled								Disabled	
9	Enabled	80	1	False	False	Auto	True	Rstp Mode	Disabled	Discarding
10	Enabled	80	20000	False	False	Auto	True	Rstp Mode	Disabled	Discarding
11	Enabled	80	20000	False	False	Auto	True	Rstp Mode	Disabled	Discarding
12	Enabled	80	20000	False	False	Auto	True	Rstp Mode	Disabled	Discarding
Switch	Enabled	80	200000	False		Auto				

Submit

Spanning Tree (RSTP) - Port Configuration page items

Item	Description/Command
Port	The port number of the currently displayed unit.
STP Participation	Enables or disables STP participation on the port. The default setting is Disabled.
Priority (hex)	The bridge spanning tree parameter that prioritizes the lowest port path cost to the root. When one or more ports have the same path cost, STP selects the path with the highest priority (lowest numerical value).
Path Cost	The bridge spanning tree parameter that determines the lowest path cost to the root.

Item	Description/Command
Admin Edge Status	<p>The administrative value of the Edge Port parameter. A value of True indicates that this port is assumed to be an edge-port, and a value of False indicates that this port is assumed to be a nonedge-port.</p> <p>An Edge Port goes directly to Forwarding state without delay. Edge ports do not receive any Topology Change notifications and cannot influence the Spanning Tree Algorithm in detecting network loops. This is a particular port setting, not a learning mode.</p>
Oper Edge Status	Can be True or False. This is set to False when AdminEdge is set to True and the port receives BPDUs (any kind) or when AdminEdge is set to False.
Admin P2P Status	The administrative point-to-point status of the LAN segment attached to this port. A value of 0 indicates that this port is always treated as being connected to a point-to-point link. A value of 1 indicates that this port is treated as having a shared media connection. A value of 2 indicates that this port is considered to have a point-to-point link if it is an Aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation, or by management means.
Oper P2P Status	This field indicates the operational point-to-point status of the LAN segment attached to the port. It also indicates whether a port is considered to have a point-to-point connection. The value is determined by management or by auto-detection, as described in the AdminP2P object.
Oper Protocol Version	Displays the operational mode of the port.
Role	The current role of the port as defined by Rapid Spanning Tree Protocol. The role of a port can be Root, Designated, Alternate, or Backup.
State	The current state of the port as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame. If the bridge detects a port that is malfunctioning, the port is placed into the disabled state.

—End—

Configuring MSTP using Web-based management

To configure MSTP using Web-based management, refer to the following sections:

- ["Creating MSTI instances" \(page 242\)](#)
- ["Configuring MSTI bridge settings" \(page 243\)](#)
- ["Adding VLANs to the MSTI" \(page 246\)](#)
- ["Configuring Cist ports" \(page 248\)](#)

- "Configuring MSTI port properties" (page 250)

Creating MSTI instances

To create MSTI instances:

Step	Action
------	--------

- | | |
|---|---|
| 1 | From the main menu, choose Applications > Spanning Tree > Bridge Configuration . |
|---|---|

The MSTP Bridge Configuration page appears.

MSTP Bridge Configuration page



- | | |
|---|--|
| 2 | To create an MSTI, choose an MSTI from the Spanning Tree - Msti Bridge Creation list, and click Submit . |
|---|--|

The new MSTI instance appears in the Spanning Tree - Msti Bridge Configuration section.

The following table describes the items on the Msti Bridge Configuration page.

Msti Bridge Configuration page items

Section	Item	Description
Spanning Tree - CIST Bridge Configuration		Displays a configuration page for the CIST.
	Bridge Regional Root	Port and the MAC address of the root switch.
	Bridge Priority	The priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID.

Section	Item	Description
	Root Cost	The cost of the path to the root as seen from this bridge.
	Root Port	The port number of the port which offers the lowest path cost from this bridge to the root bridge.
Spanning Tree - Msti Bridge Configuration		Displays a configuration page for the MSTI.
		Deletes the MSTI.
	Msti	Displays the index of MSTP.
	Bridge Regional Root	Displays the unique Bridge Identifier of the bridge.
	Bridge Priority	Type the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID.
	Root Cost	The cost of the path to the root as seen from this bridge.
	Root Port	The port number of the port which offers the lowest path cost from this bridge to the root bridge.
	State	Specifies whether the bridge instance is enabled or disabled.
Spanning Tree - Msti Bridge Creation	Msti	Displays the index of MSTP. To add an MSTI, choose an MSTI identifier from the list and click submit.

—End—

Configuring MSTI bridge settings

To configure the MSTI bridge settings on the switch:

Step	Action
------	--------

- | | |
|---|---|
| 1 | From the MSTP Bridge Configuration page, under Spanning Tree - Msti Bridge Configuration , choose the Msti Bridge Configuration Action icon. |
|---|---|

The Msti Bridge Configuration page appears.

Msti Bridge Configuration page

Application > Spanning Tree (MSTP) > Msti Bridge Configuration ?

Spanning Tree - Msti Bridge Configuration	
Msti	1
State	Disabled <input type="button" value="v"/>
Bridge Priority	8000 <input type="button" value="v"/> (hex)
Bridge Regional Root	80-00-00-11-19-35-d0-01
Root Cost	0
Root Port	None

Msti Bridge Configuration page items

Item	Description
Msti	The Multiple Spanning Tree instance.
State	Used to control whether the bridge instance is enabled or disabled.
Bridge Priority	The writable portion of the MSTI bridge identifier comprising the first two octets.
Bridge Regional Root	Indicates the MSTI regional root identifier value for the MSTI. All configuration bridge PDUs originated by this node use this value as the MSTI Regional Root Identifier parameter.
Root Cost	The cost of the path to the MSTI regional root as seen by this bridge.
Root Port	The port number of the port that offers the lowest path cost from this bridge to the MSTI region root bridge.

—End—

Configuring CIST bridge settings

To configure CIST settings on the switch:

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the MSTP Bridge Configuration page, under Spanning Tree - Msti Bridge Configuration , choose the CIST Bridge Configuration icon. |
|---|--|

The CIST Bridge Configuration page appears.

CIST Bridge Configuration page

Application > Spanning Tree (MSTP) > Cist Bridge Configuration

Spanning Tree - Cist Bridge Configuration	
Bridge Priority	8000 <input type="button" value="v"/> (hex)
Bridge Max Age	20 seconds (6..40)
Bridge Forward Delay Time	15 seconds (4..30)
Tx Hold Count	3 (1..10)
PathCost Default Type	32-bit <input type="button" value="v"/>
Max Hop Count	2000 (500..4000, increments of 100)
Max Mst Instance Number	8
Number of Msti Supported	2

Spanning Tree - Region Configuration	
Config Id Selector	0 (1..255)
Region Name	00:11:f9:35:d0:00
Region Version	0 (1..65535)
Config Digest	ac-36-17-7f-50-28-3c-d4-b8-38-21-d8-ab-26-de-62

Cist Bridge Configuration page items

Section	Item	Description
Spanning Tree - CIST Bridge Configuration	Bridge Priority	The value of the writable portion of the bridge identifier comprising the first two octets.
	Bridge Max Age	The value in seconds that all bridges use for MaxAge when this bridge acts as the root. The range is 6 to 40.
	Bridge Forward Delay Time	The value in seconds that all bridges use for ForwardDelay when this bridge acts as the root. IEEE 802.1D specifies that the range for this parameter is related to the value of Bridge Max Age. The range is 4 to 30.
	Tx Hold Count	The value used by the Port Transmit state machine to limit the maximum transmission rate.
	PathCost Default Type	The version of the spanning tree default path costs that this bridge uses. 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.

Section	Item	Description
	Max Hop Count	The maximum hop count value in 1/100 seconds. The value must be a multiple of 100. The range is 600 to 4000.
	Root Port	The highest possible value for the MSTI ID in this mode.
	Number of Msti Supported	The number of MSTI supported in this mode.
Spanning Tree - Region Configuration	Config Id Selector	The MSTP config ID selector. The default value is 0.
	Region Name	The MSTP region name. The default value is the bridge MAC address.
	Region Version	The MSTP region version. The default value is 0.
	Config Digest	The configuration digest value for this region.

—End—

Adding VLANs to the MSTI

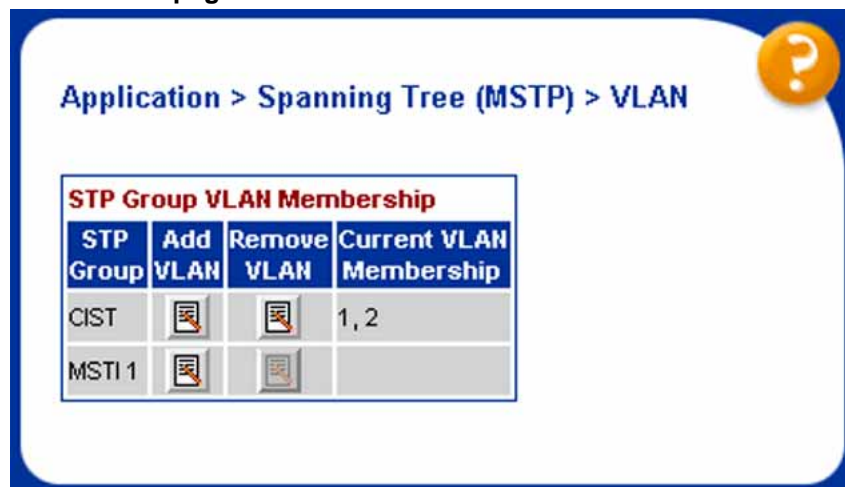
To add a VLAN to an MSTI:

Step Action

- 1 From the main menu, choose **Application > Spanning Tree > Bridge VLAN**.

The MSTP VLAN page appears.

MSTP VLAN page



The table displays the current VLAN membership for the MSTIs.

- 2 To add a VLAN:
 - a. Click the modification icon in the **Add VLAN** column for the CIST or MSTI.

The MSTP VLAN Membership (Add) page appears.

MSTP VLAN Membership (Add) page

Application > Spanning Tree (MSTP) > VLAN > VLAN Membership

VLAN Membership	
Current VLAN Membership	1
Add VLAN Membership	<input type="text"/>

Note: Use SPACE to separate VLAN Ids.

Submit Back

- b. Enter the ID numbers of the VLANs you want to add to the MSTI.
 - c. Click **Submit**.

The VLAN is added to the current VLAN Membership column in the appropriate MSTI row.

- 3 To remove a VLAN:
 - a. Click the modification icon in the **Remove VLAN** column.

The VLAN Membership (Remove) page appears.

MSTP VLAN Membership (Remove) page

Application > Spanning Tree (MSTP) > VLAN > VLAN Membership

VLAN Membership	
Current VLAN Membership	1
Remove VLAN Membership	<input type="text"/>

Note: Use SPACE to separate VLAN Ids.

- b. Enter the number of the VLANs you want to remove from the MSTI.
- c. Click **Submit**.

The VLAN is removed from the Current VLAN Membership column in the appropriate CIST or MSTI row.

—End—

Configuring Cist ports

To configure CIST ports:

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the main menu, choose Application > Spanning Tree (MSTP) > Cist Port Configuration . |
|---|--|

The Cist Port Configuration page appears.

Cist Port Configuration page

Application > Spanning Tree (MSTP) > Cist Port Configuration

Spanning Tree - Cist Port Setting

Port	STP Participation	Priority (hex)	Path Cost	Admin Edge Status	Oper Edge Status	Admin P2P Status	Oper P2P Status	Hello Time (seconds)	Role	State
1	Enabled	80	200000	False	False	Auto	True	2	Root	Forwarding
2	Enabled	80	20000	False	False	Auto	True	2	Disabled	Discarding
3	Enabled	80	20000	False	False	Auto	True	2	Disabled	Discarding
4	Enabled	80	20000	False	False	Auto	True	2	Disabled	Discarding
5	Enabled	80	20000	False	False	Auto	True	2	Disabled	Discarding
6	Enabled	80	200000	False	False	Auto	True	2	Disabled	Discarding
7	Disabled									Disabled
8	Disabled									Disabled
9	Enabled	80	1	False	False	Auto	True	2	Disabled	Discarding
10	Enabled	80	20000	False	False	Auto	True	2	Disabled	Discarding
11	Enabled	80	20000	False	False	Auto	True	2	Disabled	Discarding
12	Enabled	80	20000	False	False	Auto	True	2	Disabled	Discarding
Switch	Enabled	80	200000	False		Auto		2		

Submit

[Ports 13 - 24](#) [Ports 25 - 26](#)

Cist Port Configuration page items

Section	Description
Port	Indicates the name of the port.
STP Participation	Provides information about current participation for a port in CIST (in this case). In new implementation this can be only Enabled or Disabled. Enabled means Normal Learning, like in STP802.1d mode. Disabled means that port doesn't transmit any BPDUs and is not under the influence of Spanning Tree Algorithm (STA).
Priority	Indicates the four most significant bits of the Port Identifier for a given Spanning Tree instance. The value 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.
Path Cost	The cost of the path to the root as seen from this bridge.
Admin Edge Status	The administrative value of the Edge Port parameter. A value of True indicates that this port is assumed to be an edge-port and a value of False indicates that this port is assumed to be a nonedge-port. An Edge Port goes directly to Forwarding state without delay. Edge ports do not receive any Topology Change notifications and cannot influence the Spanning Tree Algorithm in detecting network loops. This is a particular port setting, not a learning mode.
Oper Edge Status	Can be True or False. This is set to False when AdminEdge is set to True and the port receives BPDUs (any kind) or when AdminEdge is set to False.

Section	Description
Admin P2P Status	The administrative point-to-point status of the LAN segment attached to this port. A value of 0 indicates that this port is always treated as being connected to a point-to-point link. A value of 1 indicates that this port is treated as having a shared media connection. A value of 2 indicates that this port is considered to have a point-to-point link if it is an Aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation, or by management means.
Oper P2P Status	This field indicates the operational point-to-point status of the LAN segment attached to the port. It also indicates whether a port is considered to have a point-to-point connection. The value is determined by management or by auto-detection, as described in the AdminP2P object.
Hello Time	Sets the hello time on the single or multiple port.
Role	The current role of the port as defined by the Multiple Spanning Tree Protocol. The role of a port can be Root, Designated, Alternate, or Backup.
State	Indicates the current state of the port as defined by the Multiple Spanning Tree Protocol. The state of a port can be Forwarding in one instance, and Discarding (Blocking) in another.

—End—

Configuring MSTI port properties

To configure MSTI port properties:

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the main menu, choose Application > Spanning Tree (MSTP) > Msti Port Configuration . |
|---|--|

The Msti Port Configuration page appears.

Msti Port Configuration page

Application > Spanning Tree (MSTP) > Msti Port Configuration ?

MST Instance

Msti

Submit

Spanning Tree - Msti Port Setting

Port	Priority (hex)	Path Cost
1	<input type="text" value="80"/>	<input type="text" value="20000"/>
2	<input type="text" value="80"/>	<input type="text" value="20000"/>
3		
4	<input type="text" value="80"/>	<input type="text" value="20000"/>
5	<input type="text" value="80"/>	<input type="text" value="20000"/>
6		
7		
8		
9		
10		
11		
12		
Switch	<input type="text" value="80"/> <input type="checkbox"/>	<input type="text" value="200000"/> <input type="checkbox"/>

Submit

[Ports 13 - 24](#) [Ports 25 - 26](#)

Msti Port Configuration page items

Section	Item	Description
MST Instance	Msti	The MSTI instance ID.
Spanning Tree - Msti Port Setting	Priority	Indicates the four most significant bits of the Port Identifier for a given spanning tree instance. You can modify this item independently for each spanning tree instance the bridge supports.
	Path Cost	The contribution of this port to the cost of paths towards the MSTI root that include this port.

—End—

Setting the STP mode using Device Manager

To set the STP operational mode using Device Manager:

Step	Action
1	From the Device Manager menu bar, choose VLAN > Spanning Tree > Globals . The Spanning Tree dialog box appears with the Globals tab displayed.
2	In the SpanningTreeAdminMode field, select the STP mode. The available modes are: <ul style="list-style-type: none"> • nortelStpg • rstp • mstp
3	Click Apply . A warning message appears reminding you that you must reset the switch for the change to take effect.
4	Click Yes .
5	Click Close .
6	To reset the switch, choose Edit > Chassis .
7	From the System tab, choose the reboot option and click Apply .

—End—

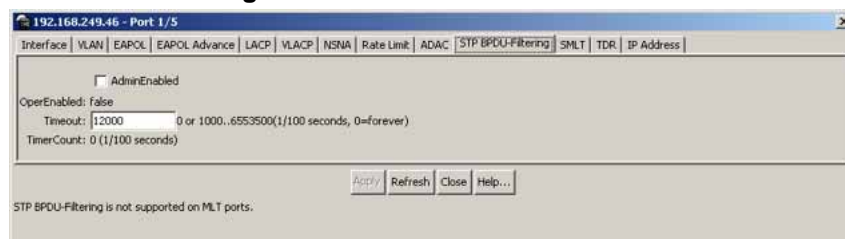
Configuring STP BPDU Filtering using Device Manager

You can use the **STP BPDU-Filtering** tab to configure STP BPDU Filtering on a port. This tab is available in all three STP modes.

To configure STP BPDU Filtering:

Step	Action
1	From the Device Manager menu, choose Edit > Port . The Port dialog box appears with the Interface tab displayed.
2	Click the STP BPDU-Filtering tab. The STP BPDU-Filtering tab appears.

STP BPDU-Filtering tab



STP BPDU-Filtering tab fields

Field	Description
AdminEnabled	Enables and disables BPDU filtering on the port.
OperEnabled	Indicates the current operational status of BPDU filtering on the port: true (enabled) or false (disabled).
Timeout	When BPDU filtering is enabled, this indicates the time (in 1/100 seconds) during which the port remains disabled after it receives a BPDU. The port timer is disabled if this value is set to 0. The default value is 12000 (120 seconds).
TimerCount	Displays the time remaining for the port to stay in the disabled state after receiving a BPDU.

