

BLADEOS™

# Command Reference

BNT Virtual Fabric 10Gb Switch Module for IBM BladeCenter®

Version 6.3

---

Part Number: BMD00190, April 2010

**BLADE**  
NETWORK TECHNOLOGIES

2350 Mission College Blvd.  
Suite 600  
Santa Clara, CA 95054  
[www.bladenetwork.net](http://www.bladenetwork.net)

Copyright © 2010 BLADE Network Technologies, Inc., 2350 Mission College Blvd., Suite 600, Santa Clara, California, 95054, USA. All rights reserved. Part Number: BMD00190.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of BLADE Network Technologies, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

U.S. Government End Users: This document is provided with a “commercial item” as defined by FAR 2.101 (Oct. 1995) and contains “commercial technical data” and “commercial software documentation” as those terms are used in FAR 12.211-12.212 (Oct. 1995). Government End Users are authorized to use this documentation only in accordance with those rights and restrictions set forth herein, consistent with FAR 12.211- 12.212 (Oct. 1995), DFARS 227.7202 (JUN 1995) and DFARS 252.227-7015 (Nov. 1995).

BLADE Network Technologies, Inc. reserves the right to change any products described herein at any time, and without notice. BLADE Network Technologies, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by BLADE Network Technologies, Inc. The use and purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of BLADE Network Technologies, Inc.

BLADE Network Technologies, the BLADE logo, BLADEHarmony, BNT, NMotion, RackSwitch, Rackonomics, RackSwitch Solution Partner, ServerMobility, SmartConnect and VMready are trademarks of BLADE Network Technologies. All other names or marks are property of their respective owners.

Originated in the USA.

# Contents

---

## **Preface ■ 17**

Who Should Use This Book ■ 17

How This Book Is Organized ■ 17

Typographic Conventions ■ 19

How To Get Help ■ 21

## **Chapter 1: The Command Line Interface ■ 23**

Connecting to the Switch ■ 23

Management Module Setup ■ 24

Factory-Default vs. MM-Assigned IP Addresses ■ 24

Default Gateway ■ 25

Configuring Management Module for Switch Access ■ 25

Connecting to the Switch via Telnet ■ 26

Connecting to the Switch via SSH ■ 27

Accessing the Switch ■ 28

Setup vs. CLI ■ 30

Command Line History and Editing ■ 30

Idle Timeout ■ 30

## **Chapter 2: First-Time Configuration ■ 31**

Using the Setup Utility ■ 31

Information Needed for Setup ■ 31

Starting Setup When You Log In ■ 32

Stopping and Restarting Setup Manually ■ 33

Stopping Setup ■ 33

Restarting Setup ■ 33

Optional Setup for Telnet Support ■ 33

Setting Passwords ■ 34

Changing the Default Administrator Password ■ 34

Changing the Default User Password ■ 36

## **Chapter 3: Menu Basics ■ 39**

The Main Menu ■ 39

Menu Summary ■ 40

Global Commands ■ 41

Command Line History and Editing ■ 44

## Command Line Interface Shortcuts ■ 45

CLI List and Range Inputs ■ 45

Command Stacking ■ 45

Command Abbreviation ■ 46

Tab Completion ■ 46

## Chapter 4: The Information Menu ■ 47

## Information Menu ■ 48

## System Information Menu ■ 51

Error Disable and Recovery Information ■ 53

/info/sys/snmpv3 ■ 53

## SNMPv3 System Information Menu ■ 53

SNMPv3 USM User Table Information ■ 55

SNMPv3 View Table Information ■ 56

SNMPv3 Access Table Information ■ 57

SNMPv3 Group Table Information ■ 58

SNMPv3 Community Table Information ■ 58

SNMPv3 Target Address Table Information ■ 59

SNMPv3 Target Parameters Table Information ■ 60

SNMPv3 Notify Table Information ■ 61

SNMPv3 Dump Information ■ 62

## BladeCenter Chassis Information ■ 63

General System Information ■ 64

Show Recent Syslog Messages ■ 65

User Status Information ■ 66

## Stacking Information Menu ■ 67

Stacking Switch Information ■ 69

## Layer 2 Information Menu ■ 70

Active MultiPath Information ■ 73

Show AMP Global Information ■ 74

Show AMP Group Information ■ 75

## FDB Information Menu ■ 76

Show All FDB Information ■ 77

## Link Aggregation Control Protocol Information Menu ■ 78

Show All LACP Information ■ 79

## Layer 2 Failover Information Menu ■ 80

Show Layer 2 Failover Information ■ 80

## Hot Links Information Menu ■ 81

Hotlinks Trigger Information ■ 81

LLDP Information Menu	■	82
LLDP Remote Device Information	■	83
Unidirectional Link Detection Information Menu	■	84
UDLD Port Information	■	84
OAM Discovery Information Menu	■	85
OAM Port Information	■	85
802.1X Information	■	86
Spanning Tree Information	■	88
RSTP/MSTP Information	■	91
Common Internal Spanning Tree Information	■	94
Trunk Group Information	■	96
VLAN Information	■	97
Layer 3 Information Menu	■	98
IP Routing Information Menu	■	101
Show All IP Route Information	■	102
ARP Information Menu	■	104
Show All ARP Entry Information	■	105
ARP Address List Information	■	105
BGP Information Menu	■	106
BGP Peer Information	■	106
BGP Summary Information	■	107
Show All BGP Information	■	107
OSPF Information Menu	■	108
OSPF General Information	■	110
OSPF Interface Information	■	110
OSPF Database Information Menu	■	111
OSPF Route Codes Information	■	113
OSPFv3 Information Menu	■	114
OSPFv3 Area Index Information Menu	■	116
OSPFv3 Information	■	117
OSPFv3 Interface Information	■	118
OSPFv3 Database Information Menu	■	118
OSPFv3 Route Codes Information	■	120
Routing Information Protocol Information Menu	■	120
RIP Routes Information	■	121
Show RIP Interface Information	■	121
IPv6 Routing Information Menu	■	122
IPv6 Routing Table Information	■	122
IPv6 Neighbor Discovery Cache Information Menu	■	123
IPv6 Neighbor Discovery Cache Information	■	123

Interface Information	■	124
ECMP Static Routes Information	■	125
IP Information	■	126
IGMP Multicast Group Information Menu	■	127
IGMP Multicast Router Port Information Menu	■	128
IGMP Multicast Router Dump Information	■	128
IGMP Group Information	■	129
VRRP Information	■	130
Quality of Service Information Menu	■	131
802.1p Information	■	131
Access Control List Information Menu	■	133
Access Control List Information	■	134
RMON Information Menu	■	135
RMON History Information	■	136
RMON Alarm Information	■	137
RMON Event Information	■	138
Link Status Information	■	140
Port Information	■	142
Port Transceiver Status	■	143
Virtualization Information	■	144
Virtual Machines Information	■	144
Virtual Machine (VM) Information	■	145
VMware Information	■	145
VMware Host Information	■	146
Converged Enhanced Ethernet Information	■	147
DCBX Information	■	148
DCBX Control Information	■	149
DCBX Feature Information	■	149
DCBX ETS Information	■	151
DCBX PFC Information	■	152
DCBX Application Protocol Information	■	153
ETS Information Menu	■	154
ETS Information	■	155
PFC Information	■	156
PFC Information	■	156
FCoE Information	■	157
FIP Snooping Information	■	157
FIP Snooping Port Information	■	158
Information Dump	■	159

**Chapter 5: The Statistics Menu ■ 161****Statistics Menu ■ 161****Port Statistics Menu ■ 163**

802.1x Authenticator Statistics ■ 165

802.1x Authenticator Diagnostics ■ 166

Active MultiPath Statistics ■ 169

Bridging Statistics ■ 170

Ethernet Statistics ■ 171

Interface Statistics ■ 174

Interface Protocol Statistics ■ 177

Link Statistics ■ 177

RMON Statistics ■ 178

**Layer 2 Statistics Menu ■ 181**

Active MultiPath Statistics ■ 182

Active MultiPath Group Statistics ■ 183

FDB Statistics ■ 184

LACP Statistics ■ 185

Hotlinks Statistics ■ 186

LLDP Port Statistics ■ 187

OAM Statistics ■ 188

OAM Statistics ■ 189

**Layer 3 Statistics Menu ■ 190**

IPv4 Statistics ■ 193

IPv6 Statistics ■ 196

IPv4 Route Statistics ■ 201

IPv6 Route Statistics ■ 202

ARP Statistics ■ 202

DNS Statistics ■ 203

ICMP Statistics ■ 204

TCP Statistics ■ 206

UDP Statistics ■ 208

IGMP Statistics ■ 209

OSPF Statistics Menu ■ 210

OSPF Global Statistics ■ 211

OSPFv3 Statistics Menu ■ 215

OSPFv3 Statistics Menu ■ 216

OSPFv3 Global Statistics ■ 217

VRRP Statistics ■ 221

Routing Information Protocol Statistics ■ 222

**Management Processor Statistics Menu ■ 223**

MP Packet Statistics ■ 224

TCP Statistics ■ 225

UCB Statistics ■ 226

CPU Statistics ■ 226

**ACL Statistics Menu ■ 227**

ACL Statistics List ■ 227

VLAN Map Statistics ■ 228

**Fiber Channel over Ethernet Statistics ■ 229****SNMP Statistics ■ 230****NTP Statistics ■ 234****Statistics Dump ■ 235****Chapter 6: The Configuration Menu ■ 237****Configuration Menu ■ 237****Viewing, Applying, and Saving Changes ■ 239**

Viewing Pending Changes ■ 239

Applying Pending Changes ■ 240

Saving the Configuration ■ 240

**System Configuration Menu ■ 241**

Error Disable Configuration ■ 244

System Host Log Configuration Menu ■ 245

SSH Server Configuration Menu ■ 246

RADIUS Server Configuration Menu ■ 248

TACACS+ Server Configuration Menu ■ 250

LDAP Server Configuration Menu ■ 254

NTP Server Configuration Menu ■ 256

System SNMP Configuration Menu ■ 257

SNMPv3 Configuration Menu ■ 259

User Security Model Configuration Menu ■ 261

SNMPv3 View Configuration Menu ■ 262

View-Based Access Control Model Configuration Menu ■ 263

SNMPv3 Group Configuration Menu ■ 265

SNMPv3 Community Table Configuration Menu ■ 266

SNMPv3 Target Address Table Configuration Menu ■ 267

SNMPv3 Target Parameters Table Configuration Menu ■ 268

SNMPv3 Notify Table Configuration Menu ■ 269



System Access Configuration Menu	■	271
Management Networks Configuration Menu	■	273
User Access Control Configuration Menu	■	274
System User ID Configuration Menu	■	275
Strong Password Configuration Menu	■	276
HTTPS Access Configuration	■	277
Custom Daylight Savings Time Configuration Menu	■	279
sFlow Configuration Menu	■	280
sFlow Port Configuration Menu	■	281
Port Configuration Menu	■	282
Temporarily Disabling a Port	■	285
Port Error Disable and Recovery Configuration	■	285
Port Link Configuration Menu	■	286
UniDirectional Link Detection Configuration Menu	■	287
Port OAM Configuration Menu	■	288
Port ACL Configuration Menu	■	289
Port Spanning Tree Configuration Menu	■	290
Stacking Configuration Menu	■	291
Stacking Switch Menu	■	292
Quality of Service Configuration Menu	■	293
802.1p Configuration Menu	■	294
DSCP Configuration Menu	■	295
Access Control List Configuration Menu	■	296
ACL Configuration Menu	■	297
Ethernet Filtering Configuration Menu	■	298
IP version 4 Filtering Configuration Menu	■	299
TCP/UDP Filtering Configuration Menu	■	301
ACL Metering Configuration Menu	■	302
Re-Mark Configuration Menu	■	303
Re-Marking In-Profile Configuration Menu	■	304
Re-Marking Out-of-Profile Configuration Menu	■	305
Update User Priority Configuration Menu	■	305
Packet Format Filtering Configuration Menu	■	306
VMAP Configuration	■	307
ACL Group Configuration Menu	■	308
Port Mirroring Configuration	■	309
Port-Mirroring Configuration Menu	■	310

Layer 2 Configuration Menu	■	311
802.1X Configuration Menu	■	313
802.1X Global Configuration Menu	■	314
802.1X Guest VLAN Configuration Menu	■	316
802.1X Port Configuration Menu	■	317
Active MultiPath Protocol Configuration	■	319
AMP Group Configuration	■	321
RSTP/MSTP/PVRST Configuration Menu	■	323
Common Internal Spanning Tree Configuration Menu	■	325
CIST Bridge Configuration Menu	■	326
CIST Port Configuration Menu	■	327
Spanning Tree Configuration Menu	■	328
Spanning Tree Bridge Configuration Menu	■	329
Spanning Tree Port Configuration Menu	■	331
Forwarding Database Configuration Menu	■	332
Static Multicast MAC Configuration Menu	■	333
Static FDB Configuration Menu	■	334
LLDP Configuration Menu	■	335
LLDP Port Configuration Menu	■	336
LLDP Optional TLV Configuration Menu	■	337
Trunk Configuration Menu	■	339
IP Trunk Hash Configuration Menu	■	340
Layer 2 Trunk Hash Menu	■	341
Layer 3 Trunk Hash Menu	■	342
LACP Configuration Menu	■	343
LACP Port Configuration Menu	■	344
Layer 2 Failover Configuration Menu	■	345
Failover Trigger Configuration Menu	■	346
Auto Monitor Configuration Menu	■	347
Manual Monitor Configuration Menu	■	348
Manual Monitor Port Configuration Menu	■	349
Manual Monitor Control Configuration Menu	■	350
Hot Links Configuration Menu	■	351
Hot Links Trigger Configuration Menu	■	352
Hot Links Trigger Master Configuration Menu	■	353
Hot Links Trigger Backup Configuration Menu	■	354
VLAN Configuration Menu	■	355
Protocol-Based VLAN Configuration Menu	■	357
Private VLAN Configuration Menu	■	359

Layer 3 Configuration Menu	■ 360
IP Interface Configuration Menu	■ 363
IPv6 Neighbor Discovery Configuration Menu	■ 365
Default Gateway Configuration Menu	■ 367
IPv4 Static Route Configuration Menu	■ 368
IP Multicast Route Configuration Menu	■ 370
ARP Configuration Menu	■ 372
ARP Static Configuration Menu	■ 373
IP Forwarding Configuration Menu	■ 374
Network Filter Configuration Menu	■ 375
Routing Map Configuration Menu	■ 376
IP Access List Configuration Menu	■ 378
Autonomous System Filter Path Menu	■ 379
Routing Information Protocol Configuration Menu	■ 380
Routing Information Protocol Interface Configuration Menu	■ 381
RIP Route Redistribution Configuration Menu	■ 383
Open Shortest Path First Configuration Menu	■ 384
Area Index Configuration Menu	■ 386
OSPF Summary Range Configuration Menu	■ 388
OSPF Interface Configuration Menu	■ 389
OSPF Virtual Link Configuration Menu	■ 391
OSPF Host Entry Configuration Menu	■ 392
OSPF Route Redistribution Configuration Menu	■ 393
OSPF MD5 Key Configuration Menu	■ 394
Border Gateway Protocol Configuration Menu	■ 395
BGP Peer Configuration Menu	■ 397
BGP Redistribution Configuration Menu	■ 399
BGP Aggregation Configuration Menu	■ 401
IGMP Configuration Menu	■ 402
IGMP Snooping Configuration Menu	■ 403
IGMP Version 3 Configuration Menu	■ 404
IGMP Relay Configuration Menu	■ 406
IGMP Relay Multicast Router Configuration Menu	■ 407
IGMP Static Multicast Router Configuration Menu	■ 408
IGMP Filtering Configuration Menu	■ 409
IGMP Filter Definition Menu	■ 410
IGMP Filtering Port Configuration Menu	■ 411
IGMP Advanced Configuration Menu	■ 412
Domain Name System Configuration Menu	■ 413
Bootstrap Protocol Relay Configuration Menu	■ 415

- VRP Configuration Menu ■ 416
  - Virtual Router Configuration Menu ■ 418
  - Virtual Router Priority Tracking Configuration Menu ■ 420
  - Virtual Router Group Configuration Menu ■ 422
  - Virtual Router Group Priority Tracking Configuration Menu ■ 424
  - VRP Interface Configuration Menu ■ 425
  - VRP Tracking Configuration Menu ■ 426
- IPv6 Default Gateway Configuration Menu ■ 427
- IPv6 Static Route Configuration Menu ■ 428
- IPv6 Neighbor Discovery Cache Configuration Menu ■ 429
- Open Shortest Path First Version 3 Configuration Menu ■ 430
  - Area Index Configuration Menu ■ 433
  - OSPFv3 Summary Range Configuration Menu ■ 435
  - OSPFv3 AS-External Range Configuration Menu ■ 436
  - OSPFv3 Interface Configuration Menu ■ 438
  - OSPFv3 Virtual Link Configuration Menu ■ 440
  - OSPFv3 Host Entry Configuration Menu ■ 441
  - OSPFv3 Redist Entry Configuration Menu ■ 442
  - OSPFv3 Redistribute Configuration Menu ■ 443
- IP Loopback Interface Configuration Menu ■ 444
- Converged Enhanced Ethernet Configuration ■ 445
  - CEE Global Configuration ■ 446
    - ETS Global Configuration ■ 446
    - ETS Global Priority Group Configuration ■ 447
  - Priority Flow Control Global Configuration ■ 448
    - 802.1p Priority Flow Control Configuration ■ 449
  - CEE Port Configuration ■ 450
  - DCBX Port Configuration ■ 450
  - PFC Port Configuration ■ 452
    - 802.1p PFC Port Configuration ■ 453
- Fiber Channel over Ethernet Configuration ■ 454
  - FIPS Configuration ■ 454
  - FIPS Port Configuration ■ 456
- Remote Monitoring Configuration ■ 457
  - RMON History Configuration Menu ■ 458
  - RMON Event Configuration Menu ■ 459
  - RMON Alarm Configuration Menu ■ 460

Virtualization Configuration	■	462
Virtual Machines Policy Configuration	■	463
VM Policy Bandwidth Management	■	463
Virtual NIC Configuration	■	464
vNIC Port Configuration	■	465
vNIC Port Configuration	■	466
Virtual NIC Group Configuration	■	467
VM Group Configuration	■	469
VM Profile Configuration	■	471
VM Profile Edit	■	472
VM Ware Configuration	■	473
Dump	■	474
Saving the Active Switch Configuration	■	474
Restoring the Active Switch Configuration	■	475

## Chapter 7: The Operations Menu ■ 477

Operations Menu	■	477
Operations-Level Port Options Menu	■	480
Operations-Level Port 802.1X Options Menu	■	481
Operations-Level FCoE Menu	■	482
FCoE FIP Snooping Operations	■	482
Operations-Level VRRP Options Menu	■	483
Operations-Level IP Options Menu	■	484
Operations-Level BGP Options Menu	■	484
Protected Mode Options Menu	■	485
System Operations Menu	■	486
Virtualization Operations	■	487
VMware Operations	■	487

## Chapter 8: The Boot Options Menu ■ 491

Boot Menu	■	491
Bridge Module Menu	■	492
Stacking Boot Menu	■	493
Scheduled Reboot Menu	■	496
Netboot Configuration Menu	■	497
Updating the Switch Software Image	■	499
Loading New Software to Your Switch	■	499
Using the BBI	■	499
Using the CLI	■	501

- Selecting a Software Image to Run ■ 502
- Uploading a Software Image from Your Switch ■ 502
- Selecting a Configuration Block ■ 503
- Resetting the Switch ■ 504
- Accessing the ISCLI ■ 504
- Using the Boot Management Menu ■ 505
- Recovering from a Failed Upgrade ■ 505

## **Chapter 9: The Maintenance Menu ■ 509**

- Maintenance Menu ■ 509
- System Maintenance Menu ■ 511
- Forwarding Database Maintenance Menu ■ 512
- Debugging Menu ■ 513
- LLDP Cache Manipulation Menu ■ 514
- ARP Cache Maintenance Menu ■ 515
- IP Route Manipulation Menu ■ 516
- IGMP Maintenance Menu ■ 517
  - IGMP Group Maintenance Menu ■ 518
  - IGMP Multicast Routers Maintenance Menu ■ 519
- IPv6 Neighbor Discovery Cache Manipulation ■ 520
- IPv6 Route Manipulation Menu ■ 521
- Uuencode Flash Dump ■ 522
- FTP/TFTP System Dump Put ■ 522
- Clearing Dump Information ■ 523
- Unscheduled System Dumps ■ 523

## **Appendix A: BLADEOS Syslog Messages ■ 525**

- LOG\_CRIT ■ 526
- LOG\_WARNING ■ 526
- LOG\_ALERT ■ 528
- LOG\_ERR ■ 531
- LOG\_NOTICE ■ 535
- LOG\_INFO ■ 547

## **Appendix B: BLADEOS SNMP Agent ■ 553**

- SNMP Overview ■ 553
- Switch Images and Configuration Files ■ 556
  - Loading a New Switch Image ■ 557
  - Loading a Saved Switch Configuration ■ 558

Saving the Switch Configuration ■ 558

Saving a Switch Dump ■ 559

**Index** ■ 561





# Preface

---

The *BLADEOS 6.3 Command Reference* describes how to configure and use the BLADEOS 6.3 software with your Virtual Fabric 10Gb Switch Module (VFSM) for IBM BladeCenter.

For documentation on installing the switches physically, see the *Installation Guide* for your VFSM. For details about configuration and operation of your VFSM, see the *BLADEOS 6.3 Application Guide*.

## Who Should Use This Book

---

This book is intended for network installers and system administrators engaged in configuring and maintaining a network. The administrator should be familiar with Ethernet concepts, IP addressing, the IEEE 802.1D Spanning Tree Protocol, and SNMP configuration parameters.

## How This Book Is Organized

---

**Chapter 1, “The Command Line Interface,”** describes how to connect to the switch and access the information and configuration menus.

**Chapter 2, “First-Time Configuration,”** describes how to use the Setup utility for initial switch configuration and how to change the system passwords.