—End—

Creating and Managing STGs using Device Manager

You can use the Java Device Manager (JDM) screens detailed in this section to create and manage Spanning Tree Groups.

Note: The STG dialog boxes and tabs described in this section are accessible only when the STP mode is set to Nortel STPG.

To configure STGs using Device Manager, refer to the following:

- ["Configuring STG global properties" \(page 254\)](#)
- ["Creating an STG" \(page 255\)](#)
- ["Adding a VLAN to an STG" \(page 257\)](#)
- ["Moving a VLAN between STGs" \(page 258\)](#)
- ["Deleting an STG" \(page 258\)](#)

- "Displaying STG Status" (page 258)
- "Displaying STG ports" (page 259)
- "Configuring STG port properties" (page 261)

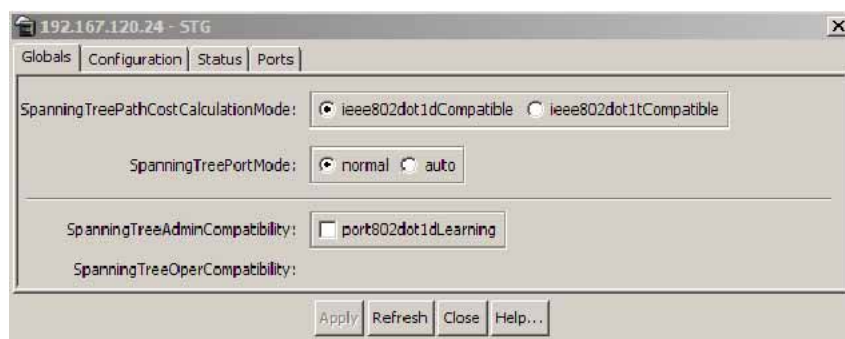
Configuring STG global properties

To configure the STG global properties:

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the Device Manager menu, choose VLAN > Spanning Tree > STG . |
|---|--|

The STG dialog box appears with the Globals tab displayed.



- | | |
|---|---|
| 2 | Select the STP path cost calculation mode: <ul style="list-style-type: none"> • ieee802dot1dCompatible • ieee802dot1tCompatible |
| 3 | Select the STP port mode: <ul style="list-style-type: none"> • normal • auto |
| 4 | Check the SpanningTreeAdminCompatibility box to enable 802.1d port learning. |
| 5 | Click Apply .
"STG Globals tab fields" (page 255) describes the fields in the STG Globals tab. |

STG Globals tab fields

Field	Description
SpanningTreePathCostCalculationMode	This object indicates the current spanning-tree path cost calculation mode. The value <code>ieee802dot1dCompatible</code> is valid only when the switch is running in Nortel STPG mode.
SpanningTreePortMode	This object sets the STG port membership mode for all Spanning Tree Groups on the switch.
SpanningTreeAdminCompatibility	This field Indicates whether the learning mode of a port stays in the Forwarding state or changes to the Disabled state when the port operation status goes down. If the box is checked, the port goes to the disabled state when down.
SpanningTreeOperCompatibility	This field indicates the operational compatibility mode for features controlled by the associated object.

—End—

Creating an STG

To create a Spanning Tree Group:

Step	Action
1	From the Device Manager menu, choose VLAN > Spanning Tree > STG . The STG dialog box appears with the Globals tab displayed.
2	Click the Configuration tab. The Configuration tab appears (" STG Configuration tab " (page 256)).

STG Configuration tab

Id	BridgeAddress	NumPorts	ProtocolSpecification	Priority	BridgeMaxAge	BridgeHelloTime	BridgeForwardDelay	EnableStp	TaggedBpduAddress	TaggedBpduVlanId
1	00:11:f9:35:d0:02	26	ieee8021d	32768	2000	200	1500	true	01:80:c2:00:00:00	4001
2	00:11:f9:35:d0:03	26	ieee8021d	32768	2000	200	1500	false	01:80:c2:00:00:00	4002
3	00:11:f9:35:d0:04	26	ieee8021d	32768	2000	200	1500	false	01:80:c2:00:00:00	4003
4	00:11:f9:35:d0:05	26	ieee8021d	32768	2000	200	1500	false	01:80:c2:00:00:00	4004

- 3 Click **Insert**.

The **Insert Configuration** dialog box appears ("Insert Configuration dialog box" (page 256)).

- 4 In the fields provided, fill in the information for the new STG.

Insert Configuration dialog box

"STG Configuration tab fields" (page 256) describes the fields in the Configuration tab.

STG Configuration tab fields

Field	Description
Id	Enter an integer between 1 and 8 that identifies the STG; 1 is the default STG.
BridgeAddress	Displays the MAC address used by this bridge; it is usually the smallest MAC address of all ports in the bridge.
NumPorts	Displays the number of ports controlled by this bridging entity.
ProtocolSpecification	Displays the version of spanning tree that is running.
Priority	Enter the first two octets of the 8-octet bridge ID; the range is 0 to 65 535.

Field	Description
BridgeMaxAge	Enter the maximum time you want to allow before the specified STG times out, in seconds; the range is 600 to 4 000.
BridgeHelloTime	Enter the maximum time between hellos, in seconds; the range is 100 to 1 000.
BridgeForwardDelay	Enter the maximum delay in forwarding, in seconds; the range is 400 to 3 000.
EnableStp	Enables or disables the spanning tree group.
TaggedBpduAddress	The address for the tagged BPDU.
TaggedBpduVlanId	Enter the VLAN ID for tagged BPDUs.

5 Click **Insert**.

—End—

The new STG is displayed in the STG Configuration tab.

Adding a VLAN to an STG

When using Device Manager, a VLAN can only be added to an STG at the time the VLAN is created.

To add a VLAN to an STG:

Step	Action
1	If it does not already exist, create the STG to which you want to add the VLAN. See " Creating an STG " (page 255) for more information about creating STGs.
2	Create the VLAN, making sure to select the desired StgId on the Insert VLAN screen.
3	Open the VLAN dialog box and view the Basic tab to confirm that the StgId field for the VLAN is the correct STG.

—End—

Moving a VLAN between STGs

You cannot use Device Manager to move VLANs between STGs on the Nortel Ethernet Routing Switch 5500 Series. Instead, delete the VLAN to be moved and add a replacement VLAN in the STG to which you want to move the VLAN.

Deleting an STG

To delete an STG, follow this procedure:

Step Action

- 1 From the menu, select **VLAN > Spanning Tree > STG**.
The STG dialog box appears ("[STG Configuration tab](#)" (page 256)).
 - 2 On the **Configuration** tab, select the STGs to be deleted.
 - 3 Click **Delete**.
-

—End—

Displaying STG Status

To display the status of an STG, follow this procedure:

Step Action

- 1 From the menu, select **VLAN > Spanning Tree > STG** .
The STG dialog box appears with the **Globals** tab displayed.
- 2 Select the **Status** tab.
The status of all current STGs is displayed. "[STG Status tab](#)" (page 258) illustrates this tab.

STG Status tab

Id	BridgeAddress	NumPorts	ProtocolSpecification	TimeSinceTopologyChange	TopChanges	DesignatedRoot	RootCost	RootPort	MaxAge	HelloTime	HoldTime	ForwardDelay
1	00:11:f9:35:d0:02	26	ieee8021d	0 day, 07h:06m:05s		01:80:00:00:04:38:d5:9a:81	20	1/3	2000	200	100	1500
2	00:11:f9:35:d0:03	26	ieee8021d	0 day, 07h:07m:04s		00:80:00:00:11:f9:26:d0:02	0	0	2000	200	100	1500
3	00:11:f9:35:d0:04	26	ieee8021d	0 day, 07h:07m:30s		00:00:00:00:00:00:00:00	0	0	0	0	0	0
4	00:11:f9:35:d0:05	26	ieee8021d	0 day, 07h:07m:30s		00:00:00:00:00:00:00:00	0	0	0	0	0	0

"[Status tab fields](#)" (page 258) describes the fields on this tab.

Status tab fields

Field	Description
Id	Displays the STG ID.

Field	Description
BridgeAddress	Displays the MAC address used by this bridge.
NumPorts	Displays the number of ports controlled by this bridging entity.
ProtocolSpecification	Displays the version of spanning tree that is running.
TimeSinceTopology Change	Displays the time, in hundredths of seconds, since the last topology change.
TopChanges	Displays the number of topology changes since the switch was reset.
DesignatedRoot	Displays the MAC address of the STP designated root.
RootCost	Displays the cost of the path to the root.
RootPort	Displays the port number of the port with the lowest-cost path from this bridge to the root bridge.
MaxAge	Displays the maximum age, in hundredths of a second, of STP information learned from any port in the network before the information is discarded.
HelloTime	Displays the amount of time, in hundredths of seconds, between Hello messages.
HoldTime	Displays the interval, in hundredths of seconds, during which no more than two Hello messages can be transmitted.
ForwardDelay	Displays the interval, in hundredths of seconds, during which the switch stays in Listening or Learning mode, before moving to Forwarding mode. This value is also used to age dynamic entries in the Forwarding Database.

—End—

Displaying STG ports

To display the STG port status:

Step	Action
------	--------

- | | |
|---|---|
| 1 | From the menu, select VLAN > Spanning Tree > STG . |
|---|---|

The STG dialog box appears with the Globals tab displayed.

- 2 Click the **Ports** tab.

The Ports tab is illustrated in "STG Ports tab" (page 260).

STG Ports tab

StgId	Priority	State	EnableStp	FastStart	AdminPathCost	PathCost	DesignatedRoot	DesignatedCost	DesignatedBridge	DesignatedPort	ForwardTransitions
1/1	1	disabled	false	false	0	1	80:00:00:11:f9:35:d0:01	0	80:00:00:11:f9:35:d0:01	80:01	00
1/1	2	128 forwarding	true	false	0	1	80:00:00:11:f9:35:d0:02	0	80:00:00:11:f9:35:d0:02	80:01	01
1/1	3	128 disabled	false	false	0	1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	00
1/1	4	128 disabled	false	false	0	1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	00
1/2	1	128 disabled	false	false	0	1	80:00:00:11:f9:35:d0:01	0	80:00:00:11:f9:35:d0:01	80:02	00
1/2	2	128 forwarding	true	false	0	1	80:00:00:11:f9:35:d0:02	0	80:00:00:11:f9:35:d0:02	80:02	01
1/2	3	128 disabled	false	false	0	1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	00
1/2	4	128 disabled	false	false	0	1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	00
1/3	1	128 forwarding	true	false	0	10	80:00:00:04:38:d5:9a:81	10	80:00:00:09:97:38:9e:61	80:0e	01
1/3	2	128 disabled	false	false	0	1	80:00:00:11:f9:35:d0:02	0	80:00:00:11:f9:35:d0:02	80:03	00
1/3	3	128 disabled	false	false	0	1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	00
1/3	4	128 disabled	false	false	0	1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	00
1/4	1	128 disabled	false	false	0	1	80:00:00:11:f9:35:d0:01	0	80:00:00:11:f9:35:d0:01	80:04	00
1/4	2	128 disabled	false	false	0	1	80:00:00:11:f9:35:d0:02	0	80:00:00:11:f9:35:d0:02	80:04	00
1/4	3	128 disabled	false	false	0	1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	00
1/4	4	128 disabled	false	false	0	1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	00
1/5	1	128 disabled	false	false	0	1	80:00:00:11:f9:35:d0:01	0	80:00:00:11:f9:35:d0:01	80:05	00
1/5	2	128 forwarding	true	false	0	1	80:00:00:11:f9:35:d0:02	0	80:00:00:11:f9:35:d0:02	80:05	01
1/5	3	128 disabled	false	false	0	1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	00
1/5	4	128 disabled	false	false	0	1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	00
1/6	1	128 forwarding	true	false	0	1	80:00:00:04:38:d5:9a:81	20	80:00:00:11:f9:35:d0:01	80:06	01
1/6	2	128 disabled	false	false	0	1	80:00:00:11:f9:35:d0:02	0	80:00:00:11:f9:35:d0:02	80:06	00
1/6	3	128 disabled	false	false	0	1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	00
1/6	4	128 disabled	false	false	0	1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	00
1/7	1	128 forwarding	true	false	0	1	80:00:00:04:38:d5:9a:81	20	80:00:00:11:f9:35:d0:01	80:07	01
1/7	2	128 disabled	false	false	0	1	80:00:00:11:f9:35:d0:02	0	80:00:00:11:f9:35:d0:02	80:07	00

- 3 View the information and, if desired, change the information in the Ports tab by entering updated information and by using the menus provided.

" Ports tab fields" (page 260) describes the fields on this tab.

Ports tab fields

Field	Description
<Untitled Column>	Displays the unit and port number.
StgId	Displays the STG ID number.
Priority	Specifies the port priority
State	Displays the STP state of the port: Disabled, Blocking, Listening, Learning, Forwarding.
EnableStp	Enables or disables STP on the port: True is enabled, and False is disabled.
FastStart	Enables or disables Fast Start STP on the port: True is enabled, and False is disabled.
AdminPathCost	Sets the PathCost value. The field displays 0 if no user-configured value exists.
PathCost	Displays the contribution of this port to the cost path of the spanning tree root.

Field	Description
DesignatedRoot	Displays the MAC address of the STP designated root.
DesignatedCost	Displays the path cost of the designated port of the segment connected to this port.
DesignatedBridge	Displays the MAC address of the designated bridge this port considers the designated bridge for this segment.
DesignatedPort	Displays the port ID of the designated bridge for this port segment.
ForwardTransitions	Displays the number of times the port transitioned from STP Learning to Forwarding state.

4 Click **Apply**.

—End—

Configuring STG port properties

The **STG** tab displays the spanning tree parameters for a port.

To view the **STG** tab, follow this procedure:

Step	Action
1	From the Device View, select the port to edit.
2	From the menu, select Edit > Port . The Port screen appears.
3	Select the STG tab. This tab is illustrated in "Port screen -- STG tab" (page 261).

Port screen -- STG tab



STG tab fields

Field	Description
StgId	The spanning tree group ID to which the VLAN belongs.

Field	Description
Priority	The value of the priority field that is contained in the first (in network byte order) octet of the (2-octet long) Port ID. The other octet of the Port ID is derived from the value of dot1dStpPort.
State	The current port state as defined by application of the Spanning Tree Protocol. This state controls the action a port takes when it receives a frame. If the bridge detects a port that is malfunctioning, it places that port into the broken state. For ports that are disabled (see EnableStp), this object has a value of Disabled.
EnableStp	Select True or False to enable or disable STP.
FastStart	Select True or False to enable or disable FastStart.
AdminPathCost	The administrative value of the PathCost. This is the value that has been configured by the user, or 0 if no user-configured value exists. If you specify the path cost in the PathCost field, the value in this field is modified as well.
PathCost	The contribution of this port to the cost of paths toward the spanning tree root, which includes this port. The IEEE 802.1D-1990 standard recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN.
DesignatedRoot	The unique Bridge Identifier of the bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached.
DesignatedCost	The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs.
DesignatedBridge	The Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port segment.
DesignatedPort	The Port Identifier of the port on the Designated Bridge for this port segment.
ForwardTransitions	The number of times this port has transitioned from the Learning state to the Forwarding state.

- 4 Click **Apply** after making any changes.

—End—

Configuring RSTP using Device Manager

The Rapid Spanning Tree protocol (RSTP or IEEE 802.1w) reduces the recovery time after a network breakdown. It also maintains a backward compatibility with the IEEE 802.1d which was the Spanning Tree implementation prior to RSTP. In certain configurations, the recovery time of RSTP can be reduced to less than 1 second.

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

Note: The RSTP dialog boxes and tabs described in this section are accessible only when the STP mode is set to RSTP.

This section contains information on the following topics:

- [Undefined Resource](#)
- ["RSTP Ports tab" \(page 266\)](#)
- ["RSTP Status tab" \(page 269\)](#)
- ["Graphing RSTP Port Statistics" \(page 270\)](#)

RSTP Globals tab

The Globals tab in the RSTP dialog box provides general information about RSTP when RSTP is the active mode.

To view the Globals tab:

Step	Action
1	From the Device Manager menu bar, choose VLAN > Spanning Tree > RSTP . The RSTP dialog box appears with the Globals tab displayed.

RSTP Globals tab

RSTP - Globals tab fields

Field	Description
PathCostDefault	<p>Sets the version of the Spanning Tree default Path Costs that the Bridge uses.</p> <p>The value of 16-bit uses the 16-bit default Path Costs from IEEE Std. 802.1D-1998.</p> <p>A value of 32-bit uses the 32-bit default Path Costs from IEEE Std. 802.1t.</p>
TXHoldCount	<p>The value used by the Port Transmit state machine to limit the maximum transmission rate. The value can range from 1 to 10.</p>

Field	Description
Version	The version of the Spanning Tree Protocol the bridge is currently running: <ul style="list-style-type: none"> stpCompatible: indicates that the bridge uses the Spanning Tree Protocol specified in IEEE 802.1D. rstp: indicates that the bridge uses the Rapid Spanning Tree Protocol specified in IEEE 802.1w.
Priority	The value of the writable portion of the Bridge Identifier comprising the first two octets. The values that are set for Priority must be in steps of 4096.
BridgeMaxAge	The value in 1/100 seconds that all bridges use for MaxAge when this bridge acts as the root. The value must be a multiple of 100. The range is 600 to 4000.
BridgeHelloTime	The value in 1/100 seconds that all bridges use for HelloTime when this bridge acts as the root. The value must be a multiple of 100. The range is 100 to 1000.
BridgeForward Delay	The value in 1/100 seconds that all bridges use for ForwardDelay when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of BridgeMaxAge. The value must be a multiple of 100. The range is 400 to 3000.
DesignatedRoot	The unique identifier of the Bridge recorded as the Root in the Configuration BPDUs that are transmitted by the Designated Bridge for the segment to which the port is attached. Reference IEEE 802.1D-1990: Section 4.5.5.4.
RootCost	The cost of the path to the root as seen from this bridge.
RootPort	The port number of the port that offers the lowest cost path from this bridge to the root bridge.
MaxAge	The maximum age of Spanning Tree Protocol information learned from the network on any port before being discarded. The maximum age is specified in units of hundredths of a second. This is the actual value that the bridge uses.

Field	Description
HelloTime	The amount of time required for transmission of the configuration BPDUs by the node on any port when it is the root of the spanning tree or trying to become the root. This is specified in units of hundredths of a second. This is the actual value that the bridge uses.
ForwardDelay	This time value, measured in units of hundredths of a second, controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state.
RstpUpCount	The number of times the RSTP Module has been enabled. A trap is generated on the occurrence of this event.
RstpDownCount	The number of times the RSTP Module has been disabled. A trap is generated on the occurrence of this event.
NewRootIdCount	The number of times this Bridge has detected a Root Identifier change. A trap is generated on the occurrence of this event.
TimeSinceTopologyChange	Change time (in hundredths of a second) since the TcWhile Timer for any port in this Bridge was non-zero for the Common Spanning Tree context.
TopChanges	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.

—End—

RSTP Ports tab

To view the RSTP Ports tab:

- | Step | Action |
|------|--|
| 1 | From the Device Manager menu bar, choose VLAN > Spanning Tree > RSTP .
The RSTP dialog box appears with the Globals tab displayed. |
| 2 | Click the RSTP Ports tab.
The RSTP Ports tab appears. |

RSTP Ports tab

Port	State	Priority	PathCost	ProtocolMigration	AdminEdgePort	OperEdgePort	AdminPointToPoint	OperPointToPoint	Participating	DesignatedRoot	DesignatedCost
1	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
2	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
3	forwarding	128	20000	false	false	false	ForceTrue	true	true	80:00:00:04:38:05:9a:81	10:00:00
4	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
5	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
6	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
7	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
8	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
9	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
10	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
11	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
12	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
13	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
14	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
15	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
16	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
17	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
18	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
19	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
20	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
21	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
22	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
23	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00
24	discarding	128	20000	false	false	false	ForceTrue	true	true	00:00:00:00:00:00:00:00	0:00:00

RSTP Ports tab fields

Field	Description
Port	The port number.
State	Used to identify a port state in this RSTP instance. The port state is cataloged as discarding, learning, and forwarding.
Priority	The value of the priority field which is contained in the first (in network byte order) octet of the (2 octet long) Port ID.
PathCost	The contribution of this port to the cost of paths towards the spanning tree root.
ProtocolMigration	Indicates the Protocol migration state of this port. Set this field to true to force the port to transmit RSTP BPDUs. Note: If this field is set to true and the port receives an 802.1d type BPDU, the port again begins transmitting 802.1d BPDUs.
AdminEdgePort	The administrative value of the Edge Port parameter. A value of true indicates that this port is assumed to be an edge-port and a value of false indicates that this port is assumed to be a nonedge-port.
OperEdgePort	The operational value of the Edge Port parameter. The object is initialized to false on reception of a BPDU.

Field	Description
AdminPointToPoint	<p>The administrative point-to-point status of the LAN segment attached to this port.</p> <ul style="list-style-type: none"> • A value of forceTrue indicates that this port is always treated as being connected to a point-to-point link. • A value of forceFalse indicates that this port is treated as having a shared media connection. • A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means.
OperPointToPoint	<p>The operational point-to-point status of the LAN segment attached to this port. This field indicates whether a port is considered to have a point-to-point connection. The value is determined by management or by auto-detection.</p>
Participating	<p>This field specifies whether a port is participating in the 802.1w protocol.</p>
DesignatedRoot	<p>The bridge identifier of the old root of the Spanning Tree as determined by the Spanning Tree Protocol as executed by this node.</p>
DesignatedCost	<p>The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received BPDUs.</p>
DesignatedBridge	<p>The Bridge Identifier of the bridge which this port considers to be the Designated Bridge for this port segment.</p>
DesignatedPort	<p>The Port Identifier for the port segment which is on the Designated Bridge.</p>
ForwardTransitions	<p>The number of times this port has transitioned from the Learning state to the Forwarding state.</p>

—End—

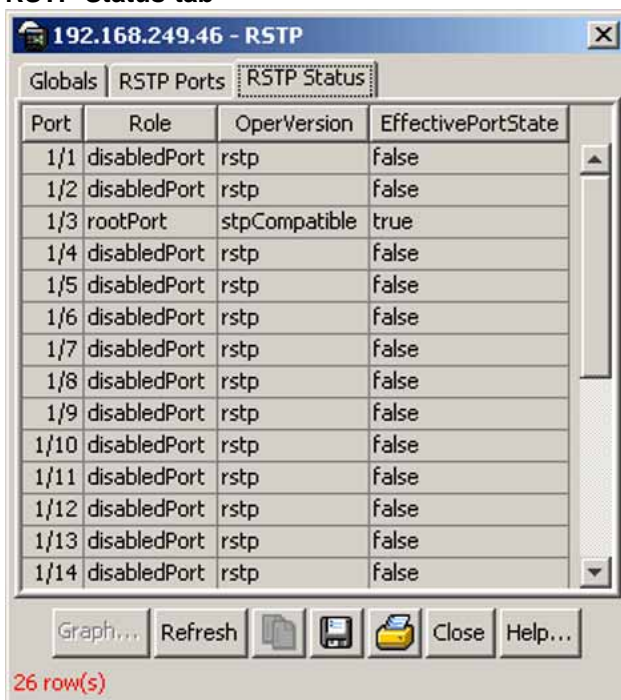
RSTP Status tab

To view the **RSTP Status** tab:

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the Device Manager menu bar, choose VLAN > Spanning Tree > RSTP .
The RSTP dialog box appears with the Globals tab displayed. |
| 2 | Click the RSTP Status tab.
The RSTP Status tab appears. |

RSTP Status tab



RSTP Status tab fields

Field	Description
Port	The port number.
Role	A role represents a functionality characteristic or capability of a resource to which policies are applied.

Field	Description
OperVersion	This indicates whether the Port is operationally in the RSTP mode or the STP-compatible mode; that is, whether the Port is transmitting RSTP BPDUs or Config/TCN BPDUs.
EffectivePortState	This is the effective Operational state of the port. This object is set to true only when the port is operationally up in the interface manager and when the force Port State and specified port state for this port is enabled. Otherwise, this object is set to false.

—End—

Graphing RSTP Port Statistics

You can use the **RSTP Stats** tab to graph RSTP port statistics.

To open the RSTP Stats tab for graphing:

Step Action

- 1 From the Device Manager menu bar, choose **VLAN > Spanning Tree > RSTP**.
The RSTP dialog box appears with the Globals tab displayed.
- 2 Click the **RSTP Status** tab.
- 3 Select a port and click **Graph** to get the statistics for the RSTP Port.
The RSTP Stats tab appears.

RSTP Stats

	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
RxRstpBpduCount	0	0	0	0	0	0
RxConfigBpduCount	418	5	0.5	0.5	0.5	0.5
RxTcnBpduCount	0	0	0	0	0	0
TxRstpBpduCount	4	0	0	0	0	0
TxConfigBpduCount	0	0	0	0	0	0
TxTcnBpduCount	0	0	0	0	0	0
InvalidRstpBpduRxCount	0	0	0	0	0	0
InvalidConfigBpduRxCount	0	0	0	0	0	0
InvalidTcnBpduRxCount	0	0	0	0	0	0
ProtocolMigrationCount	1	0	0	0	0	0

Clear Counters Close Help... Poll Interval: 10s 0 day, 00h:00m:10s

RSTP Stats tab field descriptions

Field	Description
RxRstBpduCount	The number of RST BPDUs that have been received on the port.
RxConfigBpduCount	The number of Config BPDUs that have been received on the port.
RxTcnBpduCount	The number of TCN BPDUs that have been received on the port.
TxRstBpduCount	The number of RST BPDUs that have been transmitted by this port.
TxConfigBpduCount	The number of Config BPDUs that have been transmitted by this port.
TxTcnBpduCount	The number of TCN BPDUs that have been transmitted by this port.
InvalidRstBpduRxCount	The number of invalid RSTP BPDUs that have been received on this port.
InvalidConfigBpduRxCount	The number of invalid Configuration BPDUs that have been received on this port.
InvalidTcnBpduRxCount	The number of invalid TCN BPDUs that have been received on this port.
ProtocolMigrationCount	The number of times this Port has migrated from one STP protocol version to another. The relevant protocols are STP-COMPATIBLE and RSTP.

—End—

Configuring MSTP using Device Manager

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

In the MSTP mode, the 5500 Series switches support a maximum of one Common and Internal Spanning Tree (CIST) and seven Multiple Spanning Tree Instances (MSTI).

Within the CIST, the Internal Spanning Tree component is used only by devices from the same region (for which a regional root is elected). The Common (External) Spanning Tree component of the CIST is used by devices from different regions or between devices with different STP modes.

Note: The MSTP dialog boxes and tabs described in this section are accessible only when the STP mode is set to MSTP.

This section contains information on the following topics:

- "MSTP Globals tab" (page 272)
- "CIST Port tab" (page 277)
- "Graphing CIST Port statistics" (page 280)
- "MSTI Bridges tab" (page 281)
- "Associating a VLAN with the CIST or an MSTI instance" (page 283)
- "Modifying VLAN CIST or MSTI association" (page 284)
- "MSTI Port tab" (page 285)
- "Graphing MSTI Port Statistics" (page 286)

MSTP Globals tab

To view the MSTP Globals tab:

Step	Action
1	From the Device Manager menu bar, choose VLAN > Spanning Tree > MSTP . The MSTP dialog box appears with the Globals tab displayed.

MSTP Globals tab

192.168.249.46 - MSTP

Globals | CIST Port | MSTI Bridges | MSTI Port

-MSTP-

PathCostDefaultType: 16-bit 32-bit

TxHoldCount: 1..10

MaxHopCount: 100..4000 (1/100 sec, in multiple of 100)

NoOfInstancesSupported: 8

MstpUpCount: 00

MstpDownCount: 00

-CIST-

ForceProtocolVersion: stpCompatible rstp mstp

BrgAddress: 00:11:f9:35:d0:00

Root: 80:00:00:04:38:d5:9a:81

RegionalRoot: 80:00:00:11:f9:35:d0:00

RootCost: 200000

RegionalRootCost: 0

RootPort: 1/1

BridgePriority: 0..61440 (in multiple of 4096)

BridgeMaxAge: 600..4000 (1/100 sec, in multiple of 100)

BridgeForwardDelay: 400..3000 (1/100 sec, in multiple of 100)

HoldTime: 100 (1/100 sec)

MaxAge: 2000 (1/100 sec)

ForwardDelay: 1500 (1/100 sec)

TimeSinceTopologyChange: 1 day, 00h:20m:31s

TopChanges: 02

NewRootBridgeCount: 01

-MSTI Region-

RegionName:

RegionVersion: 0..65535

ConfigIdSel: 0..255

ConfigDigest: ac:36:17:7f:50:28:3c:d4:b8:38:21:d8:ab:26:de:62

RegionConfigChangeCount: 00

Apply Refresh Close Help...

MSTP Globals tab fields

Field	Description
PathCostDefaultType	The version of the Spanning Tree default Path Costs that are used by this Bridge. A 16-bit value uses the 16-bit default path costs from IEEE Standard 802.1D-1998. A 32-bit value uses the 32-bit default path costs from IEEE Standard. 802.1t.
TxHoldCount	The value used by the Port Transmit state machine to limit the maximum transmission rate.
MaxHopCount	The Maximum Hop Count value in 1/100 seconds. The value must be a multiple of 100. The range is 100 to 4000.
NoOfInstancesSupported	Indicates the maximum number of spanning tree instances supported.
MstpUpCount	The number of times the MSTP Module is enabled. A trap is generated on the occurrence of this event.
MstpDownCount	The number of times the MSTP Module is disabled. A trap is generated on the occurrence of this event.
ForceProtocolVersion	Signifies the version of the Spanning Tree Protocol that the bridge is currently running. <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.

Field	Description
Root	The bridge identifier of the root of the common spanning tree as determined by the Spanning Tree Protocol as executed by this node. This value is used as the CIST Root Identifier parameter in all Configuration BPDUs originated by this node.
RegionalRoot	The bridge identifier of the root of the Multiple Spanning Tree region as determined by the Spanning Tree Protocol as executed by this node. This value is used as the CIST Regional Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
RootCost	The cost of the path to the CIST Root as seen from this bridge.
RegionalRootCost	The cost of the path to the CIST Regional Root as seen from this bridge.
RootPort	The port number of the port which offers the lowest path cost from the bridge to the CIST Root Bridge
BridgePriority	The value of the writable portion of the Bridge Identifier comprising the first two octets. The values that are set for Bridge Priority must be in steps of 4096.
BridgeMaxAge	The value in hundredths of a second that all bridges use for MaxAge when this bridge acts as the root. The value must be a multiple of 100. The range is 600 to 4000.
BridgeForwardDelay	The value in hundredths of a second that all bridges use for ForwardDelay when this bridge acts as the root. IEEE 802.1D specifies that the range for this parameter is related to the value of BridgeMaxAge. The value must be a multiple of 100. The range is 400 to 3000.
HoldTime	This value determines the time interval during which no more than two Configuration BPDUs can be transmitted by this node. This value is measured in units of hundredths of a second.

Field	Description
MaxAge	The maximum age, in hundredths of a second, of the Spanning Tree Protocol information learned from the network on any port before being discarded. This value is the actual value that this bridge is currently using.
ForwardDelay	This value controls how fast a port changes its STP state when moving towards the Forwarding state. This value determines how long the port stays in a particular state before moving to the next state. This value is measured in units of hundredths of a second.
TimeSinceTopology Change	The time, in hundredths of a second, since the TcWhile Timer for any port in this Bridge was non-zero for the Common Spanning Tree context.
NewRootBridgeCount	The number of times this Bridge detects a Root Bridge change for the Common Spanning Tree context. A Trap is generated when this event occurs.
TopChanges	The number of times that at least one non-zero TcWhile Timer occurred on this Bridge for the Common Spanning Tree context.
RegionName	Specifies the region name of the configuration. By default, the Region Name is equal to the Bridge Mac Address.
ConfigIdSel	The Configuration Identifier Format Selector used by the Bridge. This has a fixed value of 0 which indicates RegionName, RegionVersion, as specified in the standard.
RegionVersion	Denotes the version of the MST Region.
ConfigDigest	Signifies the Configuration Digest value for this Region. This is an MD5 digest value and hence must always be 16 octets long.
RegionConfigChange Count	The number of times a Region Configuration Identifier Change is detected. A trap is generated when this event occurs.

—End—

CIST Port tab

To view the **CIST Port** tab:

Step	Action
------	--------

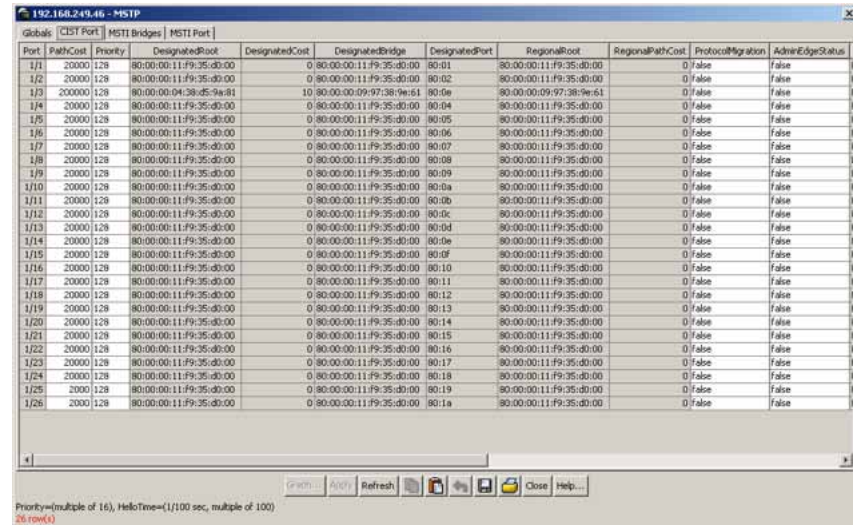
- 1 From the Device Manager menu bar, choose **VLAN > Spanning Tree > MSTP**.

The MSTP dialog box appears with the Globals tab displayed.

- 2 Click the **CIST Port** tab.

The CIST Port tab appears.

CIST Port tab



CIST Port tab fields

Field	Description
Port	The port number of the port containing Spanning Tree information.
PathCost	The contribution of this port to the cost of paths towards the CIST Root.
Priority	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.

Field	Description
DesignatedRoot	This field specifies the unique Bridge Identifier of the bridge. Recorded as the CIST Root in the configuration BPDUs which are transmitted.
DesignatedCost	The path cost of the Designated Port of the segment connected to this port.
DesignatedBridge	The unique Bridge Identifier of the bridge which the port considers to be the Designated Bridge for the port segment.
DesignatedPort	The Port identifier of the port on the Designated Bridge which is designated for the port segment.
RegionalRoot	Displays the unique Bridge Identifier of the bridge. Recorded as the CIST Regional Root Identifier in the configuration BPDUs which are transmitted.
RegionalPathCost	The contribution of this port to the cost of paths towards the CIST Regional Root.
ProtocolMigration	Indicates the Protocol migration state of this port. When operating in MSTP mode, set this field to true to force the port to transmit MSTP BPDUs without instance information. Note: If this field is set to true and the port receives an 802.1d BPDU, the port begins transmitting 802.1d BPDUs. If the port receives an 802.1w BPDU, it begins transmitting 802.1w BPDUs.
AdminEdgeStatus	The administrative value of the Edge Port parameter. A value of true indicates that this port can be assumed to be an edge-port, and a value of false indicates that this port can be assumed to be a nonedge-port.
OperEdgeStatus	Signifies the operational value of the Edge Port parameter. This value is initialized to the value of AdminEdgeStatus and set to false when the port receives a BPDU.