**Chapter 3, “Menu Basics,”** provides an overview of the menu system, including a menu map, global commands, and menu shortcuts.

**Chapter 4, “The Information Menu,”** shows how to view switch configuration parameters.

**Chapter 5, “The Statistics Menu,”** shows how to view switch performance statistics.

**Chapter 6, “The Configuration Menu,”** shows how to configure switch system parameters, ports, VLANs, Spanning Tree Protocol, SNMP, Port Mirroring, IP Routing, Port Trunking, and more.

**Chapter 7, “The Operations Menu,”** shows how to use commands which affect switch performance immediately, but do not alter permanent switch configurations (such as temporarily disabling ports). The menu describes how to activate or deactivate optional software features.

**Chapter 8, “The Boot Options Menu,”** describes the use of the primary and alternate switch images, how to load a new software image, and how to reset the software to factory defaults.

**Chapter 9, “The Maintenance Menu,”** shows how to generate and access a dump of critical switch state information, how to clear it, and how to clear part or all of the forwarding database.

**Appendix A, “BLADEOS Syslog Messages,”** shows a listing of syslog messages.

**Appendix B, “BLADEOS SNMP Agent,”** lists the Management Interface Bases (MIBs) supported in the switch software.

**“Index”** includes pointers to the description of the key words used throughout the book.

# Typographic Conventions

The following table describes the typographic styles used in this book.

**Table 1** Typographic Conventions

Typeface or Symbol	Meaning
plain fixed-width text	<p>This type is used for names of commands, files, and directories used within the text. For example:</p> <p>View the <code>readme.txt</code> file.</p> <p>It also depicts on-screen computer output and prompts.</p>
<b>bold fixed-width text</b>	<p>This bold type appears in command examples. It shows text that must be typed in exactly as shown. For example:</p> <p><b><code>/info/sys/gen</code></b></p>
<b>bold body text</b>	<p>This bold type indicates objects such as window names, dialog box names, and icons, as well as user interface objects such as buttons, and tabs.</p>
<i>italicized body text</i>	<p>This italicized type indicates book titles, special terms, or words to be emphasized.</p>
<b>block body text</b>	<p>Indicates objects such as window names, dialog box names, and icons, as well as user interface objects such as buttons and tabs.</p>
angle brackets < >	<p>Indicate a variable to enter based on the description inside the brackets. Do not type the brackets when entering the command.</p> <p>Example: If the command syntax is</p> <p><b>ping</b> &lt;IP address&gt;</p> <p>you enter</p> <p><b>ping 192.32.10.12</b></p>

**Table 1** Typographic Conventions

Typeface or Symbol	Meaning
braces { }	<p>Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.</p> <p>Example: If the command syntax is  <code>/cfg/12/vlan/vmap {add rem} &lt;1-127&gt;</code></p> <p>you enter:  <code>/cfg/12/vlan/vmap add 1</code></p> <p>or  <code>/cfg/12/vlan/vmap rem 1</code></p>
brackets [ ]	<p>Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.</p> <p>Example: If the command syntax is  <code>/cfg/sys/dhcp [mgta mgtb] enable</code></p> <p>you enter  <code>/cfg/sys/dhcp mgta enable</code></p> <p>or  <code>/cfg/sys/dhcp mgtb enable</code></p>
vertical line	<p>Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.</p> <p>Example: If the command syntax is  <code>/cfg/13/route/ecmphaash [sip dip]</code></p> <p>you enter:  <code>/cfg/13/route/ecmphaash sip</code></p> <p>or  <code>/cfg/13/route/ecmphaash dip</code></p> <p>or  <code>/cfg/13/route/ecmphaash sip dip</code></p>

## How To Get Help

---

If you need help, service, or technical assistance, see the “Getting help and technical assistance” appendix in the *BNT Virtual Fabric 10Gb Switch Module Installation Guide*.



## CHAPTER 1

# The Command Line Interface

---

Your Virtual Fabric 10Gb Switch Module (VFSM) is ready to perform basic switching functions right out of the box. Some of the more advanced features, however, require some administrative configuration before they can be used effectively.

The extensive BLADEOS switching software included in your switch provides a variety of options for accessing and configuring the switch:

- A built-in, text-based command line interface and menu system for access via a Telnet session or serial-port connection
- SNMP support for access through network management software such as IBM Director or HP OpenView
- BLADEOS Browser-Based Interface (BBI)

The command line interface is the most direct method for collecting switch information and performing switch configuration. Using a basic terminal, you are presented with a hierarchy of menus that enable you to view information and statistics about the switch, and to perform any necessary configuration.

This chapter explains how to access the Command Line Interface (CLI) for the switch.

## Connecting to the Switch

---

You can access the command line interface in any one of the following ways:

- Using a Telnet connection via the management module
- Using a Telnet connection over the network
- Using a SSH connection via the management module
- Using a serial connection via the serial port on the VFSM

## Management Module Setup

The BladeCenter VFSM is an integral subsystem within the overall BladeCenter system. The BladeCenter chassis includes a management module as the central element for overall chassis management and control.

You can use the management module to configure and manage the VFSM. The VFSM communicates with the management module(s) through its internal port 15 (MGT1) and port 16 (MGT2), which you can access through the 100 Mbps Ethernet port on each management module. The factory default settings permit management and control access to the switch module through *only* the management module or the built-in serial port. You can use the external Ethernet ports (EXTx) on the switch module for management and control of the switch, by selecting this mode as an option through the management module configuration utility program (see the applicable *BladeCenter Installation and User's Guide* publications for more information).

---

**Note** – Support for each management module is provided by a separate management port (MGT1 and MGT2). One port is active, and the other is used as a backup.

---

## Factory-Default vs. MM-Assigned IP Addresses

Each VFSM must be assigned its own Internet Protocol address, which is used for communication with an SNMP network manager or other Transmission Control Protocol/Internet Protocol (TCP/IP) applications (for example, BootP or TFTP). The factory-default IP address is 10.90.90.8x, where x corresponds to the number of the bay into which the VFSM is installed. For additional information, see the *Installation Guide*). The management module assigns an IP address of 192.168.70.1xx, where xx corresponds to the number of the bay into which each VFSM is installed, as shown in the following table:

**Table 2** VFSM IP addresses, based on switch-module bay numbers

Bay number	Factory-default IP address	IP address assigned by MM
Bay 7	10.90.90.80	192.168.70.133
Bay 8	10.90.90.82	192.168.70.134
Bay 9	10.90.90.81	192.168.70.135
Bay 10	10.90.90.83	192.168.70.136

---

**Note** – Before you install the VFSM in Bay 8 or Bay 10, confirm that your blade I/O Expansion adapter supports communication to these I/O bays.

---



## Default Gateway

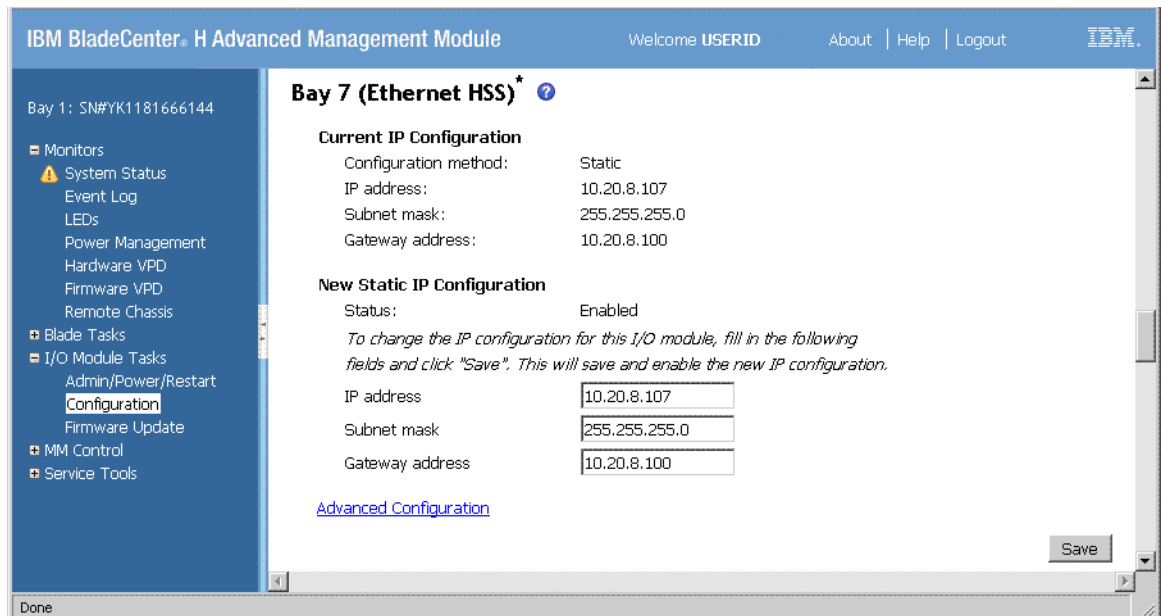
The default Gateway IP address determines where packets with a destination address outside the current subnet should be sent. Usually, the default Gateway is a router or host acting as an IP gateway to handle connections to other subnets of other TCP/IP networks. If you want to access the VFSM from outside your local network, use the management module to assign a default Gateway address to the VFSM. Choose **I/O Module Tasks > Configuration** from the navigation pane on the left, and enter the default Gateway IP address (for example, 192.168.70.125). Click **Save**.

## Configuring Management Module for Switch Access

Complete the following initial configuration steps:

1. Connect the Ethernet port of the management module to a 10/100 Mbps network (with access to a management station) or directly to a management station.
2. Access and log on to the management module, as described in the *BladeCenter Management Module User's Guide*. The management module provides the appropriate IP addresses for network access (see the applicable *BladeCenter Installation and User's Guide* publications for more information).
3. Select Configuration on the I/O Module Tasks menu on the left side of the BladeCenter Management Module window. See [Figure 1](#).

**Figure 1** Switch Management on the BladeCenter Management Module



4. You can use the default IP addresses provided by the management module, or you can assign a new IP address to the switch module through the management module. You can assign this IP address through one of the following methods:
  - Manually through the BladeCenter management module
  - Automatically through the IBM Director Configuration Wizard

---

**Note** – If you change the IP address of the VFSM, make sure that the switch module and the management module both reside on the same subnet.

---

5. Enable the following features in the management module:
  - External Ports (I/O Module Tasks > Admin/Power/Restart > Advanced Setup)
  - External management over all ports (Configuration > Advanced Configuration)
 

This setting is required if you want to access the management network through the external data ports (EXTx) on the VFSM.

The default value is `Disabled` for both features. If these features are not already enabled, change the value to `Enabled`, then `Save`.

---

**Note** – In `Advanced Configuration > Advanced Setup`, enable “Preserve new IP configuration on all switch resets,” to retain the switch’s IP interface when you restore factory defaults. This setting preserves the management port’s IP address in the management module’s memory, so you maintain connectivity to the management module after a reset.

---

You can now start a Telnet session, Browser-Based Interface (Web) session, a Secure Shell session, or a secure HTTPS session to the VFSM.

## Connecting to the Switch via Telnet

### *Configuring the Switch for Telnet Access*

Use the management module to access the VFSM through Telnet. Choose `I/O Module Tasks > Configuration` from the navigation pane on the left. Select a bay number and click `Advanced Configuration > Start Telnet/Web Session > Start Telnet Session`. A Telnet window opens a connection to the Switch Module (requires Java 1.4 Plug-in).

Once that you have configured the VFSM with an IP address and gateway, you can access the switch from any workstation connected to the management network. Telnet access provides the same options for user and administrator access as those available through the management module, minus certain Telnet and management commands.

To establish a Telnet connection with the switch, run the Telnet program on your workstation and issue the Telnet command, followed by the switch IP address:

```
telnet <switch IP address>
```

### Using Telnet to Access the Switch

Once the IP parameters on the VFSM are configured, you can access the CLI using a Telnet connection. From the management module, you can establish a Telnet connection with the switch.

You will then be prompted to enter a password as explained on [page 29](#).

## Connecting to the Switch via SSH

Although a remote network administrator can manage the configuration of a VFSM via Telnet, this method does not provide a secure connection. The SSH (Secure Shell) protocol enables you to securely log into another device over a network to execute commands remotely. As a secure alternative to using Telnet to manage switch configuration, SSH ensures that all data sent over the network is encrypted and secure.

The switch can do only one session of key/cipher generation at a time. Thus, a SSH/SCP client will not be able to login if the switch is doing key generation at that time. Similarly, the system will fail to do the key generation if a SSH/SCP client is logging in at that time.

The supported SSH encryption and authentication methods are listed below.

- Server Host Authentication: Client RSA-authenticates the switch in the beginning of every connection.
- Key Exchange: RSA
- Encryption: 3DES-CBC, DES
- User Authentication: Local password authentication, RADIUS, TACACS+

The following SSH clients have been tested:

- OpenSSH\_5.1p1 Debian-3ubuntu1
- SecureCRT 5.0 (Van Dyke Technologies, Inc.)
- Putty beta 0.60

---

**Note** – The BLADEOS implementation of SSH supports both versions 1.5 and 2.0 and supports SSH client version 1.5 - 2.x.

---

## Using SSH to Access the Switch

Once the IP parameters are configured and the SSH service is enabled on the VFSM (it is disabled by default), you can access the command line interface using an SSH connection.

To establish an SSH connection with the switch, run the SSH program on your workstation by issuing the SSH command, followed by the switch IP address:

```
>> # ssh <switch IP address>
```

If SecurID authentication is required, use the following command:

```
>> # ssh -l ace <switch IP address>
```

You will then be prompted to enter your user name and password.

## Accessing the Switch

To enable better switch management and user accountability, three levels or *classes* of user access have been implemented on the VFSM. Levels of access to CLI, Web management functions, and screens increase as needed to perform various switch management tasks. Conceptually, access classes are defined as follows:

- User interaction with the switch is completely passive—nothing can be changed on the VFSM. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.
- Operators can only effect temporary changes on the VFSM. These changes will be lost when the switch is rebooted/reset. Operators have access to the switch management features used for daily switch operations. Because any changes an operator makes are undone by a reset of the switch, operators cannot severely impact switch operation.
- Administrators are the only ones that may make permanent changes to the switch configuration—changes that are persistent across a reboot/reset of the switch. Administrators can access switch functions to configure and troubleshoot problems on the VFSM. Because administrators can also make temporary (operator-level) changes as well, they must be aware of the interactions between temporary and permanent changes.

Access to switch functions is controlled through the use of unique surnames and passwords. Once you are connected to the switch via local Telnet, remote Telnet, or SSH, you are prompted to enter a password. The default user names/password for each access level are listed in the following table.

**Note** – It is recommended that you change default switch passwords after initial configuration and as regularly as required under your network security policies. For more information, see [“Setting Passwords” on page 34](#).

**Table 3** User Access Levels

User Account	Description and Tasks Performed	Password
User	The User has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch.	user
Operator	The Operator manages all functions of the switch. The Operator can reset ports, except the management ports.	oper
Administrator	The superuser Administrator has complete access to all menus, information, and configuration commands on the VFSM, including the ability to change both the user and administrator passwords.	admin

**Note** – With the exception of the “admin” user, access to each user level can be disabled by setting the password to an empty value.

## Setup vs. CLI

---

Once the administrator password is verified, you are given complete access to the switch. If the switch is still set to its factory default configuration, the system will ask whether you wish to run Setup, a utility designed to help you through the first-time configuration process. If the switch has already been configured, the Main Menu of the CLI is displayed instead.

The following table shows the Main Menu with administrator privileges.

[Main Menu]	
info	- Information Menu
stats	- Statistics Menu
cfg	- Configuration Menu
oper	- Operations Command Menu
boot	- Boot Options Menu
maint	- Maintenance Menu
diff	- Show pending config changes [global command]
apply	- Apply pending config changes [global command]
save	- Save updated config to FLASH [global command]
revert	- Revert pending or applied changes [global command]
exit	- Exit [global command, always available]

---

**Note** – If you are accessing a user account, some menu options are not available.

---

## Command Line History and Editing

---

For a description of global commands, shortcuts, and command line editing functions, see [“Menu Basics” on page 39.](#)

## Idle Timeout

---

By default, the switch will disconnect your Telnet session after 10 minutes of inactivity. This function is controlled by the idle timeout parameter, which can be set from 1 to 60 minutes. For information on changing this parameter, see [“System Configuration Menu” on page 241.](#)

## CHAPTER 2

# First-Time Configuration

---

To help with the initial process of configuring your switch, the BLADEOS software includes a Setup utility. The Setup utility prompts you step-by-step to enter all the necessary information for basic configuration of the switch. This chapter describes how to use the Setup utility and how to change system passwords. Before you run Setup, you must first connect to the switch (see [Chapter 1, “Connecting to the Switch”](#)).

## Using the Setup Utility

---

Whenever you log in as the system administrator under the factory default configuration, you are asked whether you wish to run the Setup utility. Setup can also be activated manually from the command line interface any time after login.

## Information Needed for Setup

Setup requests the following information:

- Basic system information
  - ☐ Date & time
  - ☐ Whether to use Spanning Tree Group or not
- Optional configuration for each port
  - ☐ Speed, duplex, flow control, and negotiation mode (as appropriate)
  - ☐ Whether to use VLAN tagging or not (as appropriate)
- Optional configuration for each VLAN
  - ☐ Name of VLAN
  - ☐ Which ports are included in the VLAN

- Optional configuration of IP parameters
  - ☐ IP address, subnet mask, and VLAN for each IP interface
  - ☐ IP addresses for default gateway
  - ☐ Destination, subnet mask, and gateway IP address for each IP static route
  - ☐ Whether IP forwarding is enabled or not
  - ☐ Whether the RIP supply is enabled or not

## Starting Setup When You Log In

The Setup prompt appears automatically whenever you login as the system administrator under the factory default settings.

1. Connect to the switch.

After connecting, the login prompt will appear as shown below.

```
Enter Password:
```

2. Enter **admin** as the default administrator password.

If the factory default configuration is detected, the system prompts:

```
BNT Virtual Fabric 10Gb Switch Module
18:44:05 Wed Jan 3, 2010
```

```
The switch is booted with factory default configuration.
To ease the configuration of the switch, a "Set Up" facility which
will prompt you with those configuration items that are essential to
the operation of the switch is provided.
Would you like to run "Set Up" to configure the switch? [y/n]:
```

---

**Note** – If the default admin login is unsuccessful, or if the administrator Main Menu appears instead, the system configuration has probably been changed from the factory default settings. If you are certain that you need to return the switch to its factory default settings, see [“Selecting a Configuration Block” on page 503](#).

---

3. Enter **y** to begin the initial configuration of the switch, or **n** to bypass the Setup facility.



## Stopping and Restarting Setup Manually

### Stopping Setup

To abort the Setup utility, press <Ctrl-C> during any Setup question. When you abort Setup, the system will prompt:

```
Would you like to run from top again? [y/n]
```

Enter **n** to abort Setup, or **y** to restart the Setup program at the beginning.

### Restarting Setup

You can restart the Setup utility manually at any time by entering the following command at the administrator prompt:

```
# /cfg/setup
```

After initial configuration is complete, it is recommended that you change the default passwords as shown in [“Setting Passwords” on page 34](#).

## Optional Setup for Telnet Support

---

**Note** – This step is optional. Perform this procedure only if you are planning on connecting to the VFSM through a remote Telnet connection.

---

1. Telnet is enabled by default. To change the setting, use the following command:

```
>> # /cfg/sys/access/tnet
```

2. Apply and save the configuration(s).

```
>> System# apply  
>> System# save
```

## Setting Passwords

It is recommended that you change the user and administrator passwords after initial configuration and as regularly as required under your network security policies.

To change the administrator password, you must login using the administrator password.

**Note** – If you forget your administrator password, call your technical support representative for help using the password fix-up mode.

## Changing the Default Administrator Password

The administrator has complete access to all menus, information, and configuration commands, including the ability to change both the user and administrator passwords.

The default password for the administrator account is `admin`. To change the default password, follow this procedure:

1. Connect to the switch and log in using the `admin` password.
2. From the Main Menu, use the following command to access the Configuration Menu:

```
Main# /cfg
```

The Configuration Menu is displayed.

```
[Configuration Menu]
  sys      - System-wide Parameter Menu
  port     - Port Menu
  qos      - QOS Menu
  acl      - Access Control List Menu
  pmirr    - Port Mirroring Menu
  l2       - Layer 2 Menu
  l3       - Layer 3 Menu
  rmon     - RMON Menu
  virt     - Virtualization Menu
  setup    - Step by step configuration set up
  dump     - Dump current configuration to script file
  ptcfg    - Backup current configuration to FTP/TFTP server
  gtcfg    - Restore current configuration from FTP/TFTP server
  cur      - Display current configuration
```

3. From the Configuration Menu, use the following command to select the System Menu:

```
>> Configuration# sys
```

The System Menu is displayed.

```
[System Menu]
errdis - Errdisable Menu
syslog - Syslog Menu
sshd - SSH Server Menu
radius - RADIUS Authentication Menu
tacacs+ - TACACS+ Authentication Menu
ldap - LDAP Authentication Menu
ntp - NTP Server Menu
ssnmp - System SNMP Menu
access - System Access Menu
dst - Custom DST Menu
sflow - sFlow Menu
date - Set system date
time - Set system time
timezone - Set system timezone
dlight - Set system daylight savings
idle - Set timeout for idle CLI sessions
linkscan - Set linkscan mode
notice - Set login notice
bannr - Set login banner
hprompt - Enable/disable display hostname (sysName) in CLI prompt
reminder - Enable/disable Reminders
rstctrl - Enable/disable System reset on panic
cur - Display current system-wide parameters
```

4. From the System Menu, use the following command to select the System Access Menu:

```
>> System# access
```

The System Access Menu is displayed.

```
[System Access Menu]
mgmt - Management Network Definition Menu
user - User Access Control Menu (passwords)
https - HTTPS Web Access Menu
snmp - Set SNMP access control
tnport - Set Telnet server port number
tport - Set the TFTP Port for the system
wport - Set HTTP (Web) server port number
http - Enable/disable HTTP (Web) access
tnet - Enable/disable Telnet access
tsbbi - Enable/disable Telnet/SSH configuration from BBI
userbbi - Enable/disable user configuration from BBI
cur - Display current system access configuration
```

5. Select the administrator password.

```
System Access# user/admpw
```

6. Enter the current administrator password at the prompt:

```
Changing ADMINISTRATOR password; validation required...  
Enter current administrator password:
```

---

**Note** – If you forget your administrator password, call your technical support representative for help using the password fix-up mode.