Field	Description
AdminP2P	The administrative point-to-point status of the LAN segment attached to this port. A value of 0 indicates that this port is always treated as being connected to a point-to-point link. A value of 1 indicates that this port is treated as having a shared media connection. A value of 2 indicates that this port is considered to have a point-to-point link if it is an Aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation, or by management means.
OperP2P	This field indicates the operational point-to-point status of the LAN segment attached to the port. It also indicates whether a port is considered to have a point-to-point connection. The value is determined by management or by auto-detection, as described in the AdminP2P object.
HelloTime	The amount of time between the transmission of Configuration BPDUs transmitted by this node on the port. Measured in units of hundredths of a second.
OperVersion	This indicates whether the Port is operationally in the MSTP, RSTP, or STP-compatible mode; that is, whether the port is transmitting MST BPDUs, RST BPDUs, or Config/TCN BPDUs.
EffectivePortState	The effective operational state of the port for CIST. This is set to true only when the port is operationally up in the Interface level and Protocol level for CIST. This is set to false for all other times.
State	The current state of the port as defined by the Common Spanning Tree Protocol.
ForcePortState	The current state of the port which can be changed to either Disabled or Enabled for the base Spanning Tree instance.
SelectedPortRole	Selected port role for the Spanning Tree instance.
CurrentPortRole	Current port role for the Spanning Tree instance.

—End—

Graphing CIST Port statistics

The CIST Port Stats tab shows CIST Port statistics.

To open the CIST Port Stats tab for graphing:

Step	Action
1	From the Device Manager menu bar, choose VLAN > Spanning Tree > MSTP . The MSTP dialog box appears with the Globals tab displayed.
2	Click the CIST Port tab. The CIST Port tab appears.
3	Select a port and click Graph to get the statistics for the CIST Port. The following table describes the fields that are displayed in the CIST Port Stats tab.

CIST Port Stats fields

Field	Description
ForwardTransitions	The number of times this port transitioned to the Forwarding State.
RxMstBpduCount	The number of MST BPDUs received on this port.
RxRstBpduCount	The number of RST BPDUs received on this port.
RxConfigBpduCount	The number of Configuration BPDUs received on this port.
RxTcnBpduCount	The number of TCN BPDUs received on this port.
TxMstBpduCount	The number of MST BPDUs transmitted from this port.
TxRstBpduCount	The number of RST BPDUs transmitted from this port.
TxConfigBpduCount	The number of Configuration BPDUs transmitted from this port.
TxTcnBpduCount	The number of TCN BPDUs transmitted from this port.

Field	Description
InvalidMstBpduRxCount	The number of Invalid MST BPDUs received on this port.
InvalidRstBpduRxCount	The number of Invalid RST BPDUs received on this port.
InvalidConfigBpduRxCount	The number of Invalid Configuration BPDUs received on this port.
InvalidTcnBpduRxCount	The number of Invalid TCN BPDUs received on this port.
ProtocolMigrationCount	The number of times this port migrated from one STP protocol version to another. The relevant migration protocols are STP-COMPATIBLE and RSTP/MSTP. A trap is generated when the port migrates.

—End—

MSTI Bridges tab

To view the MSTI Bridges tab:

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the Device Manager menu bar, choose VLAN > Spanning Tree > MSTP .
The MSTP dialog box appears with the Globals tab displayed. |
| 2 | Click the MSTI Bridges tab.
The MSTI Bridges tab appears. |

MSTI Bridges tab



MSTI Bridges tab fields

Field	Description
Instance	Spanning Tree Instance to which the information belongs.

Field	Description
RegionalRoot	Indicates the MSTI Regional Root Identifier value for the Instance. This value is used as the MSTI Regional Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
Priority	The writable portion of the MSTI Bridge Identifier comprising the first two octets. The values that are set for Bridge Priority must be in steps of 4096.
RootCost	The cost of the path to the MSTI Regional Root as seen by this bridge.
RootPort	The number of the port which offers the lowest path cost from this bridge to the MSTI Region Root Bridge.
Enabled	Used to control whether the bridge instance is enabled or disabled.
TimeSinceTopology Change	The time (measured in hundredths of a second) since the TcWhile Timer for any port in this Bridge was non-zero for this Spanning Tree instance.
TopChanges	The number of times that at least one non-zero TcWhile Timer occurred on this Bridge for this Spanning Tree instance.
NewRootCount	The number of times this Bridge has detected a Root Bridge change for this Spanning Tree instance. A Trap is generated on the occurrence of this event.
InstanceUpCount	The number of times a new Spanning Tree instance was created. A Trap is generated on the occurrence of this event.
InstanceDownCount	The number of times a Spanning Tree instance was deleted. A Trap is generated on the occurrence of this event.

—End—

Inserting MSTI Bridges

To insert an MSTI bridge:

Step	Action
1	From the Device Manager menu bar, choose VLAN > Spanning Tree > MSTP . The MSTP dialog box appears with the Globals tab displayed.
2	Click the MSTI Bridges tab. The MSTI Bridges tab appears.
3	In the MSTI Bridges tab, click the Insert button. The Instance dialog box appears with the next available instance shown.
4	Click Insert . The next available instance appears in the MSTI Bridges tab.

—End—

Deleting MSTI Bridges

Step	Action
1	From the Device Manager menu bar, choose VLAN > Spanning Tree > MSTP . The MSTP dialog box appears with the Globals tab displayed.
2	Click the MSTI Bridges tab. The MSTI Bridges tab appears.
3	In the MSTI Bridges tab, click the Instance field for the MSTI bridge that you want to delete.
4	Click Delete . The selected instance is deleted from the MSTI Bridges tab.

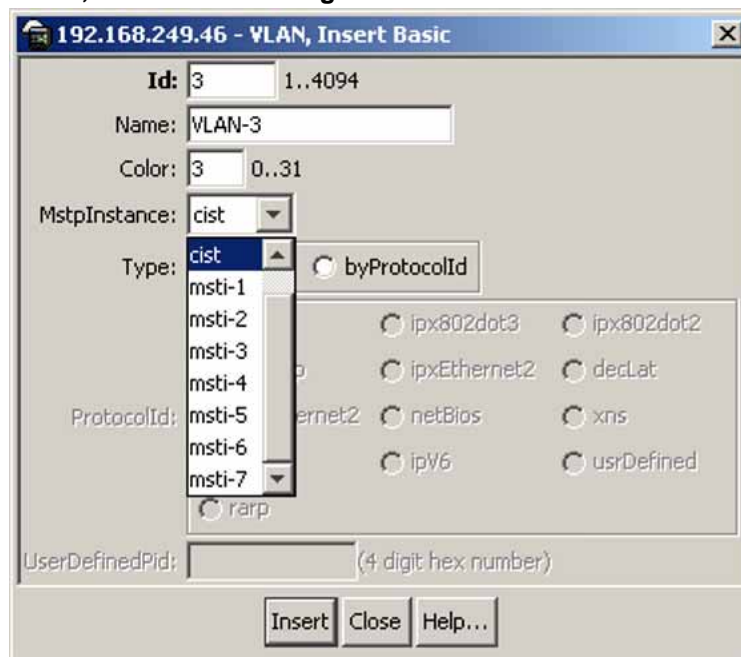
—End—

Associating a VLAN with the CIST or an MSTI instance

You can use Device Manager to associate a VLAN with the CIST or an MSTI instance. To associate a VLAN with the CIST or an MSTI instance:

- | Step | Action |
|------|--|
| 1 | From the Device Manager menu bar, choose VLAN > VLANs .
The VLAN dialog box appears with the Basic tab displayed. |
| 2 | Click Insert .
The VLAN, Insert Basic dialog box appears. |

VLAN, Insert Basic dialog box



- In the **MstpInstance** field, select the CIST or an MSTI instance from the menu.
- Populate the other fields as required.
- Click **Insert**.

—End—

Modifying VLAN CIST or MSTI association

To modify an existing VLAN association with a CIST or MSTI:

- | Step | Action |
|------|--|
| 1 | From the VLAN Basic tab, double-click in the MstpInstance field. |

The MstpInstance menu appears.

VLAN Basic tab with MstpInstance menu



- 2 Select the CIST option or one of the MSTI options and click **Apply**. This associates the VLAN with the option you selected.

—End—

MSTI Port tab

To view the MSTI Port tab:

Step Action

- 1 From the Device Manager menu bar, choose **VLAN > Spanning Tree > MSTP**.
The MSTP dialog box appears with the Globals tab displayed.
- 2 Click the **MSTI Port** tab.
The MSTI Port tab appears.

MSTI Port tab



MSTI Port tab fields

Field	Description
Port	Denotes the port number.
BridgeInstance	The number of times a Spanning Tree instance was deleted. A Trap is generated when this event occurs.
State	Indicates the current state of the port as defined by the Multiple Spanning Tree Protocol. The state of a port can be Forwarding or Discarding (Blocking).

Field	Description
ForcePortState	Signifies the current state of the port which can be changed to either Disabled or Enabled for the specific Spanning Tree instance.
PathCost	The contribution of this port to the cost of paths towards the MSTI Root which includes this port.
Priority	Indicates the four most significant bits of the Port Identifier for a given Spanning Tree instance. This value can be modified independently for each Spanning Tree instance supported by the Bridge. The values set for Port Priority must be in steps of 16.
DesignatedRoot	The unique Bridge Identifier of the bridge recorded as the MSTI Regional Root in the configuration BPDUs that are transmitted.
DesignatedBridge	The unique Bridge Identifier of the bridge which this port considers to be the Designated Bridge for the port segment.
DesignatedPort	The Port identifier of the port on the Designated Bridge for this port segment.
DesignatedCost	The path cost of the Designated Port of the segment connected to this port.
CurrentPortRole	Current Port Role of the port for this spanning tree instance.
EffectivePortState	The effective operational state of the port for the specific instance. This is set to true only when the port is operationally up in the interface level and Protocol level for the specific instance. This is set to false at all other times.

—End—

Graphing MSTI Port Statistics

The **MSTI Port** tab can be used to graph MSTI port statistics.

To open the **MSTI Port** tab for graphing:

- | Step | Action |
|------|---|
| 1 | From the Device Manager menu bar, choose VLAN > Spanning Tree > MSTP .
The MSTP dialog box appears with the Globals tab displayed. |
| 2 | Click the MSTI Port tab. |
| 3 | Select a port and click Graph to get the statistics for the MSTI Port.
The following table describes the fields in the MSTI Port Statistics fields. |

Field	Description
ForwardTransitions	Number of times this port transitioned to the Forwarding State for the specific instance.
ReceivedBPDUs	Number of BPDUs received by this port for this spanning tree instance.
TransmittedBPDUs	Number of Invalid BPDUs received on this Port for this Spanning Tree instance.
InvalidBPDUsRcvd	Number of BPDUs transmitted on this port for this Spanning Tree instance.

—End—

MultiLink Trunking (MLT)

MultiLink Trunking (MLT) can be configured in the Nortel Ethernet Routing Switch 5500 Series through the Command Line Interface (CLI), Web-based Management Interface, or the Java Device Manager (JDM). This chapter outlines the creation and management of MLTs using these switch interfaces.

Trunk groups

A trunk group refers to a group of physical ports that are aggregated together to form a single, logical, high-bandwidth port.

The Nortel Ethernet Routing Switch 5500 Series supports two types of trunk groups:

1. **Multilink trunk (MLT)** -- A multilink trunk allows a switch administrator to group multiple ports (up to eight) at the time of linking to another switch or server. This increases the aggregate throughput of the interconnection between two devices; up to 8 Gbit in full-duplex mode.

The Nortel Ethernet Routing Switch 5500 Series can be configured with up to 32 multilink trunks.

2. **Link Aggregation Group (LAG)** -- Trunk groups that are based on the Link Aggregation Control Protocol (LACP) are referred to as Link Aggregation Groups.

LACP, defined by the IEEE 802.3ad standard, enables a switch to learn the presence and capabilities of a remote switch by exchanging information with the remote switch before the formation of a trunk group. 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.

Trunk members can be configured within a single unit in the stack or distributed between any of the units within the stack configuration. Spreading trunk members across a stack is referred to as distributed trunking.

This chapter discusses the creation and management of multilink trunks. Refer to "[Configuring LACP and VLACP](#)" (page 319) for information on Link Aggregation Groups.

Creating and Managing MLTs using the CLI

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

show mlt command

The `show mlt` command displays the Multilink Trunking (MLT) configuration and utilization.

The syntax for the `show mlt` command is:

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

Substitute `<1-32>` with the number of the MLT whose utilization is to be displayed.

The `show mlt` command is executed in the Privileged EXEC command mode.

mlt command

The `mlt` command configures a multilink trunk (MLT).

The syntax for the `mlt` command is:

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

The `mlt` command is executed in the Global Configuration command mode.

"[mlt parameters](#)" (page 290) outlines the parameters for this command.

mlt parameters

Parameter	Description
id	Enter the trunk ID; the range is 1 to 32.
name <trunkname>	Specifies a text name for the trunk; enter up to 16 alphanumeric characters.
enable disable	Enables or disables the trunk.
member <portlist>	Enter the ports that are members of the trunk.

Parameter	Description
learning <disable fast normal>	Sets STP learning mode.
bpdu {all-ports single-port}	Sets trunk to send and receive BPDUs on either all ports or a single port.
loadbalance {basic advance}	Sets the MLT load-balancing mode: - basic: MAC-based load-balancing - advance: IP-based load-balancing

no mlt command

The `no mlt` command disables a multilink trunk (MLT), clearing all the port members.

The syntax for the `no mlt` command is:

```
no mlt [<id>]
```

Substitute <id> with the number of the MLT to be disabled.

The `no mlt` command is executed in the Global Configuration command mode.

show mlt spanning-tree command

The `show mlt spanning-tree` command displays the properties of multilink trunks (MLT) participating in Spanning Tree Groups (STG).

The syntax for this command is:

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

Substitute <1-32> with the multilink trunk ID of the MLT to display.

The `show mlt spanning-tree` command is executed in the Global Configuration command mode.

mlt spanning-tree command

The `mlt spanning-tree` command sets Spanning Tree Protocol (STP) participation for multilink trunks (MLT).

The syntax for the `mlt spanning-tree` command is:

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

"[mlt spanning-tree parameters](#)" (page 292) outlines the parameters for this command.

mlt spanning-tree parameters

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

The `mlt spanning-tree` command is executed in the Global Configuration command mode.

Creating and Managing MLTs using the Web-based Management Interface

The Web-based Management Interface screens detailed in this section allow for the creation and management of multilink trunks.

Creating a multilink trunk

To create a MLT, follow this procedure:

Step	Action
1	From the menu, select Applications > MultiLink Trunk > Group . The Multilink Trunk Group page appears (" MLT Group page " (page 293)).

MLT Group page

Application > MultiLink Trunk > Group

MultiLink Trunk Group Setting

Trunk	Trunk Members	STP	Trunk Mode	Trunk Name	Trunk Status			
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #1	Disabled
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #2	Disabled
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #3	Disabled
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #4	Disabled
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #5	Disabled
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #6	Disabled
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #7	Disabled
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #8	Disabled
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #9	Disabled
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #10	Disabled
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #11	Disabled
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #12	Disabled
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #13	Disabled
14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #14	Disabled
15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #15	Disabled
16	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #16	Disabled
17	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #17	Disabled
18	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #18	Disabled
19	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #19	Disabled
20	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #20	Disabled
21	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #21	Disabled
22	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #22	Disabled
23	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #23	Disabled
24	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #24	Disabled
25	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #25	Disabled
26	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #26	Disabled
27	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #27	Disabled
28	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #28	Disabled
29	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #29	Disabled
30	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #30	Disabled
31	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #31	Disabled
32	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic	Trunk #32	Disabled

Submit

- 2 In the fields provided, fill in the information for the MLT to be created. " Multilink Trunk Group Setting fields" (page 294) outlines the fields on this page.

Multilink Trunk Group Setting fields

Field	Description
Trunk Members	Type the port numbers to associate with the corresponding trunk. Note: Between two and eight switch ports can be configured together as members of a trunk to a maximum of 32 trunks. Switch ports can only be assigned to be a member of a single trunk.
STP	Choose the parameter that allows the specified trunk to participate in the spanning tree group. This setting overrides those of the individual trunk members. Selecting Fast shortens the state transition timer by two seconds. Refer to " Configuring Spanning Tree Group Participation " (page 294) on page 111 for a complete explanation of this process.
Trunk Mode	Choose the preferred trunk load-balancing mode: basic or advanced.
Trunk Name	Type a character string to create a unique name to identify the trunk, for example, Trunk1. The name, if chosen carefully, can provide meaningful information to you. For example, S1:T1 to FS2 indicates that Trunk1, in Switch1 connects to File Server 2.
Trunk Status	Choose to enable or disable any of the existing multilink trunks. Note: When a trunk is not active (Trunk Status field set to Disabled), configuration changes do not take effect until the Trunk Status field is set to Enabled.

3 Click **Submit**.

—End—

Configuring Spanning Tree Group Participation

After a multilink trunk has been established, MLT participation in a Spanning Tree Group can be configured. To configure STG participation, the MLT must have a Trunk Status of Enabled. Refer to "[Creating a multilink trunk](#)" (page 292) on page 109 for information about this process.

To configure Spanning Tree Group participation, follow this procedure:

Step Action

- 1 From the menu, select **Applications > MultiLink Trunk > Group**. The Multilink Trunk Group page appears ("[MLT Group page](#)" (page 293)).
- 2 Click the button in the **STP** column for the row that represents the multilink trunk that is to be configured.
The MultiLink Trunk Spanning Tree Settings page appears ("[MultiLink Trunk Spanning Tree Settings page](#)" (page 295)).

MultiLink Trunk Spanning Tree Settings page



- 3 Set the **STP Learning** list to reflect the desired learning mode. The three options available are:
 - **Normal** -- Sets the learning mode to normal.
 - **Fast** -- Sets the learning mode to fast.
 - **Disable** -- Disables learning.
- 4 Click **Submit**.

—End—

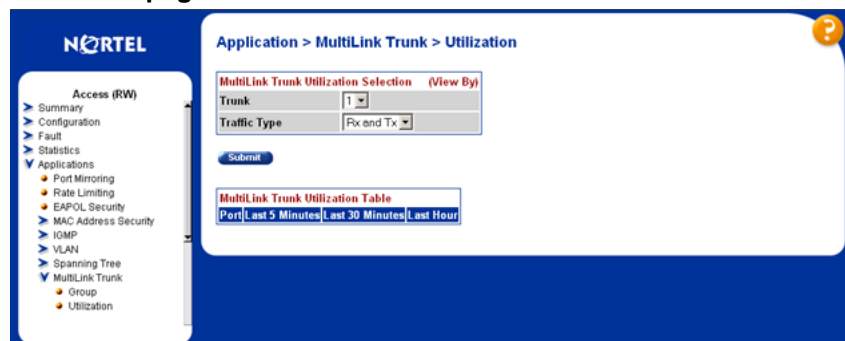
Monitoring an MLT

To monitor the bandwidth usage of the MLT, follow these steps:

Step Action

- 1 From the menu, select **Applications > MultiLink Trunk > Utilization**. The **Utilization** page appears ("[Utilization page](#)" (page 296)).

Utilization page



- 2 In the **MultiLink Trunk Utilization Selection** section, select the trunk to be monitored in the **Trunk** list and the type of traffic to be monitored in the **Traffic Type** list.
- 3 Click **Submit**.

—End—

MLT utilization statistics are displayed in the MultiLink Trunk Utilization Table section.

Creating and Managing MLTs using the Java Device Manager

The Java Device Manager (JDM) screens detailed in the following sections allow for the creation and management of multilink trunks:

- "Setting up MLTs" (page 296)
- "Adding MLT Ports" (page 300)

Setting up MLTs

To create an MLT, follow this procedure:

- | Step | Action |
|------|---|
| 1 | From the Device Manager menu bar, choose VLAN > MLT/LACP .
The MLT_LACP dialog box appears with the LACP Global tab displayed. |
| 2 | Click MultiLink Trunks . The MultiLink Trunks tab appears. |

Id	PortType	Name	PortMembers	VlanIds	Loadbalance(Mode)	Enable	MltType	RunningType	SmltId
1	access	Trunk #1			basic	false	normalMLT	normalMLT	0
2	access	Trunk #2	1/5-1/6	1	basic	true	normalMLT	normalMLT	0
3	access	Trunk #3			basic	false	normalMLT	normalMLT	0
4	access	Trunk #4			basic	false	normalMLT	normalMLT	0
5	access	Trunk #5			basic	false	normalMLT	normalMLT	0
6	access	Trunk #6			basic	false	normalMLT	normalMLT	0
7	access	Trunk #7			basic	false	normalMLT	normalMLT	0
8	access	Trunk #8			basic	false	normalMLT	normalMLT	0
9	access	Trunk #9			basic	false	normalMLT	normalMLT	0
10	access	Trunk #10			basic	false	normalMLT	normalMLT	0
11	access	Trunk #11			basic	false	normalMLT	normalMLT	0
12	access	Trunk #12			basic	false	normalMLT	normalMLT	0
13	access	Trunk #13			basic	false	normalMLT	normalMLT	0
14	access	Trunk #14			basic	false	normalMLT	normalMLT	0
15	access	Trunk #15			basic	false	normalMLT	normalMLT	0
16	access	Trunk #16			basic	false	normalMLT	normalMLT	0
17	access	Trunk #17			basic	false	normalMLT	normalMLT	0
18	access	Trunk #18			basic	false	normalMLT	normalMLT	0
19	access	Trunk #19			basic	false	normalMLT	normalMLT	0
20	access	Trunk #20			basic	false	normalMLT	normalMLT	0
21	access	Trunk #21			basic	false	normalMLT	normalMLT	0
22	access	Trunk #22			basic	false	normalMLT	normalMLT	0
23	access	Trunk #23			basic	false	normalMLT	normalMLT	0
24	access	Trunk #24			basic	false	normalMLT	normalMLT	0
25	access	Trunk #25			basic	false	normalMLT	normalMLT	0
26	access	Trunk #26			basic	false	normalMLT	normalMLT	0
27	access	Trunk #27			basic	false	normalMLT	normalMLT	0
28	access	Trunk #28			basic	false	normalMLT	normalMLT	0
29	access	Trunk #29			basic	false	normalMLT	normalMLT	0

- 3 In the fields provided on the **MultiLink Trunks** tab, enter the information necessary to complete the MLT. For a description of adding ports to the MLT (PortMembers field), see "Adding MLT Ports" (page 300). "MultiLink Trunks tab fields" (page 297) outlines the fields on this tab.

MultiLink Trunks tab fields

Field	Description
ID	The number of the MLT (assigned consecutively).
PortType	The port type: <ul style="list-style-type: none"> • Access • trunk • UntagPvidOnly • TagPvidOnly
Name	The name given to the MLT.
PortMembers	The ports that are assigned to the MLT.
VlanIds	Specifies the VLAN identifier.

Field	Description
Loadbalance(Mode)	Sets the MLT load balancing mode as either basic (MAC-based load balancing) or advanced (IP-based load balancing).
Enable	Specifies whether the multilink trunk is active.
MltType	Editable field that specifies the type of MLT: <ul style="list-style-type: none"> • normalMLT • istMLT • splitMLT
RunningType	Read-only field that displays the current MLT operational type: <ul style="list-style-type: none"> • normalMLT • istMLT • splitMLT
SmltId	The assigned SMLT ID. Both ends of the SMLT must have the same SMLT ID. The SmltId field is used when the MltType is splitMLT. The SmltId value should be 0 if the MltType is not splitMLT.

4 Click **Apply**.

—End—

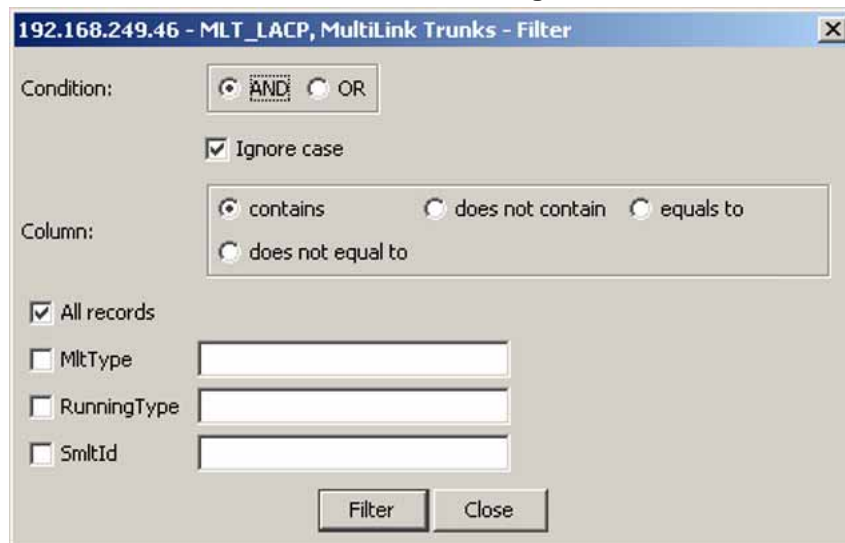
Filtering the MultiLink Trunks tab display

To filter the display of the MultiLink Trunks tab to display selected types of MLT.

Step Action

- 1 From the **MultiLink Trunks** tab, click **Filter**.
The MLT_LACP, MultiLink Trunks - Filter dialog box appears.

MLT_LACP, MultiLink Trunks - Filter dialog box



MLT_LACP, MultiLink Trunks - Filter dialog box fields

Field	Description
Condition	Select AND to include all entries in the table that include all specified parameters, or select OR to include any of the specified parameters.
Ignore case	Select Ignore case to include all entries with the parameters being set, whether in lowercase or uppercase.
Column	Select one of the following options <ul style="list-style-type: none"> • contains: shows entries that contain the parameters set • does not contain: shows entries that do not contain the parameters set • equals to: shows entries that are equal to the parameters set • does not equal to: shows entries that are not equal to the parameters set
All records	Select All records to display all the entries in the table.
MltType	To display the entries in the table by MLT type, select MltType and enter the MltType string to display.

Field	Description
RunningType	To display the entries in the table by MLT running type, select RunningType and enter the RunningType string to display.
Smltld	To display the entries in the table by Smltld type, select Smltld and enter the Smltld string to display.

- 2 Set the properties, and click **Filter**.

The MultiLink Trunks table displays information based on the specified criteria.

—End—

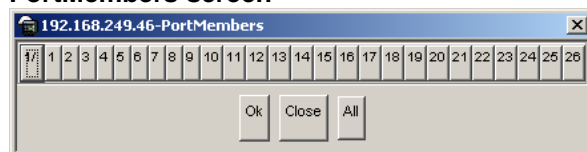
Adding MLT Ports

To add ports to an MLT, follow this procedure:

Step Action

- 1 From the Device Manager menu bar, choose **VLAN > MLT/LACP**. The MLT_LACP dialog box appears with the LACP Global tab displayed.
- 2 Click **MultiLink Trunks**.
The MultiLink Trunks tab appears.
- 3 Double-click in the **PortMembers** field for the MLT to which ports are to be added. The **PortMembers** screen appears. This screen is illustrated in "[PortMembers screen](#)" (page 300).

PortMembers screen



- 4 Click on the buttons that represent the ports that are to be added to the MLT. For the 5500 Series, up to 8 same-type ports can belong to a single MLT
- 5 Click **OK**.
- 6 Click **Apply**.

—End—

The selected ports are now displayed on the MLT_LACP dialog box in the PortMembers field.

Configuring SMLT using the CLI

To configure SMLT using the CLI, refer to the following:

- "interface mlt command" (page 301)
- "smlt command" (page 302)
- "ist command" (page 302)
- "smlt command " (page 303)
- "no smlt command" (page 303)
- "no ist command" (page 304)
- "no smlt command " (page 304)
- "default smlt command" (page 304)
- "default ist command" (page 304)
- "default smlt command " (page 305)
- "show ist command" (page 305)
- "show ist stat command" (page 305)
- "show smlt command" (page 306)

interface mlt command

ATTENTION

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

The `interface mlt` command sets the CLI command mode to MLT Interface mode from which you can configure SMLTs and ISTs.

The syntax for the `interface mlt` command is:

```
interface mlt [<1-32>]
```

where <1-32> specifies the ID of the MLT to configure.

The `interface mlt` command is in the config command mode.

Note: You create SLTs from the config-if command mode. For details, see "smlt command" (page 303).

smlt command

ATTENTION

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

The `smlt` command creates an SMLT from an existing MLT. The syntax for the `smlt` command is:

```
smlt <1-32>
```

where <1-32> specifies the ID of the SMLT to configure.

The `smlt` command is in the MLT Interface command mode.

Note: Before you can create an SMLT, you must first create and enable an MLT (see "mlt command" (page 290)).

ist command

ATTENTION

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

The `ist` command creates an IST from an existing MLT. The syntax for the `ist` command is:

```
ist [enable] [peer-ip <A.B.C.D>] [vlan <1-4096>]
```

The `ist` command is in the MLT Interface command mode.

The following table describes the parameters for this command.

ist parameters and variables

Parameter	Description
enable	Enables the IST on the MLT specified by the interface mlt command.

Parameter	Description
vlan <1-4096>	Specifies a VLAN ID for the IST.
peer-ip <A.B.C.D>	Specifies the peer IP address for the IST.

The peer IP address is the IP address of the IST VLAN on the peer aggregation switch. A VLAN created on the redundant aggregation switch must also be created on the second aggregation switch. The IST treats the two switches as a single switch. To allow the two switches to communicate, you must assign an IP address to both VLANs.

For example:

```

switch A                               switch B
VLAN 20                                 VLAN 20
10.1.1.1 /24                            10.1.1.2 /24 *
      <-----IST----->

```

* Same subnet, same VLAN.

smlt command

ATTENTION

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

The `smlt` command creates an SLT on a port. The syntax for the `smlt` command is:

```
smlt [port <portlist>] <1-512>
```

The `smlt` command is in the config-if command mode.

The following table describes the parameters for this command.

smlt port parameters and variables

Parameter	Description
port <portlist>	Specifies the port to configure as an SLT.
<1-512>	Specifies the ID for the SLT.

no smlt command

The `no smlt` command disables the SMLT. The syntax for the `no smlt` command is:

```
no smlt <1-32>
```

The `no smlt` command is in the MLT Interface command mode.

no ist command

The `no ist` command disables the IST and clears the IST settings. The syntax for the `no ist` command is:

```
no ist [enable] [peer-ip]
```

The `no ist` command is in the MLT Interface command mode.

The following table describes the parameters for this command.

no ist parameters and variables

Parameter	Description
enable	Disables the IST on the MLT specified by the interface <code>mlt</code> command.
vlan <1-4096>	Clears the VLAN ID from the IST.
peer-ip <A.B.C.D>	Clears the peer IP address from the IST.

no smlt command

The `no smlt` command disables the SLT on a port. The syntax for the `no smlt` command is:

```
no smlt [port <portlist>]
```

where <portlist> is the port or list of ports on which to disable the SLT.

The `no smlt` command is in the config-if command mode.

default smlt command

The `default smlt` command disables the SMLT. The syntax for the `default smlt` command is:

```
default smlt <1-32>
```

The `default smlt` command is in the MLT Interface command mode.

default ist command

The `default ist` command disables the IST and clears the IST settings. The syntax for the `default ist` command is:

```
default ist [enable] [peer-ip]
```

The `default ist` command is in the MLT Interface command mode.

The following table describes the parameters for this command.

default ist parameters and variables

Parameter	Description
enable	Disables the IST on the MLT specified by the interface mlt command.
peer-ip <A.B.C.D>	Clears the peer IP address from the IST.

default smlt command

The `default smlt` command disables the SLT on a port. The syntax for the `default smlt` command is:

```
default smlt [port <portlist>] <1-512>
```

where <portlist> is the port or list of ports on which to disable the SLT.

The `default smlt` command is in the config-if command mode.

show ist command

The `show ist` command displays the IST parameters on the switch. The syntax for the `show ist` command is:

```
show ist
```

The `show ist` command is in the exec command mode.

The following figure shows a sample output from the `show ist` command.

show ist command output

MLT ID	Enabled	Peer IP Address	Vlan ID
1	Yes	10.30.31.99	7

show ist stat command

The `show ist stat` command displays the IST statistics on the switch. The syntax for the `show ist stat` command is:

```
show ist stat
```

The `show ist stat` command is in the exec command mode.

The following figure shows a sample output from the `show ist stat` command.

show ist stat command output

```

5530-24TFD>show ist stat
-----
IST Statistics (RX      TX)
-----
SessionDown:      0
UnknownMsgType:  0
Hello:            0      0
LearnMac:         0      0
MacAgeOut:        0      0
MacAgeExp:        0      0
StgInfo:          0      0
DelMac:           0      0
SmltDown:         0      0
SmltUp:           0      0
MacTbl:           0      0
IcmpInfo:         0      0
PortDown:         0      0
ReqMacTbl:        0      0
IpRsmлтMsg:       0      0
IpxRsmлтMsg:      0      0
LacpInfo:         0      0

```

show smlt command

The **show smlt** command displays the SMLT and SLT configurations on the switch. The syntax for the **show smlt** command is:

```
show smlt [<interface-type>]
```

The **show smlt** command is in the MLT Interface command mode.

The following table describes the parameters for this command.

show smlt port parameters and variables

Parameter	Description
<interface-type>	Interface types are <ul style="list-style-type: none"> mlt: Displays only the MLT-based SMLTs mlt id <1-32> fastethernet: Displays only the SLTs slt-id <1-512>

The following figure shows a sample output from the **show smlt** command.

show smlt command output

```

5530-24TFD>show smlt
=====
MLT SMLT Info
=====
MLT ID      SMLT ID      ADMIN TYPE      CURRENT TYPE
-----
1          1            smlt          norm
9          9            ist          norm
=====
SLT Info
=====
PORT NUM    SMLT ID      ADMIN TYPE      CURRENT TYPE
-----
14         14           slt           norm
23         21           slt           norm
24         45           slt           norm
5530-24TFD>

```

Configuring an SMLT using Device Manager

This section describes how to use Device Manager (DM) to configure Split MultiLink Trunking (SMLT) and includes the following topics:

- ["Adding an MLT-based SMLT" \(page 307\)](#)
- ["Viewing SLTs configured on your switch" \(page 308\)](#)
- ["Configuring an IST MLT" \(page 309\)](#)
- ["Removing an IST MLT" \(page 311\)](#)
- ["Viewing IST statistics" \(page 311\)](#)
- ["Configuring an SLT" \(page 313\)](#)
- ["Deleting an SLT" \(page 315\)](#)
- ["Troubleshooting IST problems" \(page 316\)](#)

Adding an MLT-based SMLT**ATTENTION**

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

You can create an SMLT from the **Multilink Trunks** tab by selecting the MLT type as SMLT and then specifying an SMLT ID.

To add an MLT-based SMLT:

Step Action

- 1 From the Device Manager menu bar, choose **VLAN > MLT/LACP**.