---

7. Enter the new administrator password at the prompt:

```
Enter new administrator password:
```

8. Enter the new administrator password, again, at the prompt:

```
Re-enter new administrator password:
```

9. Apply and save your change by entering the following commands:

```
System# apply  
System# save
```

## Changing the Default User Password

The user login has limited control of the switch. Through a user account, you can view switch information and statistics, but you can't make configuration changes.

The default password for the user account is `user`. This password can be changed from the user account. The administrator can change all passwords, as shown in the following procedure.

1. Connect to the switch and log in using the `admin` password.
2. From the Main Menu, use the following command to access the Configuration Menu:

```
Main# cfg
```

3. From the Configuration Menu, use the following command to select the System Menu:

```
>> Configuration# sys
```

4. From the System Menu, use the following command to select the System Access Menu:

```
>> System# access
```

5. Select the user password.

```
System# user/usrpw
```

6. Enter the current administrator password at the prompt.

Only the administrator can change the user password. Entering the administrator password confirms your authority.

```
Changing USER password; validation required...  
Enter current administrator password:
```

7. Enter the new user password at the prompt:

```
Enter new user password:
```

8. Enter the new user password, again, at the prompt:

```
Re-enter new user password:
```

9. Apply and save your changes:

```
System# apply  
System# save
```



## CHAPTER 3

# Menu Basics

---

The BLADEOS Command Line Interface (CLI) is used for viewing switch information and statistics. In addition, the administrator can use the CLI for performing all levels of switch configuration.

To make the CLI easy to use, the various commands have been logically grouped into a series of menus and sub-menus. Each menu displays a list of commands and/or sub-menus that are available, along with a summary of what each command will do. Below each menu is a prompt where you can enter any command appropriate to the current menu.

This chapter describes the Main Menu commands, and provides a list of commands and shortcuts that are commonly available from all the menus within the CLI.

## The Main Menu

---

The Main Menu appears after a successful connection and login. The following table shows the Main Menu for the administrator login. Some features are not available under the user login.

[Main Menu]	
info	- Information Menu
stats	- Statistics Menu
cfg	- Configuration Menu
oper	- Operations Command Menu
boot	- Boot Options Menu
maint	- Maintenance Menu
diff	- Show pending config changes [global command]
apply	- Apply pending config changes [global command]
save	- Save updated config to FLASH [global command]
revert	- Revert pending or applied changes [global command]
exit	- Exit [global command, always available]

## Menu Summary

---

### ■ **Information Menu**

Provides sub-menus for displaying information about the current status of the switch: from basic system settings to VLANs, and more.

### ■ **Statistics Menu**

Provides sub-menus for displaying switch performance statistics. Included are port, IF, IP, ICMP, TCP, UDP, SNMP, routing, ARP, DNS, and VRRP statistics.

### ■ **Configuration Menu**

This menu is available only from an administrator login. It includes sub-menus for configuring every aspect of the switch. Changes to configuration are not active until explicitly applied. Changes can be saved to non-volatile memory.

### ■ **Operations Menu**

Operations-level commands are used for making immediate and temporary changes to switch configuration. This menu is used for bringing ports temporarily in and out of service, enabling or disabling FDB learning on a port, or sending NTP requests. It is also used for activating or deactivating optional software packages.

### ■ **Boot Options Menu**

This menu is used for upgrading switch software, selecting configuration blocks, and for resetting the switch when necessary.

### ■ **Maintenance Menu**

This menu is used for debugging purposes, enabling you to generate a dump of the critical state information in the switch, and to clear entries in the forwarding database and the ARP and routing tables.



# Global Commands

Some basic commands are recognized throughout the menu hierarchy. These commands are useful for obtaining online help, navigating through menus, and for applying and saving configuration changes.

For help on a specific command, type `help`. You will see the following screen:

```
Global Commands: [can be issued from any menu]
help             up             print             pwd
lines           verbose        exit            quit
diff            apply          save            revert
revert apply
ping            traceroute     telnet          history
pushd           popd           who             chpass_p
chpass_s

The following are used to navigate the menu structure:
.  Print current menu
.. Move up one menu level
/  Top menu if first, or command separator
!  Execute command from history
```

**Table 4** Description of Global Commands

Command	Action
<b>? <i>command</i></b> <b>or help</b>	Provides more information about a specific command on the current menu. When used without the <i>command</i> parameter, a summary of the global commands is displayed.
<b>. or print</b>	Display the current menu.
<b>list</b>	Lists the commands available at the current level. You may follow the list command with a text string, and list all of the available commands that match the string.
<b>.. or up</b>	Go up one level in the menu structure.
<b>/</b>	If placed at the beginning of a command, go to the Main Menu. Otherwise, this is used to separate multiple commands placed on the same line.
<b>lines [n]</b>	Set the number of lines ( <i>n</i> ) that display on the screen at one time. The default is 24 lines. When used without a value, the current setting is displayed. Set lines to a value of 0 (zero) to disable pagination.
<b>diff</b>	Show any pending configuration changes.

Table 4 Description of Global Commands

Command	Action
<b>apply</b>	Apply pending configuration changes.
<b>save</b>	Write configuration changes to non-volatile flash memory.
<b>revert</b>	Remove pending configuration changes between “ <b>apply</b> ” commands. Use this command to remove any configuration changes made since last <b>apply</b> .
<b>revert apply</b>	Remove pending or applied configuration changes between “ <b>save</b> ” commands. Use this command to remove any configuration changes made since last <b>save</b> .
<b>exit</b> or <b>quit</b>	Exit from the command line interface and log out.
<b>ping</b>	<p>Use this command to verify station-to-station connectivity across the network. The format is as follows:</p> <pre><b>ping</b> &lt;host name&gt;   &lt;IP address&gt; [-n &lt;tries (0-4294967295)&gt;] [-w &lt;msec delay (0-4294967295)&gt;] [-l &lt;length (0/32-65500/2080)&gt;] [-s &lt;IP source&gt;] [-v &lt;tos (0-255)&gt;] [-f] [-t]</pre> <p>Where:</p> <ul style="list-style-type: none"><li>□ <b>-n</b>: Sets the number of attempts (optional).</li><li>□ <b>-w</b>: Sets the number of milliseconds between attempts (optional).</li><li>□ <b>-l</b>: Sets the ping request payload size (optional).</li><li>□ <b>-s</b>: Sets the IP source address for the IP packet (optional).</li><li>□ <b>-v</b>: Sets the Type Of Service bits in the IP header.</li><li>□ <b>-f</b>: Sets the <i>don't fragment</i> bit in the IP header (only for IPv4 addresses).</li><li>□ <b>-t</b>: Pings continuously (same as <b>-n 0</b>).</li></ul> <p>The DNS parameters must be configured if specifying hostnames (see <a href="#">“Domain Name System Configuration Menu” on page 413</a>).</p>

**Table 4** Description of Global Commands

Command	Action
<b>traceroute</b>	<p>Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows:</p> <pre><b>traceroute</b> &lt;hostname&gt;   &lt;IP address&gt; [<b>&lt;max-hops (1-32)&gt;</b> [<b>&lt;msec-delay (1-4294967295)&gt;</b> ] ]</pre> <p>Where <i>hostname/IP address</i> is the hostname or IP address of the target station, <i>max-hops</i> (optional) is the maximum distance to trace (1-32 devices), and <i>msec-delay</i> (optional) is the number of milliseconds to wait for the response.</p> <p>As with <code>ping</code>, the DNS parameters must be configured if specifying hostnames.</p>
<b>pwd</b>	Display the command path used to reach the current menu.
<b>verbose</b> <i>n</i>	<p>Sets the level of information displayed on the screen:</p> <p><b>0</b> = Quiet: Nothing appears except errors—not even prompts.</p> <p><b>1</b> = Normal: Prompts and requested output are shown, but no menus.</p> <p><b>2</b> = Verbose: Everything is shown.</p> <p>When used without a value, the current setting is displayed.</p>
<b>telnet</b>	<p>This command is used to telnet out of the switch. The format is as follows:</p> <pre><b>telnet</b> &lt;hostname&gt;   &lt;IP address&gt; [<b>&lt;port&gt;</b>]</pre> <p>Where <i>IP address</i> is the hostname or IP address of the device.</p>
<b>history</b>	This command displays the most recent commands.
<b>pushd</b>	Save the current menu path, so you can jump back to it using <code>popd</code> .
<b>popd</b>	Go to the menu path and position previously saved by using <code>pushd</code> .
<b>who</b>	Displays a list of users that are logged on to the switch.
<b>chpass_p</b>	Configures the password for the primary TACACS+ server.
<b>chpass_s</b>	Configures the password for the secondary TACACS+ server.

## Command Line History and Editing

Using the command line interface, you can retrieve and modify previously entered commands with just a few keystrokes. The following options are available globally at the command line:

**Table 5** Command Line History and Editing Options

Option	Description
<b>history</b>	Display a numbered list of the last 64 previously entered commands.
<b>!!</b>	Repeat the last entered command.
<b>!n</b>	Repeat the $n^{\text{th}}$ command shown on the history list.
<Ctrl-p>	(Also the up arrow key.) Recall the <i>previous</i> command from the history list. This can be used multiple times to work backward through the last 64 commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-n>	(Also the down arrow key.) Recall the <i>next</i> command from the history list. This can be used multiple times to work forward through the last 64 commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-a>	Move the cursor to the beginning of command line.
<Ctrl-e>	Move cursor to the <i>end</i> of the command line.
<Ctrl-b>	(Also the left arrow key.) Move the cursor <i>back</i> one position to the left.
<Ctrl-f>	(Also the right arrow key.) Move the cursor <i>forward</i> one position to the right.
<Backspace>	(Also the Delete key.) Erase one character to the left of the cursor position.
<Ctrl-d>	<i>Delete</i> one character at the cursor position.
<Ctrl-k>	<i>Kill</i> (erase) all characters from the cursor position to the end of the command line.
<Ctrl-l>	Redraw the screen.
<Ctrl-u>	Clear the entire line.
Other keys	Insert new characters at the cursor position.

## Command Line Interface Shortcuts

---

The following shortcuts allow you to enter commands quickly and easily.

### CLI List and Range Inputs

For CLI commands that allow an individual item to be selected from within a numeric range, lists and ranges of items can now be specified. For example, the `/info/vlan` command permits the following options:

# <code>/info/vlan</code>	<i>(show all VLANs)</i>
# <code>/info/vlan 1</code>	<i>(show only VLAN 1)</i>
# <code>/info/vlan 1,3,4095</code>	<i>(show listed VLANs)</i>
# <code>/info/vlan 1-20</code>	<i>(show range 1 through 20)</i>
# <code>/info/vlan 1-5,90-99,4090-4095</code>	<i>(show multiple ranges)</i>
# <code>/info/vlan 1-5,19,20,4090-4095</code>	<i>(show a mix of lists and ranges)</i>

The numbers in a range must be separated by a dash: `<start of range>-<end of range>`

Multiple ranges or list items are permitted using a comma: `<range or item 1>,<range or item 2>`

Do not use spaces within list and range specifications.

Ranges can also be used to apply the same command option to multiple items. For example, to enable multiple ports with one command:

# <code>/cfg/port 1-4/ena</code>	<i>(Enable ports 1 though 4)</i>
----------------------------------	----------------------------------

---

**Note** – Port ranges accept only port numbers, not aliases such as INT1 or EXT1.

---

### Command Stacking

As a shortcut, you can type multiple commands on a single line, separated by forward slashes (/). You can connect as many commands as required to access the menu option that you want. For example, the keyboard shortcut to access the Spanning Tree Port Configuration Menu from the `Main#` prompt is as follows:

Main# <code>cfg/12/stg 1/port</code>
--------------------------------------

## Command Abbreviation

Most commands can be abbreviated by entering the first characters which distinguish the command from the others in the same menu or sub-menu. For example, the command shown above could also be entered as follows:

```
Main# c/12/stg 1/po
```

## Tab Completion

By entering the first letter of a command at any menu prompt and hitting <Tab>, the CLI will display all commands or options in that menu that begin with that letter. Entering additional letters will further refine the list of commands or options displayed. If only one command fits the input text when <Tab> is pressed, that command will be supplied on the command line, waiting to be entered. If the <Tab> key is pressed without any input on the command line, the currently active menu will be displayed.

## CHAPTER 4

# The Information Menu

---

You can view configuration information for the switch in both the user and administrator command modes. This chapter discusses how to use the command line interface to display switch information.

/info

# Information Menu

[Information Menu]	
sys	- System Information Menu
stack	- Stacking Menu
l2	- Layer 2 Information Menu
l3	- Layer 3 Information Menu
qos	- QoS Menu
acl	- Show ACL information
rmon	- Show RMON information
link	- Show link status
port	- Show port information
transcvr	- Show Port Transceiver status
virt	- Show Virtualization information
cee	- CEE Information Menu
fcoe	- Fiber Channel Over Ethernet Information Menu
dcbx	- DCBX Debug Menu
dump	- Dump all information

The information provided by each menu option is briefly described in [Table 6](#), with pointers to detailed information.

**Table 6** Information Menu Options (/info)

**Command Syntax and Usage**

**sys**

Displays the System Information Menu. For details, see [page 51](#).

**stack**

Displays the Stacking Information Menu. For details, see [page 67](#).

**l2**

Displays the Layer 2 Information Menu. For details, see [page 70](#).

**l3**

Displays the Layer 3 Information Menu. For details, see [page 98](#).

**qos**

Displays the Quality of Service (QoS) Information Menu. For details, see [page 131](#).

**acl**

Displays the current configuration profile for each Access Control List (ACL) and ACL Group. For details, see [page 134](#).



**Table 6** Information Menu Options (/info)

---

**Command Syntax and Usage**

---

**rmon**

Displays the Remote Monitoring (RMON) Information Menu. For details, see [page 135](#).

---

**link**

Displays configuration information about each port, including:

- ☐ Port alias and number
- ☐ Port speed
- ☐ Duplex mode (half, full, or auto)
- ☐ Flow control for transmit and receive (no, yes, or both)
- ☐ Link status (up, down, or disabled)

For details, see [page 140](#).

---

**port**

Displays port status information, including:

- ☐ Port alias and number
- ☐ Whether the port uses VLAN Tagging or not
- ☐ Port VLAN ID (PVID)
- ☐ Port name
- ☐ VLAN membership
- ☐ Fast Forwarding status
- ☐ FDB Learning status
- ☐ Flood Blocking status

For details, see [page 142](#).

---

**transcvr**

Displays the status of the port transceiver module on each external port.

For details, see [page 143](#).

---

**virt**

Displays the Virtualization information menu. For details, see [page 144](#).

---

**cee**

Displays the Converged Enhanced Ethernet (CEE) information menu. For details, see [page 147](#).

---

**Table 6** Information Menu Options (/info)

Command Syntax and Usage	
<b>fcoe</b>	Displays the Fiber Channel over Ethernet (FCoE) information menu. For details, see <a href="#">page 157</a> .
<b>dump</b>	Dumps all switch information available from the Information Menu (10K or more, depending on your configuration).  If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

/info/sys

# System Information Menu

---

[System Menu]	
errdis	- Errdisable Menu
snmpv3	- SNMPv3 Information Menu
chassis	- Show BladeCenter Chassis related information
general	- Show general system information
log	- Show last 100 syslog messages
user	- Show current user status
dump	- Dump all system information

The information provided by each menu option is briefly described in [Table 7](#), with pointers to where detailed information can be found.

**Table 7** System Menu Options (/info/sys)

---

## Command Syntax and Usage

---

### errdis

Displays Error Disable and Recovery Information menu. To view the menu options, see [page 53](#).

---

### snmpv3

Displays SNMPv3 Information Menu. To view the menu options, see [page 53](#).

---

### chassis

Displays information about the BladeCenter chassis. For details, see [page 63](#).

---

**Table 7** System Menu Options (/info/sys)

---

**Command Syntax and Usage**

---

**general**

Displays system information, including:

- ☐ System date and time
- ☐ Switch model name and number
- ☐ Switch name and location
- ☐ Time of last boot
- ☐ MAC address of the switch management processor
- ☐ IP address of management interface
- ☐ Hardware version and part number
- ☐ Software image file and version number
- ☐ Configuration name
- ☐ Log-in banner, if one is configured

For details, see [page 64](#).

---

**log**

Displays most recent syslog messages. For details, see [page 65](#).

---

**user**

Displays configured user names and their status. For details, see [page 66](#).

---

**dump**

Dumps all switch information available from the Information Menu (10K or more, depending on your configuration).

---

`/info/sys/errdis`  
**Error Disable and Recovery Information**

```
[ErrDisable Information Menu]
  recovery - Show ErrDisable recovery information
  timers   - Show ErrDisable timer information
  dump     - Show all of the above
```

This menu allows you to display information about the Error Disable and Recovery feature for interface ports.

**Table 8** Error Disable Information Options

---

**Command Syntax and Usage**

---

**recovery**

Displays a list ports with their Error Recovery status.

---

**timers**

Displays a list of active recovery timers, if applicable.

---

**dump**

Displays all Error Disable and Recovery information.

---

`/info/sys/snmpv3`  
**SNMPv3 System Information Menu**

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please refer to RFC2271 to RFC2276.

[SNMPv3 Information Menu]	
usm	- Show usmUser table information
view	- Show vacmViewTreeFamily table information
access	- Show vacmAccess table information
group	- Show vacmSecurityToGroup table information
comm	- Show community table information
taddr	- Show targetAddr table information
tparam	- Show targetParams table information
notify	- Show notify table information
dump	- Show all SNMPv3 information

**Table 9** SNMPv3 information Menu Options (/info/sys/snmpv3)

**Command Syntax and Usage**

**usm**

Displays User Security Model (USM) table information. To view the table, see [page 55](#).

**view**

Displays information about view, sub-trees, mask and type of view. To view a sample, see [page 56](#).

**access**

Displays View-based Access Control information. To view a sample, see [page 57](#).

**group**

Displays information about the group that includes, the security model, user name, and group name. To view a sample, see [page 58](#).

**comm**

Displays information about the community table information. To view a sample, see [page 58](#).

**taddr**

Displays the Target Address table information. To view a sample, see [page 59](#).

**tparam**

Displays the Target parameters table information. To view a sample, see [page 60](#).

**Table 9** SNMPv3 information Menu Options (/info/sys/snmpv3)

Command Syntax and Usage
<b>notify</b>
Displays the Notify table information. To view a sample, see <a href="#">page 61</a> .
<b>dump</b>
Displays all the SNMPv3 information. To view a sample, see <a href="#">page 62</a> .

**/info/sys/snmpv3/usm**  
SNMPv3 USM User Table Information

The User-based Security Model (USM) in SNMPv3 provides security services such as authentication and privacy of messages. This security model makes use of a defined set of user identities displayed in the USM user table. The USM user table contains the following information:

- the user name
- a security name in the form of a string whose format is independent of the Security Model
- an authentication protocol, which is an indication that the messages sent on behalf of the user can be authenticated
- the privacy protocol

usmUser Table:	
User Name	Protocol
-----	-----
adminmd5	HMAC_MD5, DES PRIVACY
adminsha	HMAC_SHA, DES PRIVACY
vlv2only	NO AUTH, NO PRIVACY

**Table 10** USM User Table Information Parameters (/info/sys/usm)

Field	Description
User Name	This is a string that represents the name of the user that you can use to access the switch.
Protocol	This indicates whether messages sent on behalf of this user are protected from disclosure using a privacy protocol. BLADEOS supports DES algorithm for privacy. The software also supports two authentication algorithms: MD5 and HMAC-SHA.

`/info/sys/snmpv3/view`  
SNMPv3 View Table Information

The user can control and restrict the access allowed to a group to only a subset of the management information in the management domain that the group can access within each context by specifying the group’s rights in terms of a particular MIB view for security reasons.

View Name	Subtree	Mask	Type
-----	-----	-----	-----
iso	1.3		included
v1v2only	1.3		included
v1v2only	1.3.6.1.6.3.15		excluded
v1v2only	1.3.6.1.6.3.16		excluded
v1v2only	1.3.6.1.6.3.18		excluded

**Table 11** SNMPv3 View Table Information Parameters (`/info/sys/snmpv3/view`)

Field	Description
View Name	Displays the name of the view.
Subtree	Displays the MIB subtree as an OID string. A view subtree is the set of all MIB object instances which have a common Object Identifier prefix to their names.
Mask	Displays the bit mask.
Type	Displays whether a family of <code>view subtrees</code> is included or excluded from the MIB view.



`/info/sys/snmpv3/access`  
SNMPv3 Access Table Information

The access control sub system provides authorization services.

The vacmAccessTable maps a group name, security information, a context, and a message type, which could be the read or write type of operation or notification into a MIB view.

The View-based Access Control Model defines a set of services that an application can use for checking access rights of a group. This group's access rights are determined by a read-view, a write-view and a notify-view. The read-view represents the set of object instances authorized for the group while reading the objects. The write-view represents the set of object instances authorized for the group when writing objects. The notify-view represents the set of object instances authorized for the group when sending a notification.

Group Name	Prefix	Model	Level	Match	ReadV	WriteV	NotifyV
-----	-----	-----	-----	-----	-----	-----	-----
v1v2grp		snmpv1	noAuthNoPriv	exact	iso	iso	v1v2only
admingrp		usm	authPriv	exact	iso	iso	iso

**Table 12** SNMPv3 Access Table Information (`/info/sys/snmpv3/access`)

Field	Description
Group Name	Displays the name of group.
Prefix	Displays the prefix that is configured to match the values.
Model	Displays the security model used, for example, SNMPv1, or SNMPv2 or USM.
Level	Displays the minimum level of security required to gain rights of access. For example, noAuthNoPriv, authNoPriv, or authPriv.
Match	Displays the match for the contextName. The options are: exact and prefix.
ReadV	Displays the MIB view to which this entry authorizes the read access.
WriteV	Displays the MIB view to which this entry authorizes the write access.
NotifyV	Displays the Notify view to which this entry authorizes the notify access.