- The MLT_LACP dialog box appears with the LACP Global tab displayed.
- 2 Select the **Multilink Trunks** tab.
The Multilink Trunks tab appears.
 - 3 From the displayed list of MLTs, choose an available MLT to configure as an SMLT.
 - 4 In the row containing the desired MLT, double-click the **PortMembers** field.
The PortMembers dialog box appears, displaying the available ports.
 - 5 Click the ports to include in the MLT-based SMLT.
For the 5500 Series, up to eight same-type ports can belong to a single MLT.
 - 6 Click **OK**.
The MltPortMembers dialog box closes, and the ports are added to the PortMembers field.
 - 7 Double-click the **MltType** field and choose **splitMLT** from the list.
 - 8 In the **SmltId** field, type an unused SMLT ID (1 - 32).
Note: The corresponding SMLTs between aggregation switches must have matching SMLT IDs. The same ID number must be used on both sides.
 - 9 Click **Apply**.

—End—

Viewing SLTs configured on your switch

To view the SLTs configured on your switch:

- | Step | Action |
|------|---|
| 1 | From the Device Manager menu bar, choose VLAN > MLT/LACP .
The MLT_LACP dialog box appears with the LACP Global tab displayed. |
| 2 | Select the Single Port SMLT tab.
The Single Port SMLT tab appears. |

—End—

Single Port SMLT tab**Single Port SMLT tab fields**

Field	Description
Port	Read only field that displays the port index number.
SmltId	The ID number of the SLT (1 - 512).
OperType	Read only field that displays the current port operational type: <ul style="list-style-type: none"> normal smlt (single port Split MLT)

Configuring an IST MLT**ATTENTION**

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

To configure an IST MLT:

Step Action

- From the Device Manager menu bar, choose **VLAN > MLT/LACP**.
The MLT_LACP dialog box appears with the LACP Global tab displayed.
- Select the **Multilink Trunks** tab.
The Multilink Trunks tab appears.
- In the row containing the desired MLT, double-click the **PortMembers** field.

The PortMembers dialog box appears, displaying the available ports.

- 4 Select the ports to include in the MLT and click **OK**.

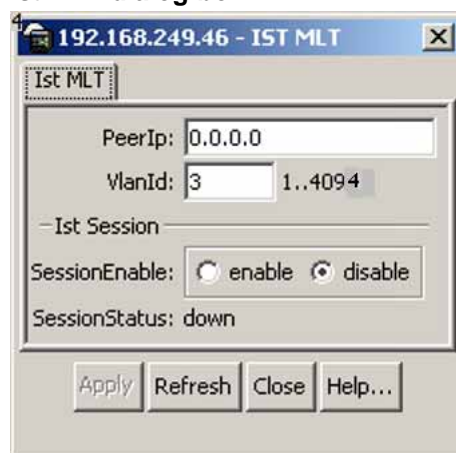
For the 5500 Series, up to eight same-type ports can belong to a single MLT.

The MltPortMembers dialog box closes, and the ports are added to the PortMembers field.

- 5 Double-click the **Enable** field and choose **true**.
- 6 Double-click the **MltType** field and choose **istMLT** from the list.
- 7 Click **Apply**.
- 8 Select any field in the IST MLT row and click the **istMlt** button.

The **ist MLT** dialog box ("Ist MLT dialog box" (page 310)) appears. For field definitions, see "IST MLT fields" (page 311).

Ist MLT dialog box



- 9 In the **PeerIp** field, enter a peer IP address.
- 10 In the **VlanId** field, enter a VLAN ID.
- 11 In the **SessionEnable** field, click **enable**.
- 12 Click **Apply**.

The IST MLT dialog box closes, and the changes are applied. The IST MLT is now configured.

—End—

IST MLT fields

Field	Description
PeerI	IST MLT peer IP address.
VlanId	An IST VLAN ID number from 1 to 4095.
SessionEnable	Enable/disable IST functionality.
Session Status	Read only: up or down

Removing an IST MLT

To remove an existing IST MLT from your switch:

Step	Action
1	From the Multilink Trunks tab, change the MltType field for the IST from istMLT to normalMLT .
2	Click Apply .

—End—

Viewing IST statistics

To view IST statistics on an interface:

Step	Action
1	From the Device Manager menu bar, choose VLAN > MLT/LACP . The MLT_LACP dialog box appears with the LACP Global tab displayed.
2	Click the Ist/SMLT Stats tab. The IST protocol packet statistics are displayed (" Ist/SMLT Stats tab " (page 312)).

Ist/SMLT Stats tab

	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
SmltIstDownCnt	0	0	0	0	0	0
SmltHelloTxMsgCnt	0	0	0	0	0	0
SmltHelloRxMsgCnt	0	0	0	0	0	0
SmltLearnMacAddrTxMsgCnt	0	0	0	0	0	0
SmltLearnMacAddrRxMsgCnt	0	0	0	0	0	0
SmltMacAddrAgeOutTxMsgCnt	0	0	0	0	0	0
SmltMacAddrAgeOutRxMsgCnt	0	0	0	0	0	0
SmltMacAddrAgeExpTxMsgCnt	0	0	0	0	0	0
SmltMacAddrAgeExpRxMsgCnt	0	0	0	0	0	0
SmltStgInfoTxMsgCnt	0	0	0	0	0	0
SmltStgInfoRxMsgCnt	0	0	0	0	0	0
SmltDelMacAddrTxMsgCnt	0	0	0	0	0	0
SmltDelMacAddrRxMsgCnt	0	0	0	0	0	0
SmltSmltDownTxMsgCnt	0	0	0	0	0	0
SmltSmltDownRxMsgCnt	0	0	0	0	0	0
SmltSmltUpTxMsgCnt	0	0	0	0	0	0
SmltSmltUpRxMsgCnt	0	0	0	0	0	0
SmltSendMacTbITxMsgCnt	0	0	0	0	0	0
SmltSendMacTbIRxMsgCnt	0	0	0	0	0	0
SmltIcmpTxMsgCnt	0	0	0	0	0	0
SmltIcmpRxMsgCnt	0	0	0	0	0	0
SmltPortDownTxMsgCnt	0	0	0	0	0	0
SmltPortDownRxMsgCnt	0	0	0	0	0	0
SmltReqMacTbITxMsgCnt	0	0	0	0	0	0
SmltReqMacTbIRxMsgCnt	0	0	0	0	0	0
SmltRxUnknownMsgTypeCnt	0	0	0	0	0	0

—End—

Ist/SMLT Stats tab fields

Field	Description
SmltIstDownCnt	The number of IST down messages.
SmltHelloTxMsgCnt	The number of hello messages transmitted.
SmltHelloRxMsgCnt	The number of hello messages received.
SmltLearnMacAddrTxMsgCnt	The number of learn MAC address messages transmitted.
SmltLearnMacAddrRxMsgCnt	The number of learn MAC address messages received.
SmltMacAddrAgeOutTxMsgCnt	The number of MAC address aging out messages transmitted.
SmltMacAddrAgeOutRxMsgCnt	The number of MAC address aging out messages received.
SmltMacAddrAgeExpTxMsgCnt	The number of MAC address age expired messages transmitted.

Field	Description
SmltMacAddrAgeExpRxMsgCnt	The number of MAC address age expired messages received.
SmltStgInfoTxMsgCnt	The number of SMLT STG info messages transmitted.
SmltStgInfoRxMsgCnt	The number of SMLT STG info messages received.
SmltDelMacAddrTxMsgCnt	The number of deleted MAC address messages transmitted.
SmltDelMacAddrRxMsgCnt	The number of deleted MAC address messages received.
SmltSmltDownTxMsgCnt	The number of SMLT down messages transmitted.
SmltSmltDownRxMsgCnt	The number of SMLT down messages received.
SmltSmltUpTxMsgCnt	The number of SMLT up messages transmitted.
SmltSmltUpRxMsgCnt	The number of SMLT up messages received.
SmltSendMacTblTxMsgCnt	The number of send MAC table messages transmitted.
SmltSendMacTblRxMsgCnt	The number of send MAC table messages received.
SmltIcmpTxMsgCnt	The number of IGMP messages transmitted.
SmltIcmpRxMsgCnt	The number of IGMP messages received.
SmltPortDownTxMsgCnt	The number of port down messages transmitted.
SmltPortDownRxMsgCnt	The number of port down messages received.
SmltReqMacTblTxMsgCnt	The number of request MAC table messages transmitted.
SmltReqMacTblRxMsgCnt	The number of request MAC table messages received.
SmltRxUnknownMsgTypeCnt	The number unknown SMLT messages received.

Configuring an SLT

ATTENTION

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

Ports that are already configured as MLT or MLT-based SMLT cannot be configured as a single port SLT. You must first remove the split trunk and then reconfigure the ports as an SLT.

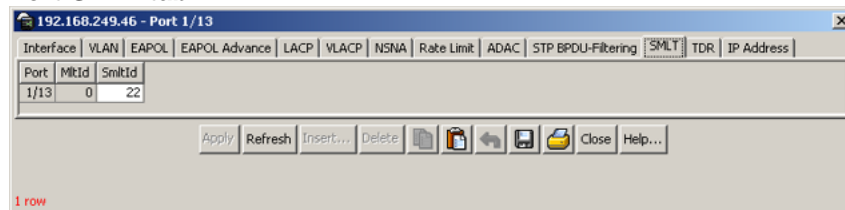
To configure an SLT:

Step	Action
------	--------

- From the Device Manager main window, select the port.
The port is highlighted.
- From the menu bar, choose **Edit > Port**.
The Port dialog box appears with the Interface tab displayed.
- Click the **SMLT** tab.
The port SMLT tab ("Port SMLT tab" (page 314)) appears.

Note: If the MltId field is not zero, this indicates that the port is already configured as an MLT or MLT-based SMLT. If so, you cannot configure an SLT on the port.

Port SMLT tab



- Click **Insert**.
The Insert SMLT dialog box ("Port, Insert SMLT dialog box" (page 314)) appears.

Port, Insert SMLT dialog box



- In the **SmltId** field, enter an unused SMLT ID number from 1 to 512.
To view the SMLT IDs that are already in use on your switch, see "Viewing SLTs configured on your switch" (page 308).
- Click **Insert**.

The Insert SMLT dialog box closes, and the ID is entered into the SMLT tab.

—End—

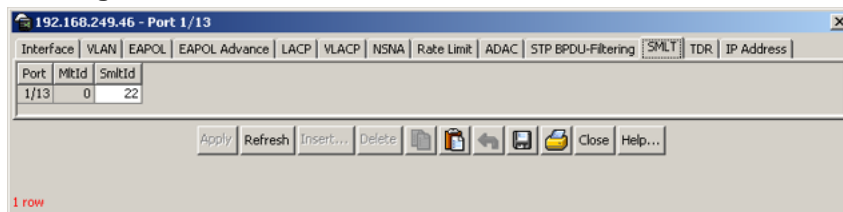
Port SMLT tab fields

Field	Description
Port	The slot/port number for the port.
Mitld	<p>Read only field, displaying one of the following:</p> <ul style="list-style-type: none"> • A value of 1 - 32 indicates that the port is part of an MLT and that, as a result, SLT cannot be configured on this port. • A value of 0 indicates that no MLT is assigned, and the port can be configured for SLT.
Smltld	<p>The Split MLT ID, an integer from 1 to 512.</p> <ul style="list-style-type: none"> • A read-only field with a value of 1-512 indicates the SLT ID assignment for the port. • Find an unused SMLT ID by viewing the currently-used IDs.

Deleting an SLT

To delete an SLT:

Step	Action
1	<p>From the Device Manager main window, select the port. The port is highlighted.</p>
2	<p>From the menu bar, choose Edit > Port. The Port dialog box appears with the Interface tab displayed.</p>
3	<p>Click the SMLT tab. The port SMLT tab ("Deleting an SLT" (page 316)) appears, displaying the SLT ID.</p>

Deleting an SLT

- 4 Select the Port SLT.
 - 5 Click **Delete**.
 - 6 Click **Close**.
- The SLT configured for this port is deleted.

—End—

Troubleshooting IST problems

This section provides procedures for troubleshooting IST problems and single-user problems.

Troubleshooting IST problems

To troubleshoot SMLT IST problems:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Ensure that Global IP Routing is enabled. |
| 2 | Ensure that peers can ping each other. |
| 3 | Enter the <code>show ist stat</code> command to display the IST message count.

The hello count should increment. |
| 4 | Enter the <code>show mltr</code> command to display all the MLTs in the switch and their properties, including running type, members, and status. Check the SMLT/SLT numbering: switches connected by SMLT must have the same SMLT IDs. |
| 5 | Ensure that the IST is up and running by using the <code>show ist</code> command. |
| 6 | If the IST is not running, ensure that: <ol style="list-style-type: none"> a. The correct VLAN ID exists on both sides of the IST |

- b. The IST configuration contains the correct local and peer IP addresses
- 7 If IST is running, check whether the SMLT port is operating by using the `show smlt info` command.
- a. If the current type is SMLT, the status is correct.
 - b. If the current type is NORMAL, the link is running in a normal (single) mode and not in SMLT mode. The reasons for this can be as follows:
 - The remote SMLT link is not operational.
 - The ID is not configured on the other switch. To determine this, check to see whether the SMLT IDs match.
 - The IST is not up and running.

—End—

Configuring LACP and VLACP

Link Aggregation (LA) provides a new mechanism for creating and managing trunk groups. Trunk group can be controlled and configured automatically with the help of LACP. Trunk groups that are based on the Link Aggregation Control Protocol (LACP) are referred to as Link Aggregation Groups.

LACP, defined by the IEEE 802.3ad standard, enables a switch to learn the presence and capabilities of a remote switch by exchanging information with the remote switch before the formation of a trunk group. Either switch can accept or reject the aggregation request with the far end on a per port basis. A link that cannot join a trunk group operates as an individual link.

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

LACP and VLACP can be configured and managed using the Command Line Interface (CLI) or Java Device Manager (JDM). The Web-based Management Interface also supports LACP, but not VLACP.

This chapter contains information on the following topics:

- ["Configuring LACP and VLACP using the CLI" \(page 319\)](#)
- ["Configuring LACP and VLACP using Device Manager" \(page 331\)](#)
- ["Configuring LACP using Web-based management" \(page 338\)](#)

Configuring LACP and VLACP using the CLI

This section contains information on the following topics:

- ["Configuring Link Aggregation using the CLI" \(page 319\)](#)
- ["Configuring VLACP using the CLI" \(page 325\)](#)

Configuring Link Aggregation using the CLI

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

To configure Link Aggregation using the CLI, refer to the following:

- "show lacp system command" (page 320)
- "show lacp port command" (page 320)
- "show lacp port-mode command" (page 321)
- "show lacp stats command" (page 321)
- "lacp clear-stats command" (page 321)
- "show lacp debug member command" (page 322)
- "show lacp aggr command" (page 322)
- "lacp system-priority command" (page 322)
- "lacp aggregation command" (page 323)
- "no lacp aggregation command" (page 323)
- "lacp key command" (page 323)
- "lacp mode command" (page 323)
- "lacp priority command" (page 324)
- "lacp timeout-time command" (page 325)
- "lacp port-mode command" (page 325)

show lacp system command

The `show lacp system` command displays system-wide LACP settings.

The syntax for the `show lacp system` command is:

```
show lacp system
```

The `show lacp system` command is executed in the Privileged EXEC command mode.

show lacp port command

The `show lacp port` command displays information on the per-port LACP configuration. Select ports either by port number or by aggregator value.

The syntax for the `show lacp port` command is:

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

The `show lacp port` command is executed in the Privileged EXEC command mode.

" [show lacp port parameters](#)" (page 321) describes the parameters for the `show lacp port` command.

show lacp port parameters

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

show lacp port-mode command

The `show lacp port-mode` command displays the current port mode (default or advanced).

The syntax for `show lacp port-mode` command is:

```
show lacp port-mode
```

The `show lacp port-mode` command is executed in the Privileged EXEC command mode.

show lacp stats command

The `show lacp stats` command displays LACP port statistics. Select ports either by port number or by aggregator value.

The syntax for the `show lacp stats` command is:

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

The `show lacp stats` command is executed in the Privileged EXEC command mode.

"[show lacp stats parameters](#)" (page 321) describes the parameters for the `show lacp stats` command.

show lacp stats parameters

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

lacp clear-stats command

The `lacp clear-stats` command clears the existing LACP port statistics.

The syntax for the `lacp clear-stats` command is:

```
lACP clear-stats <portList>
```

The `lACP clear-stats` command is executed in the Interface Configuration command mode.

show lACP debug member command

The `show lACP debug member` command displays the port debug information.

The syntax for the `show lACP debug member` command is:

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

Substitute `<portList>` with the ports for which to display debug information.

The `show lACP debug member` command is executed in the Privileged EXEC command mode.

show lACP aggr command

The `show lACP aggr` command displays LACP aggregators or LACP trunks.

The syntax for the `show lACP aggr` command is:

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

Substitute `<1-65535>` with the number of the LACP aggregator for which to display information.

The `show lACP aggr` command is executed in the Privileged EXEC command mode.

lACP system-priority command

The `lACP system-priority` command configures the LACP system priority. It is used to set the system-wide LACP priority. The factory default priority value is 32768.

The syntax for the `lACP system-priority` command is:

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

Substitute `<0-65535>` with the priority value to assign to LACP.

The `lACP system-priority` command is executed in the Global Configuration command mode.

lacp aggregation command

The `lacp aggregation` command enables the port aggregation mode. The syntax for the `lacp aggregation` command is:

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

Substitute `<portList>` with the ports to enable link aggregation on.

This command is executed in the Interface Configuration command mode.

no lacp aggregation command

The `no lacp aggregation` command disables the port aggregation mode.

The syntax for the `no lacp aggregation` command is:

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

Substitute `<portList>` with the ports on which to disable port aggregation.

The `no lacp aggregation` command is executed in the Interface Configuration mode.

lacp key command

The `lacp key` command configures the administrative LACP key for a set of ports.

The syntax for the `lacp key` command is:

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

"[lacp key parameters](#)" (page 323) outlines the parameters for this command.

lacp key parameters

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

The `lacp key` command is executed in the Interface Configuration command mode.

lacp mode command

The `lacp mode` command configures the LACP mode of operations for a set of ports.

The syntax for the `lacp mode` command is:

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

"lacp mode parameters" (page 324) outlines the parameters for this command.

lacp mode parameters

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

The `lacp mode` command is executed in the Interface Configuration command mode.

lacp priority command

The `lacp priority` command configures the per-port LACP priority for a set of ports.

The syntax for the `lacp priority` command is:

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

"lacp priority parameters" (page 324) outlines the parameters for this command.

lacp priority parameters

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

The `lacp priority` command is executed in the Interface Configuration command mode.

lACP timeout-time command

The `lACP timeout-time` command configures the LACP periodic transmission timeout interval for a set of ports.

The syntax for the `lACP timeout-time` command is:

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

"[lACP timeout-time parameters](#)" (page 325) outlines the parameters for this command.

lACP timeout-time parameters

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

lACP port-mode command

The `lACP port-mode` command configures the LACP port mode on the switch.

The syntax for the `lACP port-mode` command is:

```
lACP port-mode {default | advance}
```

The `lACP port-mode` command is in the config command mode.

The following table outlines the parameters for this command.

lACP port-mode parameters

Parameter	Description
default	Default LACP port mode.
advance	Advanced LACP port mode.

Configuring VLACP using the CLI

To configure VLACP using the CLI, refer to the following commands:

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

- "[vlACP enable command](#)" (page 326)
- "[vlACP macaddress command](#)" (page 326)
- "[vlACP port command](#)" (page 326)
- "[no vlACP enable command](#)" (page 329)
- "[no vlACP macaddress command](#)" (page 329)

- "no vlacp port command" (page 329)
- "show vlacp command" (page 330)
- "show vlacp interface command" (page 330)

vlacp enable command

The `vlacp enable` command globally enables VLACP for the device.

The syntax for the `vlacp enable` command is:

```
vlacp enable
```

The `vlacp enable` command is in the config command mode.

The `vlacp enable` command has no parameters or variables.

vlacp macaddress command

The `vlacp macaddress` command sets the multicast MAC address used by the device for VLACPDUs.

The syntax for the `vlacp macaddress` command is:

```
vlacp macaddress <macaddress>
```

where `<macaddress>` is the specified MAC address.

The `vlacp macaddress` command is in the config command mode.

vlacp port command

The `vlacp port` configures VLACP parameters on a port. The syntax for the `vlacp port` command is:

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

The `vlacp port` command is in the config-if mode.

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

vlacp port command parameters

Parameters and variables	Description
<code><slot/port></code>	Specifies the slot and port number.

Parameters and variables	Description
<code>enable disable</code>	Enables or disables VLACP.
<code>timeout <long/short></code>	<p>Specifies whether the timeout control value for the port is a long or short timeout.</p> <ul style="list-style-type: none"> • <i>long</i> sets the port timeout value to: (timeout-scale value) × (slow-periodic-time value). • <i>short</i> sets the port's timeout value to: (timeout-scale value) × (fast-periodic-time value). <p>For example, if the timeout is set to short while the timeout-scale value is 3 and the fast-periodic-time value is 400 ms, the timer expires after 1200 ms.</p> <p>Default is long.</p>
<code>fast-periodic-time <integer></code>	<p>Specifies the number of milliseconds between periodic VLACPDU transmissions using short timeouts.</p> <p>The range is 400-20000 milliseconds. Default is 500.</p>
<code>slow-periodic-time <integer></code>	<p>Specifies the number of milliseconds between periodic VLACPDU transmissions using long timeouts.</p> <p>The range is 10000-30000 milliseconds. Default is 30000.</p>

Parameters and variables	Description
<code>timeout-scale <integer></code>	<p>Sets a timeout scale for the port, where $\text{timeout} = (\text{periodic time}) \times (\text{timeout scale})$.</p> <p>The range is 1-10. Default is 3.</p> <p>Note: 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.</p> <p>To prevent this scenario from happening, set the timeout-scale to a value larger than 1.</p>
<code>funcmac-addr <mac></code>	<p>Specifies the address of the far-end switch/stack configured to be the partner of this switch/stack. If none is configured, any VLACP-enabled switch communicating with the local switch through VLACP PDUs is considered to be the partner switch.</p> <p>Note: 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.</p> <p>The port-specific <code>funcmac-addr</code> parameter does not specify a multicast MAC address, but instead specifies the MAC address of the switch or stack to which this port is sending VLACPDUs.</p> <p>You are not always required to configure <code>funcmac-addr</code>. If not configured, the first VLACP-enabled switch that receives the PDUs from a unit assumes that it is the intended recipient and processes the PDUs accordingly.</p> <p>If you want an intermediate switch to drop VLACP packets, configure the <code>funcmac-addr</code> parameter to the</p>

Parameters and variables	Description
	desired destination MAC address. With <code>funcmac-addr</code> configured, the intermediate switches do not misinterpret the VLACP packets.
<code>ethertype <hex></code>	Sets the VLACP protocol identification for this port. Defines the ethertype value of the VLACP frame. The range is 8101-81FF. Default is 8103.

no vlacp enable command

The `no vlacp enable` command globally disables VLACP for the device.

The syntax for the `no vlacp enable` command is:

```
no vlacp enable
```

The `no vlacp enable` command is in the config command mode.

The `no vlacp enable` command has no parameters or variables.

no vlacp macaddress command

The `no vlacp macaddress` command resets the multicast MAC address used by the device for VLACPDUs to the default value (01:80:c2:00:11:00).

The syntax for the `no vlacp macaddress` command is:

```
no vlacp macaddress
```

The `no vlacp macaddress` command is in the config command mode.

The `no vlacp macaddress` command has no parameters or variables.

no vlacp port command

The `no vlacp port` command disables VLACP on the port.

The syntax for the `no vlacp port` command is:

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

The `no vlacp port` command is in the config command mode.

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

no vlacp port command parameters

Parameters and variables	Description
<code><slot/port></code>	Specifies the slot and port number.
<code>enable</code>	Disables VLACP on the specified port.
<code>funcmac-addr</code>	Sets the funcmac-addr parameter to the default value.

show vlacp command

The `show vlacp` command displays the status of VLACP on the switch. The syntax for the `show vlacp` command is:

```
show vlacp
```

The `show vlacp` command is in the `privExec` command mode.

show vlacp interface command

The `show vlacp interface` command displays the VLACP configuration details for a port or list of ports. The syntax for the `show vlacp interface` command is:

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

where `<slot/port>` specifies a port or list of ports.

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

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

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

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

The following figure shows a sample output from the `show vlacp interface` command.

show vlacp interface sample output

```

5530-24TFD(config)#show vlacp interface 4
=====
                        VLACP Information
=====
PORT ADMIN  OPER   HAVE  FAST  SLOW  TIMEOUT  TIMEOUT  ETH  MAC
  ENABLED ENABLED PARTNER TIME  TIME  TYPE    SCALE  TYPE ADDRESS
-----
0/ 4  false  false  no    500   30000  long    3    8103 00:00:00:00:00:00
5530-24TFD(config)#

```

Configuring LACP and VLACP using Device Manager

This section contains information on the following topics:

- "Configuring LACP using Device Manager" (page 331)
- "Configuring VLACP using Device Manager" (page 335)

Configuring LACP using Device Manager

You can configure LACP using the following Device Manager tabs:

- "LACP Global tab" (page 331)
- "LACP tab" (page 332)
- "LACP tab for ports" (page 334)

LACP Global tab

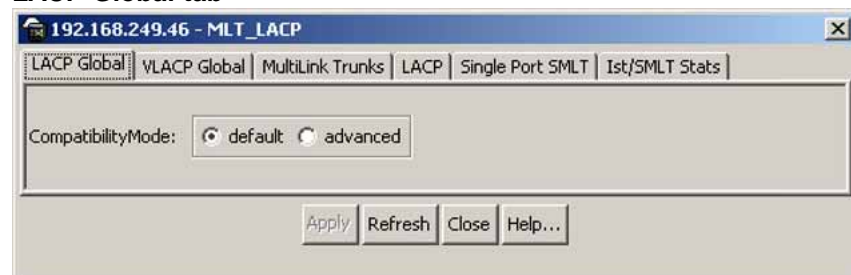
You can use the LACP Global tab to configure the LACP port compatibility mode.

To open the LACP Global tab:

Step	Action
------	--------

- | | |
|---|---|
| 1 | From the Device Manager menu bar, choose VLAN > MLT/LACP .
The MLT_LACP dialog box appears with the LACP Global tab displayed. |
|---|---|

LACP Global tab



LACP Global tab fields

Item	Description
CompatibilityMode	Specifies the port compatibility mode for LACP: <ul style="list-style-type: none"> • default • advanced

—End—

LACP tab

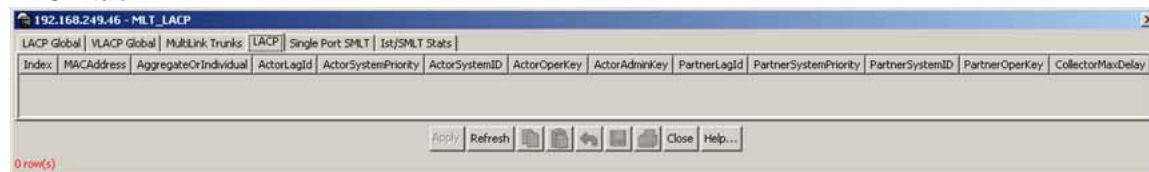
You can use the LACP tab to configure Link Aggregation Groups. To open the LACP tab:

Step	Action
------	--------

- | | |
|---|---|
| 1 | From the Device Manager menu, select VLAN > MLT/LACP .

The MLT_LACP dialog box appears with the LACP Global tab displayed. |
| 2 | Select the LACP tab.

The LACP tab appears. |

LACP tab**LACP tab fields**

Item	Description
Index	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	The MAC address used by this bridge when it must be referred to in a unique fashion.
AggregateOrIndividual	A read-only Boolean value indicating whether the Aggregation Port can Aggregate (TRUE) or can only operate as an Individual link (FALSE).

Item	Description
ActorLagID	The combined information of ActorSystemPriority, ActorSystemID, and ActorOperKey in ActorSystemPriority-ActorSystemID-ActorOperKey format.
ActorSystemPriority	A 2-octet read-write value indicating the priority value associated with the Actor's System ID.
ActorSystemID	A 6-octet read-only MAC address value that defines the value of the System ID for the System that contains this Aggregation Port.
ActorOperKey	The current operational value of the Key for the Aggregation Port. This is a 16-bit read-only value.
ActorAdminKey	The current administrative value of the Key for the Aggregation Port. This is a 16-bit read-write value.
PartnerLagID	The combined information of PartnerSystemPriority, PartnerSystemID, and PartnerOperKey in PartnerSystemPriority-PartnerSystemID-PartnerOper Key format.
PartnerSystemPriority	A 2-octet read-only value that indicates the priority value associated with the Partner's System ID.
PartnerSystemID	A 6-octet read-only MAC address value consisting of the unique identifier for the current protocol Partner of this Aggregator. A value of zero indicates that no known Partner exists. If the aggregation is manually configured, this System ID value is assigned by the local System.
PartnerOperKey	The current operational value of the Key for the Aggregator's current protocol Partner. This is a 16-bit read-only value.
CollectorMaxDelay	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.

—End—

LACP tab for ports

To view or edit the LACP tab for ports:

Step	Action
------	--------

- 1 Select the ports that you want to edit.
- 2 From the Device Manager main menu, choose **Edit > Port**.
The Port dialog box for multiple ports appears with the Interface tab displayed.
- 3 Click the **LACP** tab.
The LACP tab appears.

Port - LACP tab

Index	AdminEnabled	OperEnabled	AggregateOrIndividual	ActorSystemPriority	ActorSystemID	ActorAdminKey	ActorOperKey	SelectedAggID	AttachedAggID	ActorPort	ActorPortPriority
7(1/7)	false	false	Individual	32768	00:11:F9:35:...	1	0	0	0	7	32768
8(1/8)	false	false	Individual	32768	00:11:F9:35:...	1	0	0	0	8	32768

Port - LACP tab fields

Field	Description
Index	The ifIndex of the port
AdminEnabled*	The current administrative setting for the port. A value of true means the port is set to participate in LACP. A value of false means the port is set to not participate in LACP.
operEnabled	The current operational state for the port. A value of true means the port is participating in LACP. A value of false means the port is not participating in LACP.
AggregateOrIndividual	A read-only Boolean value indicating whether the Aggregator represents an Aggregate (true) or an Individual link (false).
ActorSystemPriority	A 2-octet read-write value used to define the priority value associated with the Actor's System ID.
ActorSystemID	A 6-octet read-only MAC address value that defines the value of the System ID for the system that contains this Port.
ActorAdminKey	The current administrative value of the Key for the Aggregation Port.

Field	Description
ActorOperKey	The current operational value of the Key for the Aggregation Port.
SelectedAgglID	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.
AttachedAgglID	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	The port number locally assigned to the Aggregation Port. The port number is communicated in LACPDUs as the Actor_Port. This value is read-only
ActorPortPriority	The priority value assigned to this Aggregation Port. This 16-bit value is read-write.
ActorAdminState*	A string of 8 bits, corresponding to the administrative values of Actor_State as transmitted by the Actor in LACPDUs.
ActorOperState	A string of 8 bits, corresponding to the current operational values of Actor_State as transmitted by the Actor in LACPDUs.
<p>*To set the LACP modes using JDM, you must ensure that the LACP port properties are set according to the desired mode, as follows:</p> <ul style="list-style-type: none"> • LACP mode Off = AdminEnabled field cleared (disabled) • LACP mode Passive = AdminEnabled field selected (enabled) • LACP mode Active = AdminEnabled field selected (enabled) and ActorAdminState options lacpActive and aggregation selected 	

—End—

Configuring VLACP using Device Manager

You can configure VLACP using the following Device Manager tabs:

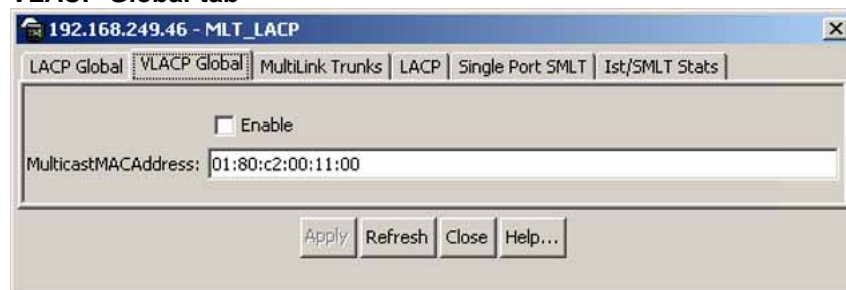
- "VLACP Global tab" (page 336)
- "VLACP tab for ports" (page 336)

VLACP Global tab

VLACP is an extension to LACP used to detect end-to-end failure. To view VLACP information for the switch:

- | Step | Action |
|------|---|
| 1 | From the Device Manager menu bar, choose VLAN > MLT/LACP .
The MLT_LACP dialog box appears with the LACP Global tab displayed. |
| 2 | Click VLACP Global .
The VLACP Global tab appears. |

—End—

VLACP Global tab**VLACP Global tab fields**

Field	Description
Enable	Enables or disables VLACP on the switch.
MulticastMACAddress	Identifies a multicast MAC address used exclusively for VLACPDUs. Default is 01:80:c2:00:11:00.

VLACP tab for ports

To view the VLACP tab for ports:

- | Step | Action |
|------|--|
| 1 | Select the ports you want to edit. |
| 2 | From the Device Manager main menu, choose Edit > Port .
The Port dialog box appears with the Interface tab displayed. |
| 3 | Click the VLACP tab.
The VLACP tab appears. |

VLACP tab

Index	AdminEnable	OperEnable	FastPeriodicTimer	SlowPeriodicTimer	Timeout	TimeoutScale	EtherType	EtherMacAddress	PortState
7(1/7)	false	false	500	30000	long	3	0x8103	00:00:00:00:00:...	down
8(1/8)	false	false	500	30000	long	3	0x8103	00:00:00:00:00:...	down

2 row(s)

VLACP tab fields

Item	Description
AdminEnable	Enables or disables VLACP on a port. The default value is False.
OperEnable	Indicates whether VLACP is operationally enabled or disabled. This is a read-only field.
FastPeriodicTimer	Specifies the number of milliseconds between periodic transmissions using short timeouts. Valid values range from 400-20000 with a default of 500.
SlowPeriodicTimer	Specifies the number of milliseconds between periodic transmissions using long timeouts. Valid values range from 10000-30000 with a default of 30000.
Timeout	Specifies whether the timeout control value is a short or long timeout.
TimeoutScale	<p>Sets a timeout scale for the port, where $\text{timeout} = (\text{periodic time}) * (\text{timeout scale})$.</p> <p>The range is 1-10. Default is 3.</p> <p>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.</p>

Item	Description
EtherType	Specifies VLACP protocol identification. The ID value is a 4-digit Hex number, with a default of 8103.
EtherMacAddress	<p>The default value is 00:00:00:00:00:00 and it can be configured with the MAC address of the switch or stack to which this port is sending VLACPDUs. It cannot be configured as a multicast MAC.</p> <p>Note: VLACP has only one multicast MAC address, configured using the MulticastMACAddress field in the VLACP Global tab, which is the Layer 2 destination address used for the VLACPDUs. The port-specific 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.</p> <p>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>
PortState	Identifies whether the VLACP port state is up or down. This is a read-only field.