## `/info/sys/snmpv3/group` SNMPv3 Group Table Information

A group is a combination of security model and security name that defines the access rights assigned to all the security names belonging to that group. The group is identified by a group name.

Sec Model	User Name	Group Name
-----	-----	-----
snmpv1	v1v2only	v1v2grp
usm	adminmd5	admingrp
usm	adminsha	admingrp

**Table 13** SNMPv3 Group Table Information Parameters  
(`/info/sys/snmpv3/group`)

Field	Description
Sec Model	Displays the security model used, which is any one of: USM, SNMPv1, SNMPv2, and SNMPv3.
User Name	Displays the name for the group.
Group Name	Displays the access name of the group.

## `/info/sys/snmpv3/comm` SNMPv3 Community Table Information

This command displays the community table information stored in the SNMP engine.

Index	Name	User Name	Tag
-----	-----	-----	-----
trap1	public	v1v2only	v1v2trap

**Table 14** SNMPv3 Community Table Parameters (`/info/sys/snmpv3/comm`)

Field	Description
Index	Displays the unique index value of a row in this table
Name	Displays the community string, which represents the configuration.
User Name	Displays the User Security Model (USM) user name.
Tag	Displays the community tag. This tag specifies a set of transport endpoints from which a command responder application accepts management requests and to which a command responder application sends an SNMP trap.

`/info/sys/snmpv3/taddr`  
SNMPv3 Target Address Table Information

This command displays the SNMPv3 target address table information, which is stored in the SNMP engine.

Name	Transport Addr	Port	Taglist	Params
trap1	47.81.25.66	162	v1v2trap	v1v2param

**Table 15** SNMPv3 Target Address Table Information Parameters  
(/info/sys/snmpv3/taddr)

Field	Description
Name	Displays the locally arbitrary, but unique identifier associated with this snmpTargetAddrEntry.
Transport Addr	Displays the transport addresses.
Port	Displays the SNMP UDP port number.
Taglist	This column contains a list of tag values which are used to select target addresses for a particular SNMP message.
Params	The value of this object identifies an entry in the snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address.

`/info/sys/snmpv3/tparam`  
SNMPv3 Target Parameters Table Information

Name	MP Model	User Name	Sec Model	Sec Level
-----	-----	-----	-----	-----
v1v2param	snmpv2c	v1v2only	snmpv1	noAuthNoPriv

**Table 16** SNMPv3 Target Parameters Table Information  
(/info/sys/snmpv3/tparam)

Field	Description
Name	Displays the locally arbitrary, but unique identifier associated with this <code>snmpTargetParamsEntry</code> .
MP Model	Displays the Message Processing Model used when generating SNMP messages using this entry.
User Name	Displays the <code>securityName</code> , which identifies the entry on whose behalf SNMP messages will be generated using this entry.
Sec Model	Displays the security model used when generating SNMP messages using this entry. The system may choose to return an <code>inconsistentValue</code> error if an attempt is made to set this variable to a value for a security model which the system does not support.
Sec Level	Displays the level of security used when generating SNMP messages using this entry.

`/info/sys/snmpv3/notify`  
SNMPv3 Notify Table Information

Name	Tag
-----	-----
v1v2trap	v1v2trap

**Table 17** SNMPv3 Notify Table Information (/info/sys/snmpv3/notify)

Field	Description
Name	The locally arbitrary, but unique identifier associated with this snmpNotifyEntry.
Tag	This represents a single tag value which is used to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable that contains a tag value equal to the value of this entry, is selected. If this entry contains a value of zero length, no entries are selected.

## /info/sys/snmpv3/dump

### SNMPv3 Dump Information

#### usmUser Table:

User Name	Protocol
adminmd5	HMAC_MD5, DES PRIVACY
adminsha	HMAC_SHA, DES PRIVACY
vlv2only	NO AUTH, NO PRIVACY

#### vacmAccess Table:

Group Name	Prefix	Model	Level	Match	ReadV	WriteV	NotifyV
vlv2grp		snmpv1	noAuthNoPriv	exact	iso	iso	vlv2only
admingrp		usm	authPriv	exact	iso	iso	iso

#### vacmViewTreeFamily Table:

View Name	Subtree	Mask	Type
iso	1.3		included
vlv2only	1.3		included
vlv2only	1.3.6.1.6.3.15		excluded
vlv2only	1.3.6.1.6.3.16		excluded
vlv2only	1.3.6.1.6.3.18		excluded

#### vacmSecurityToGroup Table:

Sec Model	User Name	Group Name
snmpv1	vlv2only	vlv2grp
usm	adminsha	admingrp

#### snmpCommunity Table:

Index	Name	User Name	Tag
-------	------	-----------	-----

#### snmpNotify Table:

Name	Tag
------	-----

#### snmpTargetAddr Table:

Name	Transport	Addr	Port	Taglist	Params
------	-----------	------	------	---------	--------

#### snmpTargetParams Table:

Name	MP Model	User Name	Sec Model	Sec Level
------	----------	-----------	-----------	-----------

## info/sys/chassis

### BladeCenter Chassis Information

#### IBM BladeCenter Chassis Related Information:

```

Switch Module Bay           = 10
Chassis Type                 = BladeCenter H
Chassis UUID                 = 606FDAF9300C3C0DAEA20227E565C1DD
Accessible Bridge Modules   = 6 4
POST Results                 = 0xff

```

#### Management Module Control -

```

Default Configuration       = FALSE
Skip Extended Memory Test   = TRUE
Disable External Ports      = FALSE
POST Diagnostics Control    = Normal Diagnostics

```

```

Control Register            = 0x39
Extended Control Register    = 0x00

```

#### Management Module Status Reporting -

```

Device PowerUp Complete     = TRUE
Over Current Fault           = FALSE
Fault LED                    = OFF
Primary Temperature Warning   = OK
Secondary Temperature Warning = OK

```

```

Status Register              = 0x40
Extended Status Register      = 0x01

```

Chassis information includes details about the chassis type and position, and management module settings.

## /info/sys/general

### General System Information

```

System Information at 0:16:42 Wed Jan 3, 2010
Time zone: America/US/Pacific
Daylight Savings Time Status: Disabled

BNT Virtual Fabric 10Gb Switch Module for IBM BladeCenter

Switch has been up 5 days, 2 hours, 16 minutes and 42 seconds.
Last boot: 0:00:47 Wed Jan 3, 2010 (reset from console)

MAC Address: 00:22:00:7d:71:00 Management IP Address (if 128): 12.31.30.128
Software Version 6.3.0 (FLASH image1), factory default configuration.

PCBA Part Number:      BAC-00042-00
Hardware Part Number:  46C7193
FAB Number:           BN-RZZ000
Serial Number:        PROTO2C04E
Manufacturing Date:    43/08
Hardware Revision:     0
Board Revision:        1
PLD Firmware Version:  4.0

Temperature Sensor 1 (Warning): 42.0 C (Warn at 88.0 C/Recover at 78.0 C)
Temperature Sensor 2 (Shutdown): 42.5 C (Shutdown at 98.0 C/Recover at 88.0 C)
Temperature Sensor 3 (Exhaust): 37.5 C
Temperature Sensor 4 (Inlet):   32.5 C

Switch is in I/O Module Bay 10

```

---

**Note** – The display of temperature will come up only if the temperature of any of the sensors exceeds the temperature threshold. There will be a warning from the software if any of the sensors exceeds this temperature threshold. The switch will shut down if the power supply overheats.

---

System information includes:

- System date and time
- Switch model
- Switch name and location
- Time of last boot
- MAC address of the switch management processor
- Software image file and version number, and configuration name.
- IP address of the management interface
- Hardware version and part number
- Log-in banner, if one is configured



## `/info/sys/log` Show Recent Syslog Messages

Date	Time	Criticality level	Message
Jul 8	17:25:41	NOTICE	system: link up on port INT1
Jul 8	17:25:41	NOTICE	system: link up on port INT8
Jul 8	17:25:41	NOTICE	system: link up on port INT7
Jul 8	17:25:41	NOTICE	system: link up on port INT2
Jul 8	17:25:41	NOTICE	system: link up on port INT1
Jul 8	17:25:41	NOTICE	system: link up on port INT4
Jul 8	17:25:41	NOTICE	system: link up on port INT3
Jul 8	17:25:41	NOTICE	system: link up on port INT6
Jul 8	17:25:41	NOTICE	system: link up on port INT5
Jul 8	17:25:41	NOTICE	system: link up on port EXT4
Jul 8	17:25:41	NOTICE	system: link up on port EXT1
Jul 8	17:25:41	NOTICE	system: link up on port EXT3
Jul 8	17:25:41	NOTICE	system: link up on port EXT2
Jul 8	17:25:41	NOTICE	system: link up on port INT3
Jul 8	17:25:42	NOTICE	system: link up on port INT2
Jul 8	17:25:42	NOTICE	system: link up on port INT4
Jul 8	17:25:42	NOTICE	system: link up on port INT3
Jul 8	17:25:42	NOTICE	system: link up on port INT6
Jul 8	17:25:42	NOTICE	system: link up on port INT5
Jul 8	17:25:42	NOTICE	system: link up on port INT1
Jul 8	17:25:42	NOTICE	system: link up on port INT6

Each syslog message has a criticality level associated with it, included in text form as a prefix to the log message. One of eight different prefixes is used, depending on the condition that the administrator is being notified of, as shown below.

- EMERG: indicates the system is unusable
- ALERT: Indicates action should be taken immediately
- CRIT: Indicates critical conditions
- ERR: indicates error conditions or errored operations
- WARNING: indicates warning conditions
- NOTICE: indicates a normal but significant condition
- INFO: indicates an information message
- DEBUG: indicates a debug-level message

## `/info/sys/user` User Status Information

```
Username:
  user      - enabled - offline
  oper      - disabled - offline
  admin     - Always Enabled - online 1 session
Current User ID table:
  1: name paul      , dis, cos user      , password valid, offline
Current strong password settings:
  strong password status: disabled
```

This command displays the status of the configured usernames.

/info/stack

# Stacking Information Menu

---

[Stacking Menu]

switch

- Show switch information

link

- Show stack link information

name

- Show stack name

backup

- Show backup unit number

vers

- Show switch firmware information

path

- Show inter switch packet path map

pushstat

- Show config/image push status information

dump

- Dump all stacking information

Table 18 lists the Stacking information menu options.

Table 18 Stacking information Menu Options (/info/stack)

---

Command Syntax and Usage

---

**switch**

Displays information about each switch in the stack, including:

- ☐ Configured Switch Number (csnum)
- ☐ Attached Switch Number (asnum)
- ☐ MAC address
- ☐ Stacking state

---

**link**

Displays link information for each switch in the stack, listed by assigned switch number.

---

**name**

Displays the name of the stack.

---

**backup**

Displays the unit number of the backup switch.

---

**vers**

Displays the firmware version number for the selected switch.

---

**path**

Displays the Stacking packet path map that shows how the stack switches are connected.

---

**Table 18** Stacking information Menu Options (/info/stack)

Command Syntax and Usage	
<b>pushstat</b>	Displays the status of the most recent firmware and configuration file push from the master to member switches.
<b>dump</b>	Displays all stacking information.

`/info/stack/switch`  
**Stacking Switch Information**

```
Stack name: MyStack
Local switch is the master.

Local switch:
  csnum          - 1
  MAC            - 00:25:03:1c:96:00
  Switch Type    - 9
  Switch Mode (cfg) - Master
  Priority        - 225
  Stack MAC      - 00:25:03:1c:96:1f

Master switch:
  csnum          - 1
  MAC            - 00:25:03:1c:96:00

Backup switch:
  csnum          - 2
  MAC            - 00:ef:61:79:00:00

Configured Switches:
-----
csnum          MAC          asnum
-----
C1      00:25:03:1c:96:00    A1
C2      00:ef:61:79:00:00    A2

Attached Switches in Stack:
-----
asnum          MAC          csnum  State
-----
A1      00:25:03:1c:96:00    C1    IN_STACK
A2      00:ef:61:79:00:00    C2    IN_STACK
```

Stack switch information includes the following:

- Stack name
- Details about the local switch from which the command was issued
- Configured switch number and MAC of the Stack Master and Stack Backup
- Configured switch numbers and their associated assigned switch numbers
- Attached switch numbers and their associated configured switch numbers

/info/l2

# Layer 2 Information Menu

[Layer 2 Menu]	
amp	- Active Multipath Information Menu
fdb	- Forwarding Database Information Menu
lacp	- Link Aggregation Control Protocol Menu
failovr	- Show Failover information
hotlink	- Show Hot Links information
lldp	- LLDP Information Menu
udld	- UDLD Information Menu
oam	- OAM Information Menu
8021x	- Show 802.1X information
stg	- Show STP information
cist	- Show CIST information
trunk	- Show Trunk Group information
vlan	- Show VLAN information
pvlan	- Show protocol VLAN information
prvlan	- Show private-vlan information
dump	- Dump all layer 2 information

The information provided by each menu option is briefly described in [Table 19](#), with pointers to where detailed information can be found.

**Table 19** Layer 2 Information Menu Options (/info/l2)

**Command Syntax and Usage**

**amp**

Displays the Active MultiPath (AMP) Information menu. For details, see [page 73](#).

**fdb**

Displays the Forwarding Database Information Menu. For details, see [page 76](#).

**lacp**

Displays the Link Aggregation Control Protocol Menu. For details, see [page 78](#).

**failovr**

Displays the Layer 2 Failover Information menu. For details, see [page 80](#).

**hotlink**

Displays the Hot Links Information menu. For details, see [page 81](#).

**lldp**

Displays the LLDP Information menu. For details, see [page 82](#).

**Table 19** Layer 2 Information Menu Options (/info/l2)

---

**Command Syntax and Usage**

---

**udld**

Displays the Unidirectional Link Detection (UDLD) Information menu. For details, see [page 84](#).

---

**oam**

Displays the Operation, Administration, and Maintenance (OAM) Information menu. For details, see [page 85](#).

---

**8021x**

Displays the 802.1X Information Menu. For details, see [page 86](#).

---

**stg**

Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (STP/PVST+, RSTP, PVRST, or MSTP), and VLAN membership.

In addition to seeing if STG is enabled or disabled, you can view the following STG bridge information:

- ☐ Priority
- ☐ Hello interval
- ☐ Maximum age value
- ☐ Forwarding delay
- ☐ Aging time

You can also see the following port-specific STG information:

- ☐ Port alias and priority
- ☐ Cost
- ☐ State
- ☐ Port Fast Forwarding state

For details, see [page 88](#).

---

**Table 19** Layer 2 Information Menu Options (/info/l2)

---

**Command Syntax and Usage**

---

**cist**

Displays Common Internal Spanning Tree (CIST) information, including the MSTP digest and VLAN membership.

CIST bridge information includes:

- ☐ Priority
- ☐ Hello interval
- ☐ Maximum age value
- ☐ Forwarding delay
- ☐ Root bridge information (priority, MAC address, path cost, root port)

CIST port information includes:

- ☐ Port number and priority
- ☐ Cost
- ☐ State

For details, see [page 94](#).

---

**trunk**

When trunk groups are configured, you can view the state of each port in the various trunk groups. For details, see [page 96](#).

---

**vlan**

Displays VLAN configuration information, including:

- ☐ VLAN Number
- ☐ VLAN Name
- ☐ Status
- ☐ Port membership of the VLAN
- ☐ VLAN management status

For details, see [page 97](#).

---

**pvlan**

Displays Protocol VLAN information.

---



**Table 19** Layer 2 Information Menu Options (/info/l2)

---

**Command Syntax and Usage**

---

**prvlan**

Displays Private VLAN information.

---

**dump**

Dumps all switch information available from the Layer 2 menu (10K or more, depending on your configuration).

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

---

**/info/l2/amp**  
**Active MultiPath Information**

```
[AMP Information Menu]
global    - Show global AMP information
group     - Show AMP group information
```

Use these commands to display Active MultiPath Protocol (AMP) information for the switch.

**Table 20** AMP Information Options

---

**Command Syntax and Usage**

---

**global**

Displays global Active MultiPath (AMP) information.

---

**group**

Displays AMP group information.

---

## /info/12/amp/global

### Show AMP Global Information

```

Active Multipath Protocol: enabled
      Protocol version   : 2
      Switch id          : 00:18:b1:a1:ae:00
      Switch type         : access
      Switch priority     : 255
      Packet interval    : 50 centiseconds
      Timeout count       : 4
      No. of groups       : 1

```

```

Group  State  Ports
-----
1      up      EXT1
              EXT2

```

```

Port    State  Trunk
-----
EXT1    fwd
EXT2    fwd

```

This displays show global AMP information for an AMP access switch. AMP global information includes the following:

- Active MultiPath Protocol information:
  - ☐ AMP status (enabled or disabled)
  - ☐ Protocol version
  - ☐ Switch ID (MAC address)
  - ☐ Switch type (access or aggregator)
  - ☐ Priority
  - ☐ Interval between AMP keep-alive packets
  - ☐ Timeout count
  - ☐ Number of active (enabled) AMP groups
- Group information
  - ☐ Group number
  - ☐ Group state (up or DOWN)
  - ☐ Ports/portchannels in the group
- Link information
  - ☐ Port number
  - ☐ State (fwd, BLOCK, or DOWN)
  - ☐ Portchannel (trunk) number

## `/info/12/amp/group <AMP group number>` Show AMP Group Information

```

Group 3: enabled, topology UP
  Port EXT1: access
    State : forwarding
    Peer  : 00:22:00:ac:d7:00
            aggregator, priority 100
  Port EXT2: access
    State : forwarding
    Peer  : 00:25:03:49:82:00
            aggregator, priority 1

```

This display shows AMP group information for an AMP access switch. AMP group information includes the following:

- AMP group number and topology status (UP or DOWN)
- AMP link 1:
  - Switch type (access/aggregator)
  - State (forwarding, BLOCKING, or DOWN)
  - Peer information (MAC address, switch type, AMP priority)
- AMP link 2:
  - Switch type (access/aggregator)
  - State (forwarding, BLOCKING, or DOWN)
  - Peer information (MAC address, switch type, AMP priority)

/info/12/fdb

## FDB Information Menu

[Forwarding Database Menu]

find

- Show a single FDB entry by MAC address

port

- Show FDB entries on a single port

trunk

- Show FDB entries on a single trunk

vlan

- Show FDB entries on a single VLAN

state

- Show FDB entries by state

mcdump

- Show FDB multicast entries

dump

- Show all FDB entries

The forwarding database (FDB) contains information that maps the media access control (MAC) address of each known device to the switch port where the device address was learned. The FDB also shows which other ports have seen frames destined for a particular MAC address.

**Note** – The master forwarding database supports up to 16K MAC address entries on the MP per switch.

**Table 21** FDB Information Menu Options (/info/12/fdb)

Command Syntax and Usage

**find** <MAC address> [*<VLAN>*]

Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, xx:xx:xx:xx:xx:xx. For example, 08:00:20:12:34:56

You can also enter the MAC address using the format, xxxxxxxxxxxx. For example, 080020123456

**port** <port number or alias>

Displays all FDB entries for a particular port.

**trunk** <trunk number>

Displays all FDB entries for a particular trunk.

**vlan** <VLAN number>

Displays all FDB entries on a single VLAN.

**state** **unknown** | **forward** | **trunk**

Displays all FDB entries of a particular state.

Table 21 FDB Information Menu Options (/info/12/fdb)

Command Syntax and Usage

**mcdump**

Displays all Multicast MAC entries in the FDB.

**dump**

Displays all entries in the Forwarding Database. For more information, see [page 77](#).

**/info/12/fdb/dump**  
Show All FDB Information

MAC address	VLAN	Port	Trnk	State	Permanent
00:04:38:90:54:18	1	EXT4		FWD	
00:09:6b:9b:01:5f	1	INT13		FWD	
00:09:6b:ca:26:ef	4095	MGT1		FWD	
00:0f:06:ec:3b:00	4095	MGT1		FWD	
00:11:43:c4:79:83	1	EXT4		FWD	P

An address that is in the forwarding (FWD) state, means that it has been learned by the switch. When in the trunking (TRK) state, the port field represents the trunk group number. If the state for the port is listed as unknown (UNK), the MAC address has not yet been learned by the switch, but has only been seen as a destination address.

When an address is in the unknown state, no outbound port is indicated, although ports which reference the address as a destination will be listed under “Reference ports.”

*Clearing Entries from the Forwarding Database*

To clear the entire FDB, refer to “[Forwarding Database Maintenance Menu](#)” on [page 512](#).

`/info/l2/lacp`  
**Link Aggregation Control Protocol Information Menu**

[LACP Menu]	
aggr	- Show LACP aggregator information for the port
port	- Show LACP port information
dump	- Show all LACP ports information

Use these commands to display Link Aggregation Protocol (LACP) status information about each port on the switch.

**Table 22** LACP Menu Options (`/info/l2/lacp`)

---

**Command Syntax and Usage**

---

**aggr** *<port alias or number>*

Displays detailed information about the LACP aggregator used by the selected port.

---

**port**

Displays LACP information about the selected port.

---

**dump**

Displays a summary of LACP information. For details, see [page 79](#).

---

`/info/12/lacp/dump`  
Show All LACP Information

port	mode	adminkey	operkey	selected	prio	aggr	trunk	status
INT1	active	30	30	yes	32768	17	19	up
INT2	active	30	30	yes	32768	17	19	up
INT3	off	3	3	no	32768	--	--	--
INT4	off	4	4	no	32768	--	--	--
...								

LACP dump includes the following information for each external port in the VFSM:

- `mode`                Displays the port’s LACP mode (active, passive, or off).
- `adminkey`            Displays the value of the port’s *adminkey*.
- `operkey`             Shows the value of the port’s operational key.
- `selected`            Indicates whether the port has been selected to be part of a Link Aggregation Group.
- `prio`                 Shows the value of the port priority.
- `aggr`                Displays the aggregator associated with each port.
- `trunk`                This value represents the LACP trunk group number.
- `status`              Displays the status of LACP on the port (up or down).