—End—

Configuring LACP using Web-based management

To configure Link Aggregation using Web-based management, refer to the following sections

- ["Bridge Configuration page" \(page 339\)](#)
- ["Port Configuration page" \(page 339\)](#)

- "Port Statistics page" (page 340)

Bridge Configuration page

To configure LACP bridge properties:

Step	Action
------	--------

- | | |
|---|---|
| 1 | From the main menu, choose Application > Link Aggregation > Bridge Configuration . |
|---|---|

The LACP Bridge Configuration page appears.

LACP Bridge Configuration page items

Item	Description
System Priority	Set system priority to all the LACP enabled aggregators.
Collector max delay	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. This is a read-only value.

—End—

Port Configuration page

To configure LACP ports:

Step	Action
------	--------

- | | |
|---|---|
| 1 | From the main menu, choose Application > Link Aggregation > Port Configuration . |
|---|---|

The LACP Port Configuration page appears

LACP Port Configuration page

Application > LACP > Port Configuration

LACP - Port Setting

Port	Priority	LACP Mode	A/I	Timeout	Admin Key	Operational Key	Aggregator ID	Trunk ID	Partner Port	Status
1	32768	Off	I	Long	1	0	0			Down
2	32768	Off	I	Long	1	0	0			Down
3	32768	Off	I	Long	1	0	0			Up
4	32768	Off	I	Long	1	0	0			Down
5	32768	Off	I	Long	1	0	0			Down
6	32768	Off	I	Long	1	0	0			Down
7	32768	Passive	A	Long	1	16385	0			Down
8	32768	Passive	A	Long	1	16385	0			Down
9	32768	Off	I	Long	1	0	0			Down
10	32768	Off	I	Long	1	0	0			Down
11	32768	Active	I	Long	2	16386	0			Down
12	32768	Active	I	Long	2	16386	0			Down
Switch	32768	<input type="checkbox"/> Off	<input type="checkbox"/> I	<input type="checkbox"/> Long	<input type="checkbox"/> 1					

Submit

[Ports 13 - 24](#) [Ports 25 - 26](#)

LACP Port Configuration page items

Item	Description
Port	Lists each port on the unit.
Priority	Lists the priority number of each port.
LACP mode	Select to enable or disable the LACP mode.
A/I	A - shows that the port can be part of a LAG; I - shows that the port is an individual link.
Timeout	Select the timeout duration from the list.
Admin key	The admin value of the Key.
Oper key	The current operational value of the Key.
Aggr Id	The identifier value of the Aggregator that this Aggregation Port has currently selected.
Trunk Id	The ID of the LAG. The possible values are: 1 - 32.
Partner Port	The index of the port from the partner switch.
Status	Status of the selected port.

—End—

Port Statistics page

To view LACP port statistics

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the main menu, choose Application > Link Aggregation > Port Statistics . |
|---|--|

The LACP Port Statistics page appears

LACP Port Statistics page

LACP - Port Statistics								
Port	LACPDUs Rx	MarkerPDUs Rx	MarkerResponsePDUs Rx	UnknownPDUs Rx	IllegalPDUs Rx	LACPDUs Tx	MarkerPDUs Tx	MarkerResponsePDUs Tx
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	1	0	0
12	0	0	0	0	0	1	0	0

Ports 13 - 24 Ports 25 - 26

LACP Port Statistics page items

Field	Description
LACPDUsRx	Denotes the number of valid LACPDUs received on this Aggregation Port. This value is read-only.
MarkerPDUsRx	Signifies the number of valid Marker PDUs received on this Aggregation Port. This value is read-only.
MarkerResponsePDUsRx	The number of valid Marker Response PDUs received on this Aggregation Port. This value is read-only.
UnknownPDUsRx	Indicates the number of frames received that can <ul style="list-style-type: none"> Carry the Slow Protocols Ethernet Type value (43B.4), but contain an unknown PDU. Are addressed to the Slow Protocols group MAC Address (43B.3), but do not carry the Slow Protocols Ethernet Type. This value is read-only.

Field	Description
IllegalPDURx	Denotes the number of frames received that carry the Slow Protocols Ethernet Type value (43B.4), but contain a badly formed PDU or an illegal value of Protocol Subtype (43B.4). This value is read-only.
LACPDUsTx	Signifies the number of LACPDUs that are transmitted on this Aggregation Port. This value is read-only.
MarkerPDUsTx	Displays the number of Marker PDUs transmitted on this Aggregation Port. This value is read-only.
MarkerResponsePDUsTx	Indicates the number of Marker Response PDUs that are transmitted on this Aggregation Port. This value is read-only.

—End—

Index

Symbols/Numerics

802.1t path cost calculation 36

A

ActorAdminKey field 333
 ActorLagID field 333
 ActorOperKey field 333
 ActorSystemID field 333
 ADAC 93
 and stacking 104
 configuring using CLI 122
 configuring using Device Manager 171
 configuring using Web-based management 147
 initial user settings 98
 operating modes 99
 Tagged-Frames operating mode 102
 Untagged-Frames-Advanced operating mode 101
 Untagged-Frames-Basic Operating Mode 100
 User Restrictions 107
 ADAC and EAP 106
 adac command (global) 123
 adac command (per port) 125
 adac detection command 127
 adac port enable command 128
 Add VLAN Membership field 183, 202
 AdminEdgePort field 267
 AdminEdgeStatus field 278
 AdminP2P field 279
 AdminPathCost field 262
 AdminPointToPoint field 268

AggregateOrIndividual field 332
 Auto-Detection and Auto-Configuration of Nortel IP Phones 93

B

BPDU Filtering 40
 BrgAddress field 274
 Bridge Forward Delay field 189, 198, 207
 Bridge Forward Delay Time field 182, 193, 201
 Bridge Hello Time field 182, 188, 192, 197
 Bridge Hold Time field 206
 Bridge Max. Age Time field 182, 192, 201
 Bridge Maximum Age Time field 188, 197, 207
 Bridge Priority (in Hex) field 182, 192
 Bridge Priority field 187, 196, 200, 205
 Bridge Tx Hold Count 201
 Bridge Tx Hold Count field 193
 BridgeForwardDelay field 265, 275
 BridgeHelloTime field 265
 BridgeInstance field 285
 BridgeMaxAge field 265, 275
 BridgePriority field 275

C

CIST Root field 205
 clear mac-address-table 120
 clear mac-address-table address 121
 clear mac-address-table interface
 FastEthernet 120
 clear mac-address-table interface mlt 121
 clear mac-address-table interface vlan 120
 CollectorMaxDelay field 333

CompatibilityMode field 332
 ConfigDigest field 276
 ConfigIdSel field 276
 configuration
 SLT 305
 configuring SMLT
 config mlt ist, create ip vlan-id 303
 configuring SMLT using DM
 adding an SMLT 307
 configuring an IST MLT 310
 viewing IST statistics 311
 configuring SMLT with Device Manager 307
 Create STP Group field 181, 200
 CurrentPortRole field 279, 286

D

default adac command 124
 default adac command (per port) 126
 default adac detection command 128
 default adac port enable command 129
 default ist command 304
 default mac-address-table aging-time 120
 Default Path Cost Type 201
 Default Path Cost Type field 193, 198, 207
 default smlt command 304
 DefaultVLANId field 162
 Delete STP Group field 181, 200
 Delete VLAN Membership field 183, 202
 deleting NSNA VLAN 168
 Designated Root field 187, 196
 DesignatedBridge field 262, 268, 278, 286
 DesignatedCost field 262, 268, 278, 286
 DesignatedPort field 262, 268, 278, 286
 DesignatedRoot field 262, 265, 268, 278, 286
 Display Spanning Tree Switch Settings
 option 180, 191, 199
 Display Spanning Tree VLAN Membership
 option 180

E

EAP and ADAC 106
 Edge field 194, 203
 EffectivePortState field 270, 279, 286
 Enable Stp field 262
 Enabled field 282

F

FastStart field 262
 filtering NSNA VLAN 169
 FilterTaggedFrames field 162
 ForcePortState field 279, 286
 ForceProtocolVersion field 274
 Forward Delay field 188, 197, 206
 ForwardDelay field 266, 276
 ForwardTransitions field 262, 268, 280, 287

H

Hello Time field 187, 196
 HelloTime field 279
 HelloTime time 266
 HoldTime field 275
 Hop Count field 207

I

IllegalPDUsRx field 342
 Index field 332
 Instance field 281
 InstanceDownCount field 282
 InstanceUpCount field 282
 Inter-switch trunk (IST)
 about 68
 configure (CLI) 302
 configure (DM) 310
 disable (CLI) 304, 304
 show (CLI) 305
 show statistics(CLI) 305
 InvalidBPDUsRcvd field 287
 InvalidConfigBpduRxCount field 281
 InvalidMstBpduRxCount field 281
 InvalidRstBpduRxCount field 281
 InvalidTcnBpduRxCount field 281
 IP directed broadcasting
 configuring with CLI 121
 IST
 about 68
 aggregation switch processes 68
 configure (CLI) 302
 configure (DM) 310
 disable (CLI) 304, 304
 show (CLI) 305
 show statistics (CLI) 305

single point of failure 68
 ist command 302
 Ist MLT dialog box 310
 Ist/SMLT tab 312

L

LACP
 Bridge Configuration page 339
 configuring 319
 configuring with Device Manager 331
 configuring with the CLI 319
 configuring with Web-based management 338
 Port Configuration page 339, 341
 port mode 88
 LACPDUstx field 341
 LACPDUstx field 342
 Learning field 194, 203
 Link aggregation 86

M

MAC address
 flush 170
 MAC address forwarding database table
 configuring with CLI 117
 mac-address-table aging-time
 command 119
 MacAddress field 332
 MarkerPDUsRx field 341
 MarkerPDUsTx field 342
 MarkerResponsePDUsRx field 341
 MarkerResponsePDUsTx field 342
 Max. Hop Count 201
 MaxAge field 265, 276
 MaxHopCount field 274
 Maximum Age Time field 188, 197, 206
 MLT 41
 configuration rules 43
 MLT and STP 47
 MLT load-balancing 44
 MLT restrictions removal 45
 MLTs
 configuring with Device Manager 296
 configuring with the CLI 290
 configuring with Web-based management 292

MSTP 36
 CIST Bridge Configuration page 244
 Cist Port Configuration page 248
 configuring using CLI 221
 configuring with Device Manager 271
 Msti Bridge Configuration page 242, 243
 MSTP mode
 Display Spanning Tree Switch Settings
 option 199
 Spanning Tree Port Configuration
 option 199, 199
 MstpDownCount field 274
 MstpUpCount field 274
 multinetting 32
 Multiple Spanning Tree Protocol 36
 MuliLink Trunking 289
 Mutlilink trunks 41

N

NewRootBridgeCount field 276
 NewRootCount field 282
 NewRootldCount field 266
 no adac command (global) 124
 no adac command (per port) 126
 no adac detection command 127
 no adac port enable command 128
 no ist command 304
 no smlt command 304
 NoOfInstancesSupported field 274
 NSNA per VLAN 166
 NSNA VLAN delete 168
 NSNA VLAN filtering 169

O

OperEdgePort field 267
 OperEdgeStatus field 278
 OperP2P field 279
 OperPointToPoint field 268
 OperVersion field 270, 279
 options
 Display Spanning Tree Switch
 Settings 199
 Spanning Tree Group Configuration 199
 Spanning Tree Port Configuration 199

P

Participating field 268
 Participation field 185
 PartnerLagID field 333
 PartnerOperKey field 333
 PartnerSystemID field 333
 PartnerSystemPriority field 333
 Path Cost field 185, 195, 204
 PathCost field 262, 267, 277, 286
 PathCostDefault 264
 PathCostDefaultType field 274
 Port field 184, 194, 203, 267, 269, 277, 285
 Port Spanning Tree window 261
 Priority field 185, 194, 204, 262, 265, 267, 277, 282, 286
 ProtocolMigration field 267, 278
 ProtocolMigrationCount field 281

R

Rapid Spanning Tree Protocol 36
 ReceivedBPDUs field 287
 Region Name field 208
 Regional Root field 205
 Regional Root Path Cost 206
 RegionalPathCost field 278
 RegionalRoot field 275, 278, 282
 RegionalRootCost field 275
 RegionConfigChangeCount field 276
 RegionName field 276
 RegionVersion field 276
 Role field 195, 204, 269
 Root field 275
 Root Path Cost field 187, 196, 206
 Root Port field 187, 196, 206
 RootCost field 265, 275, 282
 RootPort field 265, 275, 282
 RSTP 36
 Bridge Configuration page 238
 configuring using CLI 218
 configuring with Device Manager 263
 configuring with Web-based management 238
 Port Configuration page 240
 RSTP mode
 Display Spanning Tree Switch Settings 191

Spanning Tree Group Configuration 191
 Spanning Tree Port Configuration 191
 RstpDownCount field 266
 RstpUpCount field 266
 RxConfigBpduCount field 280
 RxMstBpduCount field 280
 RxRstBpduCount field 280
 RxTcnBpduCount field 280

S

secondary IP interfaces 32
 SelectedPortRole field 279
 setting the STP mode with Device Manager 252
 show adac command 130
 show adac interface command 130
 show ist command 305
 show ist stat command 305
 show mac-address-table command 118
 show smlt command 306
 SLT
 about 70, 70
 configuring with Device Manager 313
 create (CLI) 304
 delete (DM) 315
 SMLT 50
 advantages 51, 51, 51
 configuration example 67
 configuring with the CLI 301
 end station configuration example 69
 IST 68
 single port
 create (CLI) 304
 delete (DM) 315
 square configuration 57
 stack configuration 66
 STP convergence resolution 51
 traffic flow examples 69
 triangle configuration 52
 troubleshooting
 IST problems 316
 smlt command 302
 SMLT configuration steps 73
 Snoop tab 162
 Spanning Tree Configuration Menu
 screen 180, 190

- Spanning Tree Configuration Menu screen
 - in MSTP mode 198
 - Spanning Tree Group Configuration
 - option 180, 191
 - Spanning Tree Group Configuration screen 181
 - Spanning Tree Group Configuration screen in MSTP mode 199
 - Spanning Tree Group Configuration screen in RSTP mode 191
 - Spanning Tree Groups (STG) 32
 - Spanning Tree Port Configuration
 - option 180, 191, 199, 199
 - Spanning Tree Port Configuration screen 183
 - Spanning Tree Port Configuration screen in MSTP mode 202
 - Spanning Tree Port Configuration screen in RSTP mode 193
 - Spanning Tree Protocol
 - configuring using Console Interface 179
 - Spanning Tree Protocol (STP) 32
 - Spanning Tree Switch Settings screen 186
 - Spanning Tree Switch Settings screen in MSTP mode 204
 - Spanning Tree Switch Settings screen in RSTP mode 195
 - Spanning Tree VLAN Membership screen 189, 208
 - Spanning Tree window 261
 - Split MultiLink Trunking (SMLT) 50
 - State field 186, 195, 204, 262, 267, 279, 285
 - STG 32
 - 802.1t path cost calculation 36
 - configuring using Console Interface 179
 - STG port membership mode 35
 - Stgld field 261
 - STGs
 - configuring using CLI 210
 - configuring with Device Manager 253
 - configuring with Web-based management 228
 - STP 32
 - STP and MLT 47
 - STP BPDU Filtering 40
 - Configuring with CLI 209
 - Configuring with Device Manager 252
 - STP Group 190
 - STP Group field 184, 187, 203, 205, 209
 - STP Group State field 183, 202
 - STP mode
 - setting with Web-based management 227
 - settings using CLI 209
 - STP Mode field 181, 184, 187, 192, 196
 - STP mode field 200
 - STP Multicast Address field 183
 - STPG mode
 - Display Spanning Tree Switch Settings option 180
 - Display Spanning Tree VLAN Membership option 180
 - Spanning Tree Group Configuration option 180
 - Spanning Tree Port Configuration option 180
- ## T
- Tagged BPDU on tagged port field 183
 - tagging
 - VLANs 20
 - TimeSinceTopologyChange field 266, 276, 282
 - TopChanges field 266, 276, 282
 - TransmittedBPDUs field 287
 - troubleshooting
 - spanning tree groups 202
 - VLANs 202
 - Troubleshooting ISTs 316
 - Trunk field 184, 194, 203
 - Tx Hold Count field 198, 207
 - TxConfigBpduCount field 280
 - TXHoldCount field 264
 - TxHoldCount field 274
 - TxMstBpduCount field 280
 - TxRstBpduCount field 280
 - TxTcnBpduCount field 280
- ## U
- Unit field 184, 194
 - UnknownPDUsRx field 342

V

- VCC 31
 - configuring with CLI 116
- Version field 265
- VID used for tagged BPDU field 183
- Virtual Local Area Networks 19
- VLACP 89
 - configuring 319
 - configuring with Device Manager 335
 - configuring with the CLI 325
- VLAN Configuration Control
 - configuring with CLI 116
- VLAN Configuration Control (VCC) 31
- VLAN configuration rules 30
- VLAN Membership field 190, 209
- VLAN NSNA 166
- VLAN tagging 20
- VlanIds field 161
- VLANs 19
 - configuring with CLI 109
 - configuring with Device Manager 155
 - configuring with Web-based management 135
- VLANs spanning multiple switches 26
- VLANs, port-based
 - creating with Web-based management 136
- VLANs, protocol-based
 - creating with Web-based management 137

Nortel Ethernet Routing Switch 5500 Series

Configuration — VLANs, Spanning Tree, and Link Aggregation

Copyright © 2005-2007, Nortel Networks
All Rights Reserved.

Publication: NN47200-502
Document status: Standard
Document version: 03.01
Document date: 27 August 2007

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

Sourced in Canada and the United States of America

The information in this document is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

Nortel, the Nortel logo and the Globemark are trademarks of Nortel Networks.