`/info/l2/failovr`  
**Layer 2 Failover Information Menu**

[Failover Info Menu]

trigger - Show Trigger information

**Table 23** describes the Layer 2 Failover information options.

**Table 23** Failover Menu Options (`/info/l2/failovr`)

**Command Syntax and Usage**

**trigger** *<trigger number>*

Displays detailed information about the selected Layer 2 Failover trigger.

`/info/l2/failovr/trigger` *<trigger number>*  
**Show Layer 2 Failover Information**

Trigger 1 Auto Monitor: Enabled

Trigger 1 limit: 0

Monitor State: Up

Member

Status

-----

-----

trunk 1

EXT2            Operational

EXT3            Operational

Control State: Auto Disabled

Member

Status

-----

-----

INT1            Operational

INT2            Operational

INT3            Operational

INT4            Operational

...

A monitor port's Failover status is `Operational` only if all the following conditions hold true:

- Port link is up.
- If Spanning-Tree is enabled, the port is in the `Forwarding` state.
- If the port is a member of an LACP trunk group, the port is aggregated.

If any of the above conditions are not true, the monitor port is considered to be failed.



A control port is considered to be operational if the monitor trigger state is Up. Even if a port's link status is Down, Spanning-Tree status is Blocking, and the LACP status is Not Aggregated, from a teaming perspective the port status is Operational, since the trigger is Up.

A control port's status is displayed as Failed only if the monitor trigger state is Down.

**/info/12/hotlink**  
**Hot Links Information Menu**

[Hot Links Info Menu]

trigger - Show Trigger information

**Table 24** Hot Links Menu Options (/info/12/hotlink)

**Command Syntax and Usage**

**trigger**

Displays status and configuration information for each Hot Links trigger.  
To view a sample display, see [page 81](#).

**/info/12/hotlink/trigger**  
**Hotlinks Trigger Information**

Hot Links Info: Trigger

Current global Hot Links setting: ON  
bpdu disabled  
sndfdb disabled

Current Trigger 1 setting: enabled  
name "Trigger 1", preempt enabled, fdelay 1 sec

Active state: None

Master settings:  
port EXT1

Backup settings:  
port EXT2

Hot Links trigger information includes the following:

- Hot Links status (on or off)
- Status of BPDU flood option
- Status of FDB send option
- Status and configuration of each Hot Links trigger

/info/12/lldp  
LLDP Information Menu

[LLDP Information Menu]	
port	- Show LLDP port information
rx	- Show LLDP receive state machine information
tx	- Show LLDP transmit state machine information
remodev	- Show LLDP remote devices information
dump	- Show all LLDP information

Table 25 LLDP Information Menu Options (/info/12/lldp)

Command Syntax and Usage

**port** *<port alias or number>*

Displays Link Layer Discovery Protocol (LLDP) port information.

**rx**

Displays information about the LLDP receive state machine.

**tx**

Displays information about the LLDP transmit state machine.

**remodev**

Displays information received from LLDP -capable devices. To view a sample display, see [page 83](#).

**dump**

Displays all LLDP information.

`/info/12/lldp/remodev`  
LLDP Remote Device Information

LLDP Remote Devices Information				
LocalPort	Index	Remote Chassis ID	RemotePort	Remote System Name
MGT	210	00 16 ca ff 7e 00	15	BNT Gb Ethernet Switch...
EXT4	12	00 16 60 f9 3b 00	20	BNT Gb Ethernet Switch...

LLDP remote device information provides a summary of information about remote devices connected to the switch. To view detailed information about a device, as shown below, follow the **remodev** command with the index number of the remote device.

Local Port Alias: EXT1	
Remote Device Index	: 15
Remote Device TTL	: 99
Remote Device RxChanges	: false
Chassis Type	: Mac Address
Chassis Id	: 00-18-b1-33-1d-00
Port Type	: Locally Assigned
Port Id	: 23
Port Description	: EXT1
System Name	:
System Description	:
System Capabilities Supported	: bridge, router
System Capabilities Enabled	: bridge, router
Remote Management Address:	
Subtype	: IPv4
Address	: 10.100.120.181
Interface Subtype	: ifIndex
Interface Number	: 128
Object Identifier	:

/info/12/udld

## Unidirectional Link Detection Information Menu

[UDLD Information Menu]

port - Show UDLD port information

dump - Show all UDLD information

Table 26 UDLD Information Menu Options (/info/12/udld)

Command Syntax and Usage

**port** <port alias or number>

Displays UDLD information about the selected port. To view a sample display, see [page 84](#).

**dump**

Displays all UDLD information.

/info/12/udld/port <port alias or number>

### UDLD Port Information

UDLD information on port EXT1

Port enable administrative configuration setting: Enabled

Port administrative mode: normal

Port enable operational state: link up

Port operational state: advertisement

Port bidirectional status: bidirectional

Message interval: 15

Time out interval: 5

Neighbor cache: 1 neighbor detected

Entry #1

Expiration time: 31 seconds

Device Name:

Device ID: 00:da:c0:00:04:00

Port ID: EXT1

UDLD information includes the following:

- Status (enabled or disabled)
- Mode (normal or aggressive)
- Port state (link up or link down)
- Bi-directional status (unknown, unidirectional, bidirectional, TX-RX loop, neighbor mismatch)

`/info/l2/oam`  
**OAM Discovery Information Menu**

```
[OAM Information Menu]
port      - Show OAM port information
dump      - Show all OAM information
```

**Table 27** OAM Discovery Information Menu Options (`/info/l2/oam`)

**Command Syntax and Usage**

**port** *<port alias or number>*

Displays OAM information about the selected port. To view a sample display, see [page 85](#).

**dump**

Displays all OAM information.

`/info/l2/oam/port` *<port alias or number>*  
**OAM Port Information**

```
OAM information on port EXT1
State enabled
Mode active
Link up
Satisfied Yes
Evaluating No

Remote port information:
Mode active
MAC address 00:da:c0:00:04:00
Stable Yes
State valid Yes
Evaluating No
```

OAM port display shows information about the selected port and the peer to which the link is connected.

/info/12/8021x  
802.1X Information

System capability : Authenticator				
System status : disabled				
Protocol version : 1				
Port	Auth Mode	Auth Status	Authenticator PAE State	Backend Auth State
-----	-----	-----	-----	-----
INT1	force-auth	authorized	initialize	initialize
*INT2	force-auth	authorized	initialize	initialize
*INT3	force-auth	authorized	initialize	initialize
*INT4	force-auth	authorized	initialize	initialize
*INT5	force-auth	authorized	initialize	initialize
*INT6	force-auth	authorized	initialize	initialize
*INT7	force-auth	authorized	initialize	initialize
*INT8	force-auth	authorized	initialize	initialize
INT9	force-auth	authorized	initialize	initialize
INT10	force-auth	authorized	initialize	initialize
*INT11	force-auth	authorized	initialize	initialize
*INT12	force-auth	authorized	initialize	initialize
*INT13	force-auth	authorized	initialize	initialize
*INT14	force-auth	authorized	initialize	initialize
*MGT1	force-auth	authorized	initialize	initialize
*MGT2	force-auth	authorized	initialize	initialize
*EXT1	force-auth	unauthorized	initialize	initialize
*EXT2	force-auth	unauthorized	initialize	initialize
*EXT3	force-auth	unauthorized	initialize	initialize
*EXT4	force-auth	unauthorized	initialize	initialize
...				
-----				
* - Port down or disabled				

**Note** – The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

The following table describes the IEEE 802.1X parameters.

**Table 28** 802.1X Parameter Descriptions (/info/l2/8021x)

Parameter	Description
Port	Displays each port's alias.
Auth Mode	Displays the Access Control authorization mode for the port. The Authorization mode can be one of the following: <ul style="list-style-type: none"> <li>■ force-unauth</li> <li>■ auto</li> <li>■ force-auth</li> </ul>
Auth Status	Displays the current authorization status of the port, either authorized or unauthorized.
Authenticator PAE State	Displays the Authenticator Port Access Entity State. The PAE state can be one of the following: <ul style="list-style-type: none"> <li>■ initialize</li> <li>■ disconnected</li> <li>■ connecting</li> <li>■ authenticating</li> <li>■ authenticated</li> <li>■ aborting</li> <li>■ held</li> <li>■ forceAuth</li> </ul>
Backend Auth State	Displays the Backend Authorization State. The Backend Authorization state can be one of the following: <ul style="list-style-type: none"> <li>■ initialize</li> <li>■ request</li> <li>■ response</li> <li>■ success</li> <li>■ fail</li> <li>■ timeout</li> <li>■ idle</li> </ul>

/info/12/stg  
Spanning Tree Information

```

-----
upfast disabled, update 40
Pvst+ compatibility mode enabled
-----

Spanning Tree Group 1: On (STP/PVST+)
VLANs: 1

Current Root:                Path-Cost  Port Hello MaxAge FwdDel
ffff 00:13:0a:4f:7d:d0      0      EXT2    2    20    15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              65535    2      20      15      300

Port Priority Cost FastFwd   State           Designated Bridge  Des Port
-----
INT1      0      0      n  FORWARDING    *
INT2      0      0      n  FORWARDING    *
INT3      0      0      n  FORWARDING    *
INT4      0      0      n  FORWARDING    *
INT5      0      0      n  FORWARDING    *
INT6      0      0      n  FORWARDING    *
INT7      0      0      n  FORWARDING    *
INT8      0      0      n  FORWARDING    *
INT9      0      0      n  DISABLED      *
INT10     0      0      n  FORWARDING    *
INT11     0      0      n  FORWARDING    *
INT12     0      0      n  FORWARDING    *
INT13     0      0      n  FORWARDING    *
INT14     0      0      n  FORWARDING    *
EXT1     128     2      n  DISABLED
EXT2     128     2      n  DISABLED
EXT3     128     2      n  FORWARDING    ffff-00:13:0a:4f:7d:d0  8011
EXT4     128     4!     n  FORWARDING    ffff-00:22:00:7d:71:00  8017
EXT5     128     2      n  DISABLED
...
* = STP turned off for this port.
! = Automatic path cost.

```

**Note** – The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.



The switch software uses the IEEE 802.1D Spanning Tree Protocol (STP). If IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), or Per VLAN Rapid Spanning Tree Protocol (PVRST) are turned on, see [“RSTP/MSTP Information” on page 91](#).

When STP is used, in addition to seeing if STG is enabled or disabled, you can view the following STG bridge information:

**Table 29** Spanning Tree Parameter Descriptions

Parameter	Description
Current Root	The Current Root shows information about the root bridge for the Spanning Tree. Information includes the priority (in hexadecimal notation) and MAC address of the root.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STG root bridge.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STG network.
FwdDel	The Forward Delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from listening to learning and from learning state to forwarding state.
Aging	The aging time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.
Priority (port)	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
FastFwd	The FastFwd shows whether the port is in Fast Forwarding mode or not, which permits the port that participates in Spanning Tree to bypass the Listening and Learning states and enter directly into the Forwarding state.

**Table 29** Spanning Tree Parameter Descriptions (continued)

Parameter	Description
State	The state field shows the current state of the port. The state field can be BLOCKING, LISTENING, LEARNING, FORWARDING, or DISABLED.
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The identifier of the port on the Designated Bridge to which this port is connected.

/info/l2/stg  
RSTP/MSTP Information

Spanning Tree Group 1: On (RSTP)						
VLANs: 1						
Current Root:						
ffff 00:13:0a:4f:7d:d0	Path-Cost	Port	Hello	MaxAge	FwdDel	
	0	EXT4	2	20	15	
Parameters:						
Priority	Hello	MaxAge	FwdDel	Aging		
61440	2	20	15	300		
Port	Prio	Cost	State	Role	Designated Bridge	Des Port Type
-----	-----	-----	-----	-----	-----	-----
INT1	0	0	DSB *			
INT2	0	0	DSB *			
INT3	0	0	FWD *			
INT4	0	0	DSB *			
INT5	0	0	DSB *			
INT6	0	0	DSB *			
INT7	0	0	DSB *			
INT8	0	0	DSB *			
INT9	0	0	DSB *			
INT10	0	0	DSB *			
INT11	0	0	DSB *			
INT12	0	0	DSB *			
INT13	0	0	DSB *			
INT14	0	0	DSB *			
EXT1	128	2000	FWD	DESG	8000-00:11:58:ae:39:00	8011 P2P
EXT2	128	2000	DISC	BKUP	8000-00:11:58:ae:39:00	8011 P2P
EXT3	128	2000	FWD	DESG	8000-00:11:58:ae:39:00	8013 P2P
EXT4	128	20000	DISC	BKUP	8000-00:11:58:ae:39:00	8013 Shared
EXT5	128	2000	FWD			
...						
* = STP turned off for this port.						

**Note** – The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

The switch software can be set to use the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) or the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). If RSTP/MSTP is turned on (see [page 323](#)), you can view RSTP/MSTP bridge information for the Spanning Tree Group and port-specific RSTP information.

The following table describes the STP parameters in RSTP or MSTP mode.

**Table 30** RSTP/MSTP Parameter Descriptions

Parameter	Description
Current Root	The Current Root shows information about the root bridge for the Spanning Tree. Information includes the priority (in hexadecimal notation) and MAC address of the root.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network.
FwdDel	The Forward Delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from listening to learning and from learning state to forwarding state.
Aging	The aging time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.
Prio (port)	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
State	The State field shows the current state of the port. The State field in RSTP or MSTP mode can be one of the following: Discarding (DISC), Learning (LRN), Forwarding (FWD), or Disabled (DSB).
Role	The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP), Disabled (DSB), Master (MAST).

**Table 30** RSTP/MSTP Parameter Descriptions (continued)

Parameter	Description
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The port ID of the port on the Designated Bridge to which this port is connected.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are <i>AUTO</i> , <i>P2P</i> , or <i>SHARED</i> .

/info/l2/cist  
Common Internal Spanning Tree Information

Common Internal Spanning Tree: on									
VLANs: 2-4094									
Current Root: Path-Cost Port MaxAge FwdDel									
8000 00:11:58:ae:39:00 0 0 20 15									
Cist Regional Root: Path-Cost									
8000 00:11:58:ae:39:00 0									
Parameters: Priority MaxAge FwdDel Hops									
61440 20 15 20									
Port	Prio	Cost	State	Role	Designated	Bridge	Des	Port	Hello Type
-----									
INT1	0		0 DSB	*					
INT2	0		0 DSB	*					
INT3	0		0 FWD	*					
INT4	0		0 DSB	*					
INT5	0		0 DSB	*					
INT6	0		0 DSB	*					
INT7	0		0 DSB	*					
INT8	0		0 DSB	*					
INT9	0		0 DSB	*					
INT10	0		0 DSB	*					
INT11	0		0 DSB	*					
INT12	0		0 DSB	*					
INT13	0		0 DSB	*					
INT14	0		0 DSB	*					
MGT1	0		0 FWD	*					
MGT2	0		0 FWD						
*EXT1	128	20000	FWD	DESG	8000-00:11:58:ae:39:00	8011	2	P2P	
EXT2	128	20000	DISC	BKUP	8000-00:11:58:ae:39:00	8011	2	P2P	
EXT3	128	20000	FWD	DESG	8000-00:11:58:ae:39:00	8013	2	P2P	
EXT4	128	20000	DISC	BKUP	8000-00:11:58:ae:39:00	8013	2	Shared	
...									
* = STP turned off for this port.									

**Note** – The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

In addition to seeing if Common Internal Spanning Tree (CIST) is enabled or disabled, you can view CIST bridge and port-specific information. The following table describes the CIST parameters.

**Table 31** CIST Parameter Descriptions

Parameter	Description
CIST Root	The CIST Root shows information about the root bridge for the Common Internal Spanning Tree (CIST). Values on this row of information refer to the CIST root.
CIST Regional Root	The CIST Regional Root shows information about the root bridge for this MSTP region. Values on this row of information refer to the regional root.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STP network.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state.
Hops	The maximum number of bridge hops a packet can traverse before it is dropped. The default value is 20.
Priority (port)	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
State	The state field shows the current state of the port. The state field can be either Discarding (DISC), Learning (LRN), or Forwarding (FWD).

Table 31 CIST Parameter Descriptions

Parameter	Description
Role	The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP), Disabled (DSB), Master (MAST), or Unknown (UNK).
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The port ID of the port on the Designated Bridge to which this port is connected.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P, or SHARED.

/info/12/trunk

### Trunk Group Information

```
Trunk group 1: Enabled
Protocol - Static
Port state:
  EXT1: STG  1 forwarding
  EXT2: STG  1 forwarding
```

When trunk groups are configured, you can view the state of each port in the various trunk groups.

**Note –** If Spanning Tree Protocol on any port in the trunk group is set to *forwarding*, the remaining ports in the trunk group will also be set to *forwarding*.



/info/12/vlan  
VLAN Information

VLAN	Name	Status	MGT	Ports
1	Default VLAN	ena	dis	INT1-INT14 EXT1-EXT11
4095	Mgmt VLAN	ena	ena	INT1-INT14 MGT1 MGT2
Private-VLAN	Type	Mapped-To	Status	Ports
1000	primary	1001-1014	ena	EXT1 EXT2
1001	isolated	1000	ena	INT1
1002	community	1000	ena	INT2
1003	community	1000	ena	INT3

**Note –** The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

This information display includes all configured VLANs and all member ports that have an active link state. Port membership is represented in slot/port format.

VLAN information includes:

- VLAN Number
- VLAN Name
- Status
- Management status of the VLAN
- Port membership of the VLAN
- Protocol-based VLAN information, if applicable
- Private VLAN configuration, if applicable

[/info/l3](#)

## Layer 3 Information Menu

```
[Layer 3 Menu]
route      - IP Routing Information Menu
arp        - ARP Information Menu
bgp        - BGP Information Menu
ospf       - OSPF Routing Information Menu
ospf3      - OSPFv3 Routing Information Menu
rip        - RIP Routing Information Menu
route6     - IP6 Routing Information Menu
nbrcache   - IP6 Neighbor Cache Information Menu
ecmp       - Show ECMP static routes information
hash       - Show ECMP hashing result
igmp       - Show IGMP Snooping Multicast Group information
vrrp       - Show Virtual Router Redundancy Protocol information
if         - Show Interface information
ip         - Show IP information
dump       - Dump all layer 3 information
```

The information provided by each menu option is briefly described in [Table 32](#), with pointers to detailed information.

**Table 32** Layer 3 Menu Options ([/info/l3](#))

---

### Command Syntax and Usage

---

#### **route**

Displays the IP Routing Menu. Using the options of this menu, the system displays the following for each configured or learned route:

- ☐ Route destination IP address, subnet mask, and gateway address
- ☐ Type of route
- ☐ Tag indicating origin of route
- ☐ Metric for RIP tagged routes, specifying the number of hops to the destination (1-15 hops, or 16 for infinite hops)
- ☐ The IP interface that the route uses

For details, see [page 101](#).

---

#### **arp**

Displays the Address Resolution Protocol (ARP) Information Menu. For details, see [page 104](#).

---

#### **bgp**

Displays BGP Information Menu. To view menu options, see [page 106](#).

---

**Table 32** Layer 3 Menu Options (/info/l3)**Command Syntax and Usage****ospf**

Displays OSPF routing Information Menu. For details, see [page 108](#).

**ospf3**

Displays OSPFv3 routing Information Menu. For details, see [page 114](#).

**rip**

Displays Routing Information Protocol Menu. For details, see [page 120](#).

**route6**

Displays the IPv6 Routing information menu. To view menu options, see [page 122](#).

**nbrcache**

Displays the IPv6 Neighbor Discovery cache information menu. To view menu options, see [page 123](#).

**if**

Displays interface information. For details, see [page 124](#).

**ecmp**

Displays information about ECMP static routes. For details, see [page 125](#).

**hash** *<Source IP address> <number of ECMP paths>*

Displays information about ECMP hashing results. For details, see [page 125](#).

**ip**

Displays IP Information. For details, see [page 126](#).

IP information, includes:

- ❑ IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status.
- ❑ Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status
- ❑ IP forwarding settings, network filter settings, route map settings

**igmp**

Displays IGMP Information Menu. For details, see [page 127](#).

**Table 32** Layer 3 Menu Options (/info/l3)

---

**Command Syntax and Usage**

---

**vrrp**

Displays VRRP Information. For details, see [page 130](#).

---

**if**

Displays interface information. For details, see [page 124](#).

---

**ip**

Displays IP Information. For details, see [page 126](#).

IP information, includes:

- ☐ IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status.
  - ☐ Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status
  - ☐ IP forwarding settings, network filter settings, route map settings
- 

**dump**

Dumps all switch information available from the Layer 3 Menu (10K or more, depending on your configuration).

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

---

/info/l3/route  
IP Routing Information Menu

[IP Routing Menu]	
find	- Show a single route by destination IP address
gw	- Show routes to a single gateway
type	- Show routes of a single type
tag	- Show routes of a single tag
if	- Show routes on a single interface
dump	- Show all routes

Using the commands listed below, you can display all or a portion of the IP routes currently held in the switch.

**Table 33** Route Information Menu Options (/info/l3/route)

<b>Command Syntax and Usage</b>	
<b>find</b> <IP address (such as 192.4.17.101)>	
Displays a single route by destination IP address.	
<b>gw</b> <default gateway address (such as 192.4.17.44)>	
Displays routes to a single gateway.	
<b>type</b> indirect   direct   local   broadcast   martian   multicast	
Displays routes of a single type. For a description of IP routing types, see <a href="#">Table 34 on page 102</a> .	
<b>tag</b> fixed   static   addr   rip   ospf   bgp   broadcast   martian   multicast	
Displays routes of a single tag. For a description of IP routing types, see <a href="#">Table 35 on page 103</a> .	
<b>if</b> <interface number>	
Displays routes on a single interface.	
<b>dump</b>	
Displays all routes configured in the switch. For more information, see <a href="#">page 102</a> .	

`/info/13/route/dump`  
Show All IP Route Information

Status code: * - best						
Destination	Mask	Gateway	Type	Tag	Metr	If
* 12.0.0.0	255.0.0.0	11.0.0.1	direct	fixed		128
* 12.0.0.1	255.255.255.255	11.0.0.1	local	addr		128
* 12.255.255.255	255.255.255.255	11.255.255.255	broadcast	broadcast		128
* 12.0.0.0	255.0.0.0	12.0.0.1	direct	fixed		12
* 12.0.0.1	255.255.255.255	12.0.0.1	local	addr		12
* 255.255.255.255	255.255.255.255	12.255.255.255	broadcast	broadcast		2
* 224.0.0.0	224.0.0.0	0.0.0.0	martian	martian		
* 224.0.0.5	255.255.255.255	0.0.0.0	multicast	addr		

The following table describes the `Type` parameters.

**Table 34** IP Routing Type Parameters

Parameter	Description
indirect	The next hop to the host or subnet destination will be forwarded through a router at the <code>Gateway</code> address.
direct	Packets will be delivered to a destination host or subnet attached to the switch.
local	Indicates a route to one of the switch's IP interfaces.
broadcast	Indicates a broadcast route.
martian	The destination belongs to a host or subnet which is filtered out. Packets to this destination are discarded.
multicast	Indicates a multicast route.

The following table describes the `Tag` parameters.

**Table 35** IP Routing Tag Parameters

Parameter	Description
fixed	The address belongs to a host or subnet attached to the switch.
static	The address is a static route which has been configured on the VFSM.
addr	The address belongs to one of the switch's IP interfaces.
rip	The address was learned by the Routing Information Protocol (RIP).
ospf	The address was learned by Open Shortest Path First (OSPF).
bgp	The address was learned via Border Gateway Protocol (BGP)
broadcast	Indicates a broadcast address.
martian	The address belongs to a filtered group.
multicast	Indicates a multicast address.

/info/13/arp  
ARP Information Menu

[Address Resolution Protocol Menu]

find

- Show a single ARP entry by IP address

port

- Show ARP entries on a single port

vlan

- Show ARP entries on a single VLAN

addr

- Show ARP address list

dump

- Show all ARP entries

The ARP information includes IP address and MAC address of each entry, address status flags (see [Table 36 on page 104](#)), VLAN and port for the address, and port referencing information.

Table 36 ARP Information Menu Options (/info/13/arp)

Command Syntax and Usage

**find** <IP address (such as, 192.4.17.101)>

Displays a single ARP entry by IP address.

**port** <port alias or number>

Displays the ARP entries on a single port.

**vlan** <VLAN number>

Displays the ARP entries on a single VLAN.

**addr**

Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags.

**dump**

Displays all ARP entries. including:

- ☐ IP address and MAC address of each entry
- ☐ Address status flag (see below)
- ☐ The VLAN and port to which the address belongs
- ☐ The ports which have referenced the address (empty if no port has routed traffic to the IP address shown)

For more information, see [page 105](#).



## `/info/13/arp/dump`

### Show All ARP Entry Information

IP address	Flags	MAC address	VLAN	Age	Port
12.20.1.1		00:15:40:07:20:42	4095	0	INT8
12.20.20.16		00:30:13:e3:44:14	4095	2	INT8
12.20.20.18		00:30:13:e3:44:14	4095	2	INT6
12.20.23.111		00:1f:29:95:f7:e5	4095	6	INT6

The Port field shows the target port of the ARP entry.

The Flag field is interpreted as follows:

**Table 37** ARP Dump Flag Parameters

Flag	Description
P	Permanent entry created for switch IP interface.
R	Indirect route entry.
U	Unresolved ARP entry. The MAC address has not been learned.

## `/info/13/arp/addr`

### ARP Address List Information

IP address	IP mask	MAC address	VLAN	Pass-Up
205.178.18.66	255.255.255.255	00:70:cf:03:20:04		
205.178.50.1	255.255.255.255	00:70:cf:03:20:06	1	
205.178.18.64	255.255.255.255	00:70:cf:03:20:05	1	

## /info/13/bgp

### BGP Information Menu

```
[BGP Menu]
peer      - Show all BGP peers
summary   - Show all BGP peers in summary
dump      - Show BGP routing table
```

**Table 38** BGP Peer Information Menu Options (/info/13/bgp)

---

#### Command Syntax and Usage

---

##### **peer**

Displays BGP peer information. See [page 106](#) for a sample output.

---

##### **summary**

Displays peer summary information such as AS, message received, message sent, up/down, state. See [page 107](#) for a sample output.

---

##### **dump**

Displays the BGP routing table. See [page 107](#) for a sample output.

---

## /info/13/bgp/peer

### BGP Peer Information

Following is an example of the information that /info/13/bgp/peer provides.

```
BGP Peer Information:

3: 2.1.1.1          , version 4, TTL 225
  Remote AS: 100, Local AS: 100, Link type: IBGP
  Remote router ID: 3.3.3.3,   Local router ID: 1.1.201.5
  BGP status: idle, Old status: idle
  Total received packets: 0, Total sent packets: 0
  Received updates: 0, Sent updates: 0
  Keepalive: 60, Holdtime: 180, MinAdvTime: 60
  LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)
  Established state transitions: 1

4: 2.1.1.4          , version 4, TTL 225
  Remote AS: 100, Local AS: 100, Link type: IBGP
  Remote router ID: 4.4.4.4,   Local router ID: 1.1.201.5
  BGP status: idle, Old status: idle
  Total received packets: 0, Total sent packets: 0
  Received updates: 0, Sent updates: 0
  Keepalive: 60, Holdtime: 180, MinAdvTime: 60
  LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)
  Established state transitions: 1
```

**/info/13/bgp/summary**  
BGP Summary Information

Following is an example of the information that /info/13/bgp/summary provides.

BGP Peer Summary Information:							
Peer	V	AS	MsgRcvd	MsgSent	Up/Down	State	
1: 205.178.23.142	4	142	113	121	00:00:28	established	
2: 205.178.15.148	0	148	0	0	never	connect	

**/info/13/bgp/dump**  
Show All BGP Information

Following is an example of the information that /info/13/bgp/dump provides.

```
>> BGP# dump
Status codes: * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Mask	Next Hop	Metr	LcPrf	Wght	Path
*> 1.1.1.0	255.255.255.0	0.0.0.0			0	?
*> 10.100.100.0	255.255.255.0	0.0.0.0			0	?
*> 10.100.120.0	255.255.255.0	0.0.0.0			0	?

```
The 13.0.0.0 is filtered out by rrmapp; or, a loop detected.
```

## /info/l3/ospf

### OSPF Information Menu

```
[OSPF Information Menu]
  general - Show general information
  aindex  - Show area(s) information
  if      - Show interface(s) information
  virtual - Show details of virtual links
  nbr     - Show neighbor(s) information
  dbase   - Database Menu
  sumaddr - Show summary address list
  nsumadd - Show NSSA summary address list
  routes  - Show OSPF routes
  dump    - Show OSPF information
```

**Table 39** OSPF Information Menu Options (/info/l3/ospf)

---

#### Command Syntax and Usage

---

##### **general**

Displays general OSPF information. See [page 110](#) for a sample output.

---

##### **aindex** <area index (0-2)>

Displays area information for a particular area index. If no parameter is supplied, it displays area information for all the areas.

---

##### **if** <interface number>

Displays interface information for a particular interface. If no parameter is supplied, it displays information for all the interfaces. See [page 110](#) for a sample output.

---

##### **virtual**

Displays information about all the configured virtual links.

---

##### **nbr** <nbr router-id (A.B.C.D)>

Displays the status of a neighbor with a particular router ID. If no router ID is supplied, it displays the information about all the current neighbors.

---

##### **dbase**

Displays OSPF database menu. To view menu options, see [page 111](#).

---

##### **sumaddr** <area index (0-2)>

Displays the list of summary ranges belonging to non-NSSA areas.

---

**Table 39** OSPF Information Menu Options (/info/l3/ospf)

---

**Command Syntax and Usage**

---

**nsumadd** *<area index (0-2)>*

Displays the list of summary ranges belonging to NSSA areas.

---

**routes**

Displays OSPF routing table. See [page 113](#) for a sample output.

---

**dump**

Displays the OSPF information.

---

## `/info/13/ospf/general` OSPF General Information

```

OSPF Version 2
Router ID: 10.10.10.1
Started at 1663 and the process uptime is 4626
Area Border Router: yes, AS Boundary Router: no
LS types supported are 6
External LSA count 0
External LSA checksum sum 0x0
Number of interfaces in this router is 2
Number of virtual links in this router is 1
16 new lsa received and 34 lsa originated from this router
Total number of entries in the LSDB 10
Database checksum sum 0x0
Total neighbors are 1, of which
                                2 are >=INIT state,
                                2 are >=EXCH state,
                                2 are =FULL state
Number of areas is 2, of which 3-transit 0-nssa
  Area Id : 0.0.0.0
  Authentication : none
  Import ASEextern : yes
  Number of times SPF ran : 8
  Area Border Router count : 2
  AS Boundary Router count : 0
  LSA count : 5
  LSA Checksum sum : 0x2237B
  Summary : noSummary

```

## `/info/13/ospf/if <interface number>` OSPF Interface Information

```

Ip Address 10.10.12.1, Area 0.0.0.1, Admin Status UP
Router ID 10.10.10.1, State DR, Priority 1
Designated Router (ID) 10.10.10.1, Ip Address 10.10.12.1
Backup Designated Router (ID) 10.10.14.1, Ip Address 10.10.12.2
Timer intervals, Hello 10, Dead 40, Wait 1663, Retransmit 5,
                Poll interval 0, Transit delay 1
Neighbor count is 1   If Events 4, Authentication type none

```

## /info/l3/ospf/dbase

### OSPF Database Information Menu

```
[OSPF Database Menu]
  advrtr  - LS Database info for an Advertising Router
  asbrsum - ASBR Summary LS Database info
  dbsumm  - LS Database summary
  ext     - External LS Database info
  nw      - Network LS Database info
  nssa    - NSSA External LS Database info
  rtr     - Router LS Database info
  self    - Self Originated LS Database info
  summ    - Network-Summary LS Database info
  all     - All
```

**Table 40** OSPF Database Information Menu Options (/info/l3/ospf/dbase)

---

#### Command Syntax and Usage

---

**advrtr** <router-id (A.B.C.D)>

Takes advertising router as a parameter. Displays all the Link State Advertisements (LSAs) in the LS database that have the advertising router with the specified router ID, for example: 20.1.1.1.

---

**asbrsum** <adv-rtr (A.B.C.D)> | <link\_state\_id (A.B.C.D)> | <self>

Displays ASBR summary LSAs. The usage of this command is as follows:

- ☐ `asbrsum adv-rtr 20.1.1.1`  
Displays ASBR summary LSAs having the advertising router 20.1.1.1.
- ☐ `asbrsum link-state-id 10.1.1.1`  
Displays ASBR summary LSAs having the link state ID 10.1.1.1.
- ☐ `asbrsum self`  
Displays the self advertised ASBR summary LSAs.
- ☐ `asbrsum` with no parameters displays all the ASBR summary LSAs.

---

**dbsumm**

Displays the following information about the LS database in a table format:

- ☐ Number of LSAs of each type in each area.
- ☐ Total number of LSAs for each area.
- ☐ Total number of LSAs for each LSA type for all areas combined.
- ☐ Total number of LSAs for all LSA types for all areas combined.

No parameters are required.

---

**Table 40** OSPF Database Information Menu Options (/info/l3/ospf/dbase)**Command Syntax and Usage**


---

**ext** <adv-rtr (A.B.C.D)> | <link\_state\_id (A.B.C.D)> | <self>

Displays the AS-external (type 5) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command `asbrsum`.

---

**nw** <adv-rtr (A.B.C.D)> | <link\_state\_id (A.B.C.D)> | <self>

Displays the network (type 2) LSAs with detailed information of each field of the LSA.network LS database. The usage of this command is the same as the usage of the command `asbrsum`.

---

**nssa** <adv-rtr (A.B.C.D)> | <link\_state\_id (A.B.C.D)> | <self>

Displays the NSSA (type 7) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command `asbrsum`.

---

**rtr** <adv-rtr (A.B.C.D)> | <link\_state\_id (A.B.C.D)> | <self>

Displays the router (type 1) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command `asbrsum`.

---

**self**

Displays all the self-advertised LSAs. No parameters are required.

---

**summ** <adv-rtr (A.B.C.D)> | <link\_state\_id (A.B.C.D)> | <self>

Displays the network summary (type 3) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command `asbrsum`.

---

**all**

Displays all the LSAs.

---



## `/info/13/ospf/routes` OSPF Route Codes Information

```
Codes: IA - OSPF inter area,  
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
       E1 - OSPF external type 1, E2 - OSPF external type 2  
IA 10.10.0.0/16 via 200.1.1.2  
IA 40.1.1.0/28 via 20.1.1.2  
IA 80.1.1.0/24 via 200.1.1.2  
IA 100.1.1.0/24 via 20.1.1.2  
IA 140.1.1.0/27 via 20.1.1.2  
IA 150.1.1.0/28 via 200.1.1.2  
E2 172.18.1.1/32 via 30.1.1.2  
E2 172.18.1.2/32 via 30.1.1.2  
E2 172.18.1.3/32 via 30.1.1.2  
E2 172.18.1.4/32 via 30.1.1.2  
E2 172.18.1.5/32 via 30.1.1.2  
E2 172.18.1.6/32 via 30.1.1.2  
E2 172.18.1.7/32 via 30.1.1.2  
E2 172.18.1.8/32 via 30.1.1.2
```

## /info/13/ospf3

### OSPFv3 Information Menu

```
[OSPFv3 Information Menu]
  aindex    - Show area database information Menu
  dbase     - Database Menu
  areas     - Show areas information
  if        - Show interface(s) information
  virtual   - Show details of virtual links
  nbr       - Show neighbor(s) information
  host      - Show host information
  reqlist   - Show request list
  retlist   - Show retransmission list
  sumaddr   - Show summary address information
  redist    - Show config applied to routes learnt from RTM
  ranges    - Show OSPFv3 summary ranges
  routes    - Show OSPFv3 routes
  borderrrt - Show OSPFv3 routes to an abr/asbr
  dump      - Show OSPFv3 information
```

**Table 41** OSPFv3 Information Menu Options (/info/13/ospf3)

---

#### Command Syntax and Usage

---

**aindex** *<area index (0-2)>*

Displays the area information menu for a particular area index. To view menu options, see [page 116](#).

---

**dbase**

Displays the OSPFv3 database menu. To view menu options, see [page 118](#).

---

**areas**

Displays the OSPFv3 Area Table.

---

**if** *<interface number>*

Displays interface information for a particular interface. If no parameter is supplied, it displays information for all the interfaces. To view a sample display, see [page 118](#).

---

**virtual**

Displays information about all the configured virtual links.

---

**nbr** *<nbr router-id (A.B.C.D)>*

Displays the status of a neighbor with a particular router ID. If no router ID is supplied, it displays the information about all the current neighbors.

---

**Table 41** OSPFv3 Information Menu Options (/info/l3/ospf3)

---

**Command Syntax and Usage**

---

**host**

Displays OSPFv3 host configuration information.

---

**reqlist** <*nbr router-id (A.B.C.D)*>

Displays the OSPFv3 request list. If no router ID is supplied, it displays the information about all the current neighbors.

---

**retlist** <*nbr router-id (A.B.C.D)*>

Displays the OSPFv3 retransmission list. If no router ID is supplied, it displays the information about all the current neighbors.

---

**sumaddr**

Displays the OSPFv3 external summary-address configuration information.

---

**redist**

Displays OSPFv3 redistribution information to be applied to routes learned from the route table.

---

**ranges**

Displays the OSPFv3 list of all area address ranges information.

---

**routes**

Displays OSPFv3 routing table. To view a sample display, see [page 120](#).

---

**borderrt**

Displays OSPFv3 routes to an ABR or ASBR.

---

**dump**

Displays all OSPFv3 information. To view a sample display, see [page 117](#).

---

## /info/l3/ospf3/aindex <0-2> OSPFv3 Area Index Information Menu

```
[Area Info Menu]
  asex    - External LS Database info
  interprf - Inter Area Prefix LS Database info
  interrtr - Inter Area Router LS Database info
  intrapr - Intra Area Prefix LS Database info
  link    - Link LS Database info
  network - Network LS Database info
  rtr     - Router LS Database info
  nssa    - NSSA LS Database info
  all     - All
```

The following commands allow you to display database information about the specified area.

**Table 42** OSPFv3 Area Index Information Options (/info/l3/ospf3/aindex)

---

### Command Syntax and Usage

---

#### **asext [detail|hex]**

Displays AS-External LSAs database information for the selected area. If no parameter is supplied, it displays condensed information.

---

#### **interprf [detail|hex]**

Displays Inter-Area Prefix LSAs database information for the selected area. If no parameter is supplied, it displays condensed information.

---

#### **interrtr [detail|hex]**

Displays Inter-Area router LSAs database information for the selected area. If no parameter is supplied, it displays condensed information.

---

#### **intraprf [detail|hex]**

Displays Intra-Area Prefix LSAs database information for the selected area. If no parameter is supplied, it displays condensed information.

---

#### **link [detail|hex]**

Displays Link LSAs database information for the selected area. If no parameter is supplied, it displays condensed information.

---

#### **network [detail|hex]**

Displays Network LSAs database information for the selected area. If no parameter is supplied, it displays condensed information.

---

Table 42 OSPFv3 Area Index Information Options (/info/l3/ospf3/aindex)

Command Syntax and Usage

rtr [detail|hex]

Displays the Router LSAs with detailed information of each field of the LSAs. If no parameter is supplied, it displays condensed information.

nssa [detail|hex]

Displays NSSA database information for the selected area. If no parameter is supplied, it displays condensed information.

all [detail|hex]

Displays all the LSAs for the selected area. If no parameter is supplied, it displays condensed information.

/info/l3/ospf3/dump  
OSPFv3 Information

```
Router Id: 1.0.0.1           ABR Type: Standard ABR
SPF schedule delay: 5 secs   Hold time between two SPFs: 10 secs
Exit Overflow Interval: 0    Ref BW: 100000           Ext Lsdb Limit: none
Trace Value: 0x00008000     As Scope Lsa: 2           Checksum Sum: 0xfe16
Passive Interface: Disable
Nssa Asbr Default Route Translation: Disable
Autonomous System Boundary Router
Redistributing External Routes from connected, metric 10, metric type
asExtType1, no tag set
Number of Areas in this router 1
                                Area 0.0.0.0
Number of interfaces in this area is 1
Number of Area Scope Lsa: 7     Checksum Sum: 0x28512
Number of Indication Lsa: 0     SPF algorithm executed: 2 times
```

## `/info/13/ospf3/if` *<interface number>* OSPFv3 Interface Information

### Ospf3 Interface Information

```

Interface Id: 1      Instance Id: 0      Area Id: 0.0.0.0
Local Address: fe80::222:ff:fe7d:5d00    Router Id: 1.0.0.1
Network Type: BROADCAST  Cost: 1        State: BACKUP

Designated Router Id: 2.0.0.2      local address:
fe80::218:b1ff:feal:6c01

Backup Designated Router Id: 1.0.0.1      local address:
fe80::222:ff:fe7d:5d00

Transmit Delay: 1 sec    Priority: 1      IfOptions: 0x0
Timer intervals configured:
Hello: 10,  Dead: 40,  Retransmit: 5
Hello due in 6 sec
Neighbor Count is: 1,  Adjacent neighbor count is: 1
Adjacent with neighbor 2.0.0.2

```

## `/info/13/ospf3/dbase` OSPFv3 Database Information Menu

```

[OSPFv3 Database Menu]
  asextr      - External LS Database info
  interprf    - Inter Area Prefix LS Database info
  interrtr    - Inter Area Router LS Database info
  intraprfr   - Intra Area Prefix LS Database info
  link        - Link LS Database info
  network     - Network LS Database info
  rtr         - Router LS Database info
  nssa        - NSSA LS Database info
  all         - All

```

**Table 43** OSPFv3 Database Information Options (/info/l3/ospf3/dbase)**Command Syntax and Usage****asext** *<detail>* | *<hex>*

Displays AS-External LSAs database information. If no parameter is supplied, it displays condensed information.

**interprf** *<detail>* | *<hex>*

Displays Inter-Area Prefix LSAs database information. If no parameter is supplied, it displays condensed information.

**interrtr** *<detail>* | *<hex>*

Displays Inter-Area router LSAs database information. If no parameter is supplied, it displays condensed information.

**intraprf** *<detail>* | *<hex>*

Displays Intra-Area Prefix LSAs database information. If no parameter is supplied, it displays condensed information.

**link** *<detail>* | *<hex>*

Displays Link LSAs database information. If no parameter is supplied, it displays condensed information.

**network** *<detail>* | *<hex>*

Displays Network LSAs database information. If no parameter is supplied, it displays condensed information.

**rtr** *<detail>* | *<hex>*

Displays the Router LSAs with detailed information of each field of the LSAs. If no parameter is supplied, it displays condensed information.

**nssa** *<detail>* | *<hex>*

Displays Type-7 (NSSA) LSA database information. If no parameter is supplied, it displays condensed information.

**all** *<detail>* | *<hex>*

Displays all the LSAs. If no parameter is supplied, it displays condensed information.

**/info/l3/ospf3/routes**  
OSPFv3 Route Codes Information

Dest/ Prefix-Length	NextHp/ IfIndex	Cost	Rt. Type	Area
3ffe::10:0:0:0 /80	fe80::290:69ff fe90:b4bf /vlan1	30	interArea	0.0.0.0
3ffe::20:0:0:0 /80	fe80::290:69ff fe90:b4bf /vlan1	20	interArea	0.0.0.0
3ffe::30:0:0:0 /80	:: /vlan2	10	intraArea	0.0.0.0
3ffe::60:0:0:6 /128	fe80::211:22ff fe33:4426 /vlan2	10	interArea	0.0.0.0

**/info/l3/rip**  
Routing Information Protocol Information Menu

[RIP Information Menu]	
routes	- Show RIP routes
dump	- Show RIP user's configuration

Use this menu to view information about the Routing Information Protocol (RIP) configuration and statistics.

**Table 44** RIP Information Menu Options (/info/l3/rip)

**Command Syntax and Usage**

**routes**

Displays RIP routes. For more information, see [page 121](#).

**dump** *<interface number or zero for all IFs>*

Displays RIP user's configuration. For more information, see [page 121](#).



## `/info/l3/rip/routes` RIP Routes Information

```
>> IP Routing# /info/l3/rip/routes

30.1.1.0/24 directly connected
3.0.0.0/8 via 30.1.1.11 metric 4
4.0.0.0/16 via 30.1.1.11 metric 16
10.0.0.0/8 via 30.1.1.2 metric 3
20.0.0.0/8 via 30.1.1.2 metric 2
```

This table contains all dynamic routes learned through RIP, including the routes that are undergoing garbage collection with metric = 16. This table does not contain locally configured static routes.

## `/info/l3/rip/dump <interface number>` Show RIP Interface Information

```
RIP USER CONFIGURATION :
  RIP on update 30
  RIP Interface 1 : 10.4.4.2,          enabled
  version 2, listen enabled, supply enabled, default none
  poison disabled, split horizon enabled, trigg enabled,
  mcast enabled, metric 1
  auth none, key none
```

[/info/13/route6](#)  
IPv6 Routing Information Menu

```
[IP6 Routing Menu]
  summ      - Show routes summary
  dump      - Show all routes
```

Table 45 describes the IPv6 Routing information options.

Table 45 IPv6 Routing information Menu Options ([/info/13/route6](#))

Command Syntax and Usage

**summ**

Displays a summary of IPv6 routing information, including inactive routes.

**dump**

Displays all IPv6 routing information. For more information, see [page 122](#).

[/info/13/route6/dump](#)  
IPv6 Routing Table Information

```
IPv6 Routing Table - 3 entries
Codes : C - Connected, S - Static

S   ::/0 [1/20]
      via 2001:2:3:4::1, Interface 2
C   2001:2:3:4::/64 [1/1]
      via ::, Interface 2
C   fe80::20f:6aff:feec:f701/128 [1/1]
      via ::, Interface 2
```

Note that the first number inside the brackets represents the metric and the second number represents the preference for the route.

`/info/13/nbrcache`  
IPv6 Neighbor Discovery Cache Information Menu

[IP6 Neighbor Discovery Protocol Menu]

find

- Show a single NBR Cache entry by IP address

port

- Show NBR Cache entries on a single port

vlan

- Show NBR Cache entries on a single VLAN

dump

- Show all NBR Cache entries

Table 46 describes IPv6 Neighbor Discovery cache information menu options.

Table 46 IPv6 Neighbor Discovery Cache information (/info/13/nbrcache)

Command Syntax and Usage

**find** *<IPv6 address>*

Shows a single Neighbor Discovery cache entry by IP address.

**port** *<port alias or number>*

Shows the Neighbor Discovery cache entries on a single port.

**vlan** *<VLAN number>*

Shows the Neighbor Discovery cache entries on a single VLAN.

**dump**

Shows all Neighbor Discovery cache entries.

For more information, see [page 123](#).

`/info/13/nbrcache/dump`  
IPv6 Neighbor Discovery Cache Information

IPv6 Address	Age	Link-layer Addr	State	IF	VLAN	Port
-----	---	-----	-----	---	---	---
2001:2:3:4::1	10	00:50:bf:b7:76:b0	Reachable	2	1	EXT1
fe80::250:bfff:feb7:76b0	0	00:50:bf:b7:76:b0	Stale	2	1	EXT2

## /info/l3/if

### Interface Information

```
Interface information:
  1: IP4 172.31.35.5      255.255.0.0  172.31.255.255,  vlan 1, up
  2: IP6 2002:0:0:0:0:0:5/64      , vlan 1, up
      fe80::213:aff:fe4f:7c01
  3: IP6 3003:0:0:0:0:0:5/64      , vlan 2, up
      fe80::213:aff:fe4f:7c02
127: IP6 10:90:90:0:0:0:0:97/64      , vlan 4095, DOWN
128: IP4 10.90.90.97      255.255.255.0  10.90.90.255,  vlan 4095, up
```

For each interface, the following information is displayed:

- IPv4 interface address and subnet mask
- IPv6 address and prefix
- VLAN assignment
- Status (up, DOWN, disabled)

`/info/13/ecmp`  
**ECMP Static Routes Information**

Current ecmp static routes:				
Destination	Mask	Gateway	If	GW Status
-----	-----	-----	-----	-----
10.10.1.1	255.255.255.255	10.100.1.1	1	up
		10.200.2.2	1	down
10.20.2.2	255.255.255.255	10.233.3.3	1	up
10.20.2.2	255.255.255.255	10.234.4.4	1	up
10.20.2.2	255.255.255.255	10.235.5.5	1	up

ECMP route information shows the status of each ECMP route configured on the switch.

## /info/13/ip

### IP Information

```

IP information:
  AS number 0

Interface information:
  1: 10.200.30.3      255.255.0.0      10.200.255.255,  vlan 1, up
  127: IP6 10:90:90:0:0:0:0:91/64      , vlan 4095, up
      fe80::222:ff:fe7d:717e
  128: IP4 172.31.30.128  255.255.0.0      172.31.255.255,  vlan 4095, up

Loopback interface information:
  2: 2.2.2.2          255.255.255.0    2.2.2.255,      enabled

Default gateway information: metric strict
  1: 10.200.1.1,      vlan any,  up
  132: 172.31.1.1,    vlan 4095, up  active

Default IP6 gateway information:

Current BOOTP relay settings: OFF
Current primary BOOTP server: 0.0.0.0
Current secondary BOOTP server: 0.0.0.0

Current IP forwarding settings: ON, dirbr disabled, noicmpd disabled

```

IP information includes:

- IP interface information: Interface number, IP address, subnet mask, broadcast address, VLAN number, and operational status.
- Loopback interface information, if applicable
- Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status
- BootP relay settings
- IP forwarding settings, including the forwarding status of directed broadcasts, and the status of ICMP re-directs

/info/l3/igmp

## IGMP Multicast Group Information Menu

[IGMP Multicast Menu]

mrouter

-

Show IGMP Snooping Multicast Router Port information

find

-

Show a single group by IP group address

vlan

-

Show groups on a single vlan

port

-

Show groups on a single port

trunk

-

Show groups on a single trunk

detail

-

Show detail of a single group by IP group address

dump

-

Show all groups

Table 47 describes the commands used to display information about IGMP groups learned by the switch.

Table 47 IGMP Multicast Group Information Menu Options (/info/l3/igmp)

Command Syntax and Usage

mrouter

Displays IGMP Multicast Router menu. To view menu options, see [page 128](#).

**find** <IP address>

Displays a single IGMP multicast group by its IP address.

**vlan** <VLAN number>

Displays all IGMP multicast groups on a single VLAN.

**port** <port number or alias>

Displays all IGMP multicast groups on a single port.

**trunk** <trunk number>

Displays all IGMP multicast groups on a single trunk group.

**detail** <IP address>

Displays details about IGMP multicast groups, including source and timer information.

**dump**

Displays information for all multicast groups. For details, see [page 128](#)

/info/13/igmp/mrouter

## IGMP Multicast Router Port Information Menu

[IGMP Multicast Router Menu]

vlan

- Show all multicast router ports on a single vlan

dump

- Show all learned multicast router ports

Table 48 describes the commands used to display information about multicast routers (Mrouter) learned through IGMP Snooping.

Table 48 IGMP Mrouter Information Menu Options (/info/igmp/mrouter)

Command Syntax and Usage

**vlan** <VLAN number>

Displays the multicast router ports configured or learned on the selected VLAN.

**dump**

Displays information for all multicast groups learned by the switch.

/info/13/igmp/mrouter/dump

## IGMP Multicast Router Dump Information

SrcIP	VLAN	Port	Version	Expires	MRT	QRV	QQIC
-----	-----	-----	-----	-----	-----	----	----
10.1.1.1	2	21	V3	4:09	128	2	125
10.1.1.5	2	23	V2	4:09	125	-	-
10.10.10.43	9	24	V2	static	unknown	-	-

IGMP Mrouter information includes:

- Source IP address
- VLAN and port where the Mrouter is connected
- IGMP version
- Mrouter expiration
- Maximum query response time
- Querier’s Robustness Variable (QRV)
- Querier’s Query Interval Code (QQIC)



`/info/13/igmp/dump`  
**IGMP Group Information**

Note: Local groups (224.0.0.x) are not snooped/relayed and will not appear.								
Source	Group	VLAN	Port	Version	Mode	Expires	Fwd	
-----	-----	-----	-----	-----	-----	-----	---	
10.1.1.1	232.1.1.1	2	EXT4	V3	INC	4:16	Yes	
10.1.1.5	232.1.1.1	2	EXT4	V3	INC	4:16	Yes	
*	232.1.1.1	2	EXT4	V3	INC	-	No	
10.10.10.43	235.0.0.1	9	EXT1	V3	INC	2:26	Yes	
*	236.0.0.1	9	EXT1	V3	EXC	-	Yes	

IGMP Group information includes:

- IGMP source address
- IGMP Group address
- VLAN and port
- IGMP version
- IGMPv3 filter mode
- Expiration timer value
- IGMP multicast forwarding state

## [/info/13/vrrp](#) VRRP Information

Virtual Router Redundancy Protocol (VRRP) support on the VFSM provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

```
VRRP information:
  1: vrid 2, 205.178.18.210, if 1, renter, prio 100, master
  2: vrid 1, 205.178.18.202, if 1, renter, prio 100, backup
  3: vrid 3, 205.178.18.204, if 1, renter, prio 100, master
```

When virtual routers are configured, you can view the status of each virtual router using this command. VRRP information includes:

- Virtual router number
- Virtual router ID and IP address
- Interface number
- Ownership status
  - `owner` identifies the preferred master virtual router. A virtual router is the owner when the IP address of the virtual router and its IP interface are the same.
  - `renter` identifies virtual routers which are not owned by this device.
- Priority value. During the election process, the virtual router with the highest priority becomes master.
- Activity status
  - `master` identifies the elected master virtual router.
  - `backup` identifies that the virtual router is in backup mode.
  - `init` identifies that the virtual router is waiting for a startup event.  
For example, once it receives a startup event, it transitions to master if its priority is 255, (the IP address owner), or transitions to backup if it is not the IP address owner.

/info/qos

# Quality of Service Information Menu

[QoS Menu]

8021p      - Show QOS 802.1p information

**Table 49**    QoS Menu Options (/info/qos)

**Command Syntax and Usage**

**8021p**

Displays 802.1p Information. For details, see [page 131](#).

/info/qos/8021p

## 802.1p Information

Current priority to COS queue information:

Priority	COSq	Weight
-----	----	-----
0	0	1
1	1	2
2	2	3
3	3	4
4	4	5
5	5	7
6	6	15
7	7	0

Current port priority information:

Port	Priority	COSq	Weight
-----	-----	----	-----
INT1	0	0	1
INT2	0	0	1
...			
MGT1	0	0	1
MGT2	0	0	1
EXT1	0	0	1
EXT2	0	0	1
EXT3	0	0	1
EXT4	0	0	1
...			

The following table describes the IEEE 802.1p priority to COS queue information.

**Table 50** 802.1p Priority-to-COS Queue Parameter Descriptions

Parameter	Description
Priority	Displays the 802.1p priority level.
COSq	Displays the Class of Service queue.
Weight	Displays the scheduling weight of the COS queue.

The following table describes the IEEE 802.1p port priority information.

**Table 51** 802.1p Port Priority Parameter Descriptions

Parameter	Description
Port	Displays the port alias.
Priority	Displays the 802.1p priority level.
COSq	Displays the Class of Service queue.
Weight	Displays the scheduling weight.

/info/acl

# Access Control List Information Menu

[ACL Information Menu]

acl-list

- Show ACL list

acl-grp

- Show ACL group

vmap

- Show VMAP

Table 52 ACL Information Menu Options (/info/acl)

## Command Syntax and Usage

**acl-list** <ACL number>

Displays ACL list information. For details, see [page 134](#).

**acl-grp** <ACL group number>

Displays ACL group information.

**vmap** <VMAP number>

Displays VMAP list information.

`/info/acl/acl-list`  
**Access Control List Information**

```
Current ACL information:
-----
Filter 2 profile:
  Ethernet
    - VID          : 2/0xfff
  Meter
    - Set to disabled
    - Set committed rate : 64
    - Set max burst size : 32
  Re-Mark
    - Set use of TOS precedence to disabled
  Actions          : Permit
  Statistics        : enabled

No ACL groups configured.
No VMAP configured.
```

Access Control List (ACL) information includes configuration settings for each ACL list.

**Table 53** ACL List Parameter Descriptions

Parameter	Description
Filter x profile	Indicates the ACL number.
Meter	Displays the ACL meter parameters.
Re-Mark	Displays the ACL re-mark parameters.
Actions	Displays the configured action for the ACL.
Statistics	Displays the status of ACL statistics configuration (enabled or disabled).

`/info/rmon`  
**RMON Information Menu**

---

[RMON Information Menu]

hist - Show RMON History group information

alarm - Show RMON Alarm group information

event - Show RMON Event group information

dump - Show all RMON information

The following table describes the Remote Monitoring (RMON) Information menu options.

**Table 54** RMON Information Menu Options (`/info/rmon`)

---

**Command Syntax and Usage**

---

**hist**

Displays RMON History information. For details, see [page 136](#).

---

**alarm**

Displays RMON Alarm information. For details, see [page 137](#).

---

**event**

Displays RMON Event information. For details, see [page 138](#).

---

**dump**

Displays all RMON information.

---

`/info/rmon/hist`  
RMON History Information

RMON History group configuration:				
Index	IFOID	Interval	Rbnum	Gbnum
-----	-----	-----	-----	-----
1	1.3.6.1.2.1.2.2.1.1.24	30	5	5
2	1.3.6.1.2.1.2.2.1.1.22	30	5	5
3	1.3.6.1.2.1.2.2.1.1.20	30	5	5
4	1.3.6.1.2.1.2.2.1.1.19	30	5	5
5	1.3.6.1.2.1.2.2.1.1.24	1800	5	5
Index	Owner			
-----	-----			
1	dan			

The following table describes the RMON History Information parameters.

**Table 55** RMON History Parameter Descriptions

Parameter	Description
Index	Displays the index number that identifies each history instance.
IFOID	Displays the MIB Object Identifier.
Interval	Displays the time interval for each sampling bucket.
Rbnum	Displays the number of requested buckets, which is the number of data slots into which data is to be saved.
Gbnum	Displays the number of granted buckets that may hold sampled data.
Owner	Displays the owner of the history instance.



/info/rmon/alarm  
RMON Alarm Information

RMON Alarm group configuration:						
Index	Interval	Sample	Type	rLimit	fLimit	last value
-----	-----	-----	-----	-----	-----	-----
1	1800	abs	either	0	0	7822
Index	rEvtIdx	fEvtIdx	OID			
-----	-----	-----	-----			
1	0	0	1.3.6.1.2.1.2.2.1.10.1			
Index	Owner					
-----	-----					
1	dan					

The following table describes the RMON Alarm Information parameters.

Table 56 RMON Alarm Parameter Descriptions

Parameter	Description
Index	Displays the index number that identifies each alarm instance.
Interval	Displays the time interval over which data is sampled and compared with the rising and falling thresholds.
Sample	Displays the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: <div><div><input type="checkbox"/> abs—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.</div><div><input type="checkbox"/> delta—delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.</div></div>
Type	Displays the type of alarm, as follows: <div><div><input type="checkbox"/> falling—alarm is triggered when a falling threshold is crossed.</div><div><input type="checkbox"/> rising—alarm is triggered when a rising threshold is crossed.</div><div><input type="checkbox"/> either—alarm is triggered when either a rising or falling threshold is crossed.</div></div>
rLimit	Displays the rising threshold for the sampled statistic.
fLimit	Displays the falling threshold for the sampled statistic.

**Table 56** RMON Alarm Parameter Descriptions (continued)

Parameter	Description
Last value	Displays the last sampled value.
rEvtIdx	Displays the rising alarm event index that is triggered when a rising threshold is crossed.
fEvtIdx	Displays the falling alarm event index that is triggered when a falling threshold is crossed.
OID	Displays the MIB Object Identifier for each alarm index.
Owner	Displays the owner of the alarm instance.

### [/info/rmon/event](#) RMON Event Information

RMON Event group configuration:

Index	Type	Last Sent	Description
1	both	0D: 0H: 1M:20S	Event_1
2	none	0D: 0H: 0M: 0S	Event_2
3	log	0D: 0H: 0M: 0S	Event_3
4	trap	0D: 0H: 0M: 0S	Event_4
5	both	0D: 0H: 0M: 0S	Log and trap event for Link Down
10	both	0D: 0H: 0M: 0S	Log and trap event for Link Up
11	both	0D: 0H: 0M: 0S	Send log and trap for icmpInMsg
15	both	0D: 0H: 0M: 0S	Send log and trap for icmpInEchos
Index	Owner		
1	dan		

The following table describes the RMON Event Information parameters.

**Table 57** RMON Event Parameter Descriptions

Parameter	Description
Index	Displays the index number that identifies each event instance.
Type	Displays the type of notification provided for this event, as follows: none, log, trap, both.
Last sent	Displays the time that passed since the last switch reboot, when the most recent event was triggered. This value is cleared when the switch reboots.

**Table 57** RMON Event Parameter Descriptions (continued)

Parameter	Description
Description	Displays a text description of the event.
Owner	Displays the owner of the event instance.

## /info/link

# Link Status Information

Alias	Port	Speed	Duplex	Flow Ctrl		Link
----	-----	-----	-----	--TX--	--RX--	-----
INT1	1	1G/10G	full	yes	yes	down
INT2	2	1G/10G	full	yes	yes	down
INT3	3	1G/10G	full	yes	yes	down
INT4	4	1G/10G	full	yes	yes	down
INT5	5	1G/10G	full	yes	yes	down
INT6	6	1G/10G	full	yes	yes	down
INT7	7	1G/10G	full	yes	yes	down
INT8	8	1G/10G	full	yes	yes	down
INT9	9	1G/10G	full	yes	yes	down
INT10	10	1G/10G	full	yes	yes	down
INT11	11	1G/10G	full	yes	yes	down
INT12	12	1G/10G	full	yes	yes	down
INT13	13	1G/10G	full	yes	yes	down
INT14	14	1G/10G	full	yes	yes	down
MGT1	15	100	full	yes	yes	up
MGT2	16	100	full	yes	yes	disabled
EXT1	17	10000	full	yes	yes	up
EXT2	18	10000	full	yes	yes	down
EXT3	19	10000	full	yes	yes	down
EXT4	20	10000	full	yes	yes	down
EXT5	21	10000	full	yes	yes	down
EXT6	22	10000	full	yes	yes	down
EXT7	23	10000	full	yes	yes	up
EXT8	24	10000	full	yes	yes	down
EXT9	25	10000	full	yes	yes	down
EXT10	26	10000	full	yes	yes	down
EXT11	27	any	any	yes	yes	down

**Note** – The sample screen might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

Use this command to display link status information about each port on a VFSM slot, including:

- Port alias and number
- Port speed
- Duplex mode (half, full, any)
- Flow control for transmit and receive (no, yes, or both)
- Link status (up, down, or disabled)

The following display shows link status when Bridge Module connections are enabled:

Alias	Port	Speed	Duplex	Flow Ctrl		Link
-----	----	-----	-----	--TX--	----RX--	-----
INT1	1	10000	full	yes	yes	down
INT2	2	10000	full	yes	yes	down
INT3	3	10000	full	yes	yes	down
INT4	4	10000	full	yes	yes	down
INT5	5	10000	full	yes	yes	down
INT6	6	10000	full	yes	yes	down
INT7	7	10000	full	yes	yes	down
INT8	8	10000	full	yes	yes	down
INT9	9	10000	full	yes	yes	down
INT10	10	10000	full	yes	yes	down
INT11	11	10000	full	yes	yes	down
INT12	12	10000	full	yes	yes	down
INT13	13	10000	full	yes	yes	down
INT14	14	10000	full	yes	yes	down
MGT1	15	100	full	yes	yes	up
MGT2	16	100	full	yes	yes	disabled
KR 1	17	10000	full	yes	yes	up
KR 2	18	10000	full	yes	yes	up
KR 3	19	10000	full	yes	yes	up
KR 4	20	10000	full	yes	yes	up
EXT5	21	10000	full	yes	yes	down
EXT6	22	10000	full	yes	yes	down
KR 8	23	10000	full	yes	yes	down
KR 7	24	10000	full	yes	yes	down
KR 6	25	10000	full	yes	yes	down
KR 5	26	10000	full	yes	yes	down
EXT11	27	any	any	yes	yes	down
-----						
Alias	Speed					
-----	-----					
BM5	40Gbs					
BM3	40Gbs					

**Note** – The sample might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

This command displays link status information about each port on the VFSM, including:

- Ethernet port alias, number, and configuration
- Link status (up, down, or disabled)
- Bridge Module (KR) port alias, port number, and configuration (if applicable)
- Bridge Module alias and speed setting

## /info/port

# Port Information

Alias	Port	Tag	Type	Fast	RMON	Lrn	Fld	PVID	NAME	VLAN(s)
INT1	1	y	Internal	n	d	e	e	1	INT1	1
INT2	2	y	Internal	n	d	e	e	1	INT2	1
INT3	3	y	Internal	n	d	e	e	1	INT3	1
INT4	4	y	Internal	n	d	e	e	1	INT4	1
INT5	5	y	Internal	n	d	e	e	1	INT5	1
INT6	6	y	Internal	n	d	e	e	1	INT6	1
INT7	7	y	Internal	n	d	e	e	1	INT7	1
INT8	8	y	Internal	n	d	e	e	1	INT8	1
INT9	9	y	Internal	n	d	e	e	1	INT9	1
INT10	10	y	Internal	n	d	e	e	1	INT10	1
INT11	11	y	Internal	n	d	e	e	1	INT11	1
INT12	12	y	Internal	n	d	e	e	1	INT12	1
INT13	13	y	Internal	n	d	e	e	1	INT13	1
INT14	14	y	Internal	n	d	e	e	1	INT14	1
MGT1	15	y	Mgmt	n	d	e	e	4095*	MGT1	4095
MGT2	16	y	Mgmt	n	d	e	e	4095*	MGT2	4095
EXT1	17	n	External	n	d	e	e	1	EXT1	1
EXT2	18	n	External	n	d	e	e	1	EXT2	1
EXT3	19	n	External	n	d	e	e	1	EXT3	1
EXT4	20	n	External	n	d	e	e	1	EXT4	1
...										
* = PVID is tagged.										

**Note** – The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

Port information includes:

- Port alias and number
- Whether the port uses VLAN tagging or not (y or n)
- Type of port (Internal, External, or Management)
- Whether the port is configured for Port Fast Forwarding (**Fast**)
- Whether the port has Remote Monitoring (RMON) enabled
- Whether the port has FDB learning enabled (**Lrn**)
- Whether the port has Port Flood Blocking enabled (**Fld**)
- Port VLAN ID (**PVID**)
- Port name
- VLAN membership

`/info/transcvr`  
**Port Transceiver Status**

-----							
Port	Device	TX-Ena	RX-Sig	TX-Flt	Vendor	Serial	
-----							
17 -	EXT1	1m DAC	Enabled	Link	none	Molex Inc.	822230105
18 -	EXT2	NO Device					
19 -	EXT3	NO Device					
20 -	EXT4	NO Device					
21 -	EXT5	NO Device					
22 -	EXT6	NO Device					
23 -	EXT7	1m DAC	Enabled	Link	none	Molex Inc.	822230105
24 -	EXT8	NO Device					
25 -	EXT9	NO Device					
26 -	EXT10	NO Device					

This command displays the status of the transceiver module on each external port.

/info/virt

# Virtualization Information

[Virtualization Menu]	
vm	- Show Virtual Machine information

Table 58 describes general virtualization information options. More details are available in the following sections.

Table 58 Virtualization Information Options (/info/virt)

Command Syntax and Usage

vm

Displays the Virtual Machines (VM) information menu. For details, see [page 144](#).

/info/virt/vm

# Virtual Machines Information

[Virtual Machine Menu]	
vmware	- Show VMware-specific information
port	- Show per port Virtual Machine information
dump	- Show all the Virtual Machine information

Table 59 Virtual Machines (VM) Information Options (/info/virt/vm)

Command Syntax and Usage

vmware

Displays the VMware-specific information menu.

port

Displays Virtual Machine information for the selected port.

dump

Displays all Virtual Machine information. For details, see [page 144](#).



/info/virt/vm/dump  
Virtual Machine (VM) Information

IP Address	VMAC Address	Index	Port	VM Group (Profile)
*127.31.46.50	00:50:56:4e:62:f5	4	INT3	
*127.31.46.10	00:50:56:4f:f2:85	2	INT4	
+127.31.46.51	00:50:56:72:ec:86	1	INT3	
+127.31.46.11	00:50:56:7c:1c:ca	3	INT4	
127.31.46.25	00:50:56:9c:00:c8	5	INT4	
127.31.46.15	00:50:56:9c:21:2f	0	INT4	
127.31.46.35	00:50:56:9c:29:29	6	INT3	
Number of entries: 8				
* indicates VMware ESX Service Console Interface				
+ indicates VMware ESX/ESXi VMKernel or Management Interface				

VM information includes the following for each Virtual Machine (VM):

- IP address
- MAC address
- Index number assigned to the VM
- Internal port on which the VM was detected
- VM group that contains the VM, if applicable

/info/virt/vm/vmware  
VMware Information

[VMware-specific Information Menu]	
hosts	- Show the names of all VMware Hosts in Data Center
showhost	- Show networking information for the specified VMware Host
showvm	- Show networking information for the specified VMware VM
vms	- Show the names of all VMware VMs in the Data Center

Use these commands to display information about Virtual Machines (VMs) and VMware hosts in the data center. These commands require the presence of a configured Virtual Center.

Table 60 VMware Information Options (/info/virt/vm/vmware)

Command Syntax and Usage
<b>hosts</b>
Displays a list of VMware hosts. For details, see <a href="#">page 146</a> .
<b>showhost</b> <host UUID>   <host IP address>   <host host name>
Displays detailed information about a specific VMware host.

Table 60 VMware Information Options (/info/virt/vm/vmware)

Command Syntax and Usage

**showvm** <VM UUID> | <VM IP address> | <VM name>

Displays detailed information about a specific Virtual Machine (VM).

**vms**

Displays a list of VMs.

/info/virt/vm/vmware/hosts  
VMware Host Information

UUID	Name(s) , IP Address
-----	-----
80a42681-d0e5-5910-a0bf-bd23bd3f7803	127.12.41.30
3c2e063c-153c-dd11-8b32-a78dd1909a69	127.12.46.10
64f1fe30-143c-dd11-84f2-a8ba2cd7ae40	127.12.44.50
c818938e-143c-dd11-9f7a-d8defa4b83bf	127.12.46.20
fc719af0-093c-dd11-95be-b0adac1bcf86	127.12.46.30
009a581a-143c-dd11-be4c-c9fb65ff04ec	127.12.46.40

VM host information includes the following:

- UUID associated with the VMware host.
- Name or IP address of the VMware host.

/info/cee

# Converged Enhanced Ethernet Information

[CEE Information Menu]	
dcbx	- DCB Capability Exchange Protocol (DCBX) Information Menu
ets	- Enhanced Transmission Selection Information Menu
pfc	- Priority Flow Control Information Menu
dump	- Show all CEE information

Table 61 describes the Converged Enhanced Ethernet (CEE) information options.

Table 61 CEE Information Options (/info/cee)

## Command Syntax and Usage

### dcbx

Displays the DCB Capability Exchange Protocol (DCBX) information menu. To view the menu options, see [page 148](#).

### ets

Displays the Enhanced Transmission Selection (ETS) information menu. To view the menu options, see [page 154](#).

### pfc

Displays the Priority Flow Control (PFC) information menu. To view the menu options, see [page 156](#).

### dump

Displays all CEE information.

[/info/cee/dcbx](#)  
DCBX Information

[DCBX Information Menu]	
ctrl	- Show DCBX Control state machine information
feat	- Show DCBX Feature state machine information
ets	- Show DCBX ETS state machine information
pfc	- Show DCBX PFC state machine information
app	- Show DCBX Application Protocol state machine information
dump	- Show all DCBX information

Table 62 describes the Data Center Bridging Capability Exchange (DCBX) protocol information options.

Table 62 DCBX Information Options (/info/cee/dcbx)

Command Syntax and Usage	
<b>ctrl</b> [ <i>&lt;port alias or number&gt;</i> ]	Displays information about the DCBX Control state machine. For details, see <a href="#">page 149</a> .
<b>feat</b> [ <i>&lt;port alias or number&gt;</i> ]	Displays information about the DCBX Feature state machine. For details, see <a href="#">page 149</a> .
<b>ets</b> [ <i>&lt;port alias or number&gt;</i> ]	Displays information about the DCBX ETS state machine. For details, see <a href="#">page 151</a> .
<b>pfc</b> [ <i>&lt;port alias or number&gt;</i> ]	Displays information about the DCBX PFC state machine. For details, see <a href="#">page 152</a> .
<b>app</b> [ <i>&lt;port alias or number&gt;</i> ]	Displays information about the DCBX Application Protocol state machine on the selected port. For details, see <a href="#">page 153</a> .
<b>dump</b>	Displays all DCBX information.

`/info/cee/dcbx/ctrl` [*<port alias or number>*]  
**DCBX Control Information**

Alias	Port	OperStatus	OperVer	MaxVer	SeqNo	AckNo
INT1	1	enabled	0	0	0	0
INT2	2	enabled	0	0	4	2
INT3	3	enabled	0	0	0	0
INT4	4	enabled	0	0	1	1
...						

DCBX Control information includes the following:

- Port alias and number
- DCBX status (enabled or disabled)
- Operating version negotiated with the peer device
- Maximum operating version supported by the system
- Sequence number that changes each time a DCBX parameter in one or more DCB feature TLVs changes
- Sequence number of the most recent DCB feature TLV that has been acknowledged

`/info/cee/dcbx/feat` [*<port alias or number>*]  
**DCBX Feature Information**

DCBX Port Feature State-machine Info												
Alias	Port	Type	AdmState	Will	Advrt	OpVer	MxVer	PrWill	SeqNo	Err	OperMode	Syncd
INT1	1	ETS	enabled	No	Yes	0	0	No	0	No	disabled	No
INT2	2	ETS	enabled	No	Yes	0	0	Yes	4	No	enabled	Yes
INT3	3	ETS	enabled	No	Yes	0	0	No	0	No	disabled	No
INT4	4	ETS	enabled	No	Yes	0	0	Yes	1	No	enabled	Yes
INT5	5	ETS	enabled	No	Yes	0	0	Yes	1	No	enabled	Yes
INT6	6	ETS	disabled	No	Yes	0	0	No	0	No	disabled	No
INT7	7	ETS	disabled	No	Yes	0	0	No	0	No	disabled	No
INT8	8	ETS	disabled	No	Yes	0	0	No	0	No	disabled	No
INT9	9	ETS	disabled	No	Yes	0	0	No	0	No	disabled	No
INT10	10	ETS	enabled	No	Yes	0	0	No	0	No	disabled	No
...												

The following table describes the DCBX Feature information.

**Table 63** DCBX Feature Information Fields

Parameter	Description
Alias	Displays each port's alias.
Port	Displays each port's number.
Type	Feature type
AdmState	Feature status (Enabled or Disabled)
Will	Willing flag status (Yes/True or No/Untrue)
Advrt	Advertisement flag status (Yes/True or No/Untrue)
OpVer	Operating version negotiated with the peer device
MxVer	Maximum operating version supported by the system
PrWill	Peer's Willing flag status (Yes/True or No/Untrue)
SeqNo	Sequence number that changes each time a DCBX parameter in one or more DCB feature TLVs changes
Err	Error condition flag (Yes or No). Yes indicates that an error occurred during the exchange of configuration data with the peer.
OperMode	Operating status negotiated with the peer device (enabled or disabled)
Syncd	Synchronization status between this port and the peer (Yes or No)

`/info/cee/dcbx/ets` [*<port alias or number>*]  
**DCBX ETS Information**

DCBX Port Priority Group - Priority Allocation Table					
Alias	Port	Priority	PgIdDes	PgIdOper	PgIdPeer
INT2	2	0	PGID0	PGID0	PGID0
INT2	2	1	PGID0	PGID0	PGID0
INT2	2	2	PGID0	PGID0	PGID0
INT2	2	3	PGID1	PGID0	PGID0
INT2	2	4	PGID2	PGID0	PGID0
INT2	2	5	PGID2	PGID0	PGID0
INT2	2	6	PGID2	PGID0	PGID0
INT2	2	7	PGID2	PGID0	PGID0
DCBX Port Priority Group - Bandwidth Allocation Table					
Alias	Port	PrioGrp	BwDes	BwOper	BwPeer
INT2	2	0	10	10	50
INT2	2	1	50	50	50
INT2	2	2	40	40	0

The following table describes the DCBX ETS information.

**Table 64** DCBX Feature Information Fields

Parameter	Description
<b>DCBX Port Priority Group - Priority Allocation Table</b>	
Alias	Displays each port's alias
Port	Displays each port's number
PgIdDes	Priority Group ID configured on this switch
PgIdOper	Priority Group negotiated with the peer (operating Priority Group).
PgIdPeer	Priority Group ID configured on the peer
<b>DCBX Port Priority Group - Bandwidth Allocation Table</b>	
BwDes	Bandwidth allocation configured on this switch
BwOper	Bandwidth allocation negotiated with the peer (operating bandwidth)
BwPeer	Bandwidth allocation configured on the peer

`/info/cee/dcbx/pfc [<port alias or number>]`  
**DCBX PFC Information**

DCBX Port Priority Flow Control Table					
=====					
Alias	Port	Priority	EnableDesr	EnableOper	EnablePeer
-----	----	-----	-----	-----	-----
INT2	2	0	disabled	disabled	disabled
INT2	2	1	disabled	disabled	disabled
INT2	2	2	disabled	disabled	disabled
INT2	2	3	enabled	disabled	disabled
INT2	2	4	disabled	disabled	disabled
INT2	2	5	disabled	disabled	disabled
INT2	2	6	disabled	disabled	disabled
INT2	2	7	disabled	disabled	disabled

DCBX PFC information includes the following:

- Port alias and number
- 802.1p value
- **EnableDesr**: Status configured on this switch
- **EnableOper**: Status negotiated with the peer (operating status)
- **EnablePeer**: Status configured on the peer



`/info/cee/dcbx/app [<port alias or number>]`  
**DCBX Application Protocol Information**

DCBX Application Protocol Table  
=====

FCoE Priority Information  
=====

Protocol ID : 0x8906  
Selector Field : 0  
Organizationally Unique ID: 0x1b21

Alias	Port	Priority	EnableDesr	EnableOper	EnablePeer
INT2	2	0	enabled	enabled	enabled
INT2	2	1	disabled	disabled	disabled
INT2	2	2	disabled	disabled	disabled
INT2	2	3	enabled	enabled	enabled
INT2	2	4	disabled	disabled	disabled
INT2	2	5	disabled	disabled	disabled
INT2	2	6	disabled	disabled	disabled
INT2	2	7	disabled	disabled	disabled

FIP Snooping Priority Information  
=====

Protocol ID : 0x8914  
Selector Field : 0  
Organizationally Unique ID: 0x1b21

Alias	Port	Priority	EnableDesr	EnableOper	EnablePeer
INT2	2	0	enabled	enabled	enabled
INT2	2	1	disabled	disabled	disabled
INT2	2	2	disabled	disabled	disabled
INT2	2	3	enabled	enabled	enabled
INT2	2	4	disabled	disabled	disabled
INT2	2	5	disabled	disabled	disabled
INT2	2	6	disabled	disabled	disabled
INT2	2	7	disabled	disabled	disabled

The following table describes the DCBX Application Protocol information.

**Table 65** DCBX Application Protocol Information Fields

Parameter	Description
Protocol ID	Identifies the supported Application Protocol.
Selector Field	Specifies the Application Protocol type, as follows: <div><input type="checkbox"/> 0 = Ethernet Type</div> <div><input type="checkbox"/> 1 = TCP socket ID</div>
Organizationally Unique ID	DCBX TLV identifier
Alias	Port alias
Port	Port number
Priority	802.1p value
EnableDesr	Status configured on this switch
EnableOper	Status negotiated with the peer (operating status)
EnablePeer	Status configured on the peer

**/info/cee/ets**  
**ETS Information Menu**

[ETS Information Menu]
dump        - Show all ETS information

**Table 66** describes the Enhanced Transmission Selection (ETS) information options.

**Table 66** ETS Information Options (/info/cee/ets)

Command Syntax and Usage
<b>dump</b>
Displays global ETS information. For details, see <a href="#">page 155</a> .

`/info/cee/ets/dump`  
**ETS Information**

Global ETS information:

Number of COSq: 8

Mapping of 802.1p Priority to Priority Groups:

Priority	PGID	COSq
-----	----	----
0	0	0
1	0	0
2	0	0
3	1	1
4	2	2
5	2	2
6	2	2
7	2	2

Bandwidth Allocation to Priority Groups:

PGID	PG%	Description
----	---	-----
0	10	
1	50	
2	40	

Enhanced Transmission Selection (ETS) information includes the following:

- Number of Class of Service queues (COSq) configured
- 802.1p mapping to Priority Groups and Class of Service queues
- Bandwidth allocated to each Priority Group

[/info/cee/pfc](#)  
**PFC Information**

[PFC Information Menu]

port - Show PFC information related to a port

dump - Show all PFC information

Table 67 describes the Priority Flow Control (PFC) information options.

**Table 67** PFC Information Options (/info/cee/pfc)

**Command Syntax and Usage**

**port** *<port alias or number>*

Displays PFC information for the selected port.

**dump**

Displays PFC information for all ports.

[/info/cee/pfc/dump](#)  
**PFC Information**

Global PFC Information:

PFC - ON

Priority	State	Description
0	Dis	
1	Dis	
2	Dis	
3	Ena	
4	Dis	
5	Dis	
6	Dis	
7	Dis	

-----

State - indicates whether PFC is Enabled/Disabled on a particular priority

`/info/fcoe`  
**FCoE Information**

```
[Fibre Channel over Ethernet Information Menu]
fips      - FIP Snooping Information Menu
dump      - Show all FCOE information
```

Table 68 describes the Fiber Channel over Ethernet (FCoE) information options.

**Table 68** FCoE Information Options (`/info/fcoe`)

**Command Syntax and Usage**

**fips**

Displays the FIP Snooping information menu.

**dump**

Displays all current FCoE information.

`/info/fcoe/fips`  
**FIP Snooping Information**

```
[FIP Snooping Information Menu]
port      - Show FIP snooping ACLs installed on a port
fcf       - Show all FCF detected
fcoe      - Show all FCOE connections detected
dump      - Show all FIP snooping ACLs that are installed
```

Table 69 describes the Fiber Channel Initialization Protocol (FIP) Snooping information options.

**Table 69** FIP Snooping Information Options (`/info/fcoe/fips`)

**Command Syntax and Usage**

**port** *<port alias or number>*

Displays FIP Snooping (FIPS) information for the selected port, including a list of current FIPS ACLs. For details, see [page 158](#).

**fcf**

Displays FCF information for all ports.

Table 69 FIP Snooping Information Options (/info/fcoe/fips)

Command Syntax and Usage	
<b>fcoe</b>	Displays FCOE connections.
<b>dump</b>	Displays FIP Snooping information for all ports.

**/info/fcoe/fips/port** <port alias or number>  
**FIP Snooping Port Information**

```
FIP Snooping on port INT2:
This port has been configured to automatically detect FCF.
It has currently detected to have 0 FCF connecting to it.

FIPS ACLs configured on this port:
SMAC 00:c0:dd:13:9b:6f, action deny.
SMAC 00:c0:dd:13:9b:70, action deny.
SMAC 00:c0:dd:13:9b:6d, action deny.
SMAC 00:c0:dd:13:9b:6e, action deny.
DMAC 00:c0:dd:13:9b:6f, ethertype 0x8914, action permit.
DMAC 00:c0:dd:13:9b:70, ethertype 0x8914, action permit.
DMAC 00:c0:dd:13:9b:6d, ethertype 0x8914, action permit.
DMAC 00:c0:dd:13:9b:6e, ethertype 0x8914, action permit.
SMAC 0e:fc:00:01:0a:00, DMAC 00:c0:dd:13:9b:6d, ethertype 0x8906, vlan
1002, action permit.
DMAC 01:10:18:01:00:01, Ethertype 0x8914, action permit.
DMAC 01:10:18:01:00:02, Ethertype 0x8914, action permit.
Ethertype 0x8914, action deny.
Ethertype 0x8906, action deny.
SMAC 0e:fc:00:00:00:00, SMAC mask ff:ff:ff:00:00:00, action deny.
```

FIP Snooping port information includes the following:

- Fiber Channel Forwarding (FCF) mode
- Number of FCF links connected to the port
- List of FIP Snooping ACLs assigned to the port

## `/info/dump` Information Dump

---

Use the dump command to dump all switch information available from the Information Menu (10K or more, depending on your configuration). This data is useful for tuning and debugging switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.





## CHAPTER 5

# The Statistics Menu

---

You can view switch performance statistics in both the user and administrator command modes. This chapter discusses how to use the command line interface to display switch statistics.

### /stats

## Statistics Menu

---

```
[Statistics Menu]
  port      - Port Stats Menu
  12        - Layer 2 Stats Menu
  13        - Layer 3 Stats Menu
  mp        - MP-specific Stats Menu
  acl       - ACL Stats Menu
  fcoe      - FCOE Stats Menu
  snmp      - Show SNMP stats
  ntp       - Show NTP stats
  clrmp     - Clear all MP related stats
  clrports  - Clear stats for all ports
  dump      - Dump all stats
```

The information provided by each menu option is briefly described in [Table 70](#), with pointers to detailed information.

**Table 70** Statistics Menu Options (/stats)

---

#### Command Syntax and Usage

---

**port** <port alias or number>

Displays the Port Statistics Menu for the specified port. Use this command to display traffic statistics on a port-by-port basis. Traffic statistics are included in SNMP Management Information Base (MIB) objects. To view menu options, see [page 163](#).

---

**12**

Displays the Layer 2 Statistics Menu. To view menu options, see [page 181](#).

---

**Table 70** Statistics Menu Options (/stats)

---

**Command Syntax and Usage**

---

**13**

Displays the Layer 3 Stats Menu. To view menu options, see [page 190](#).

---

**mp**

Displays the Management Processor Statistics Menu. Use this command to view information on how switch management processes and resources are currently being allocated. To view menu options, see [page 223](#).

---

**acl**

Displays ACL Statistics menu. To view menu options, see [page 227](#).

---

**fcoe [clear]**

Displays Fiber Channel over Ethernet (FCoE) Statistics. To view details, see [page 229](#).

You can use the `clear` option to delete all FCoE statistics.

---

**snmp**

Displays SNMP statistics. See [page 230](#) for sample output.

---

**ntp [clear]**

Displays Network Time Protocol (NTP) Statistics. See [page 234](#) for a sample output and a description of NTP Statistics.

You can use the `clear` option to delete all NTP statistics.

---

**clrmp**

Clears all management processor statistics.

---

**clrports**

Clears statistics counters for all ports.

---

**dump**

Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. For details, see [page 235](#).

---

*/stats/port <port alias or number>*  
**Port Statistics Menu**

---

This menu displays traffic statistics on a port-by-port basis. Traffic statistics include SNMP Management Information Base (MIB) objects.

[Port Statistics Menu]

8021x

- Show 802.1x stats

amp

- Show AMP stats

bootp

- Show BOOTP relay stats

brg

- Show bridging ("dot1") stats

ether

- Show Ethernet ("dot3") stats

if

- Show interface ("if") stats

ip

- Show Internet Protocol ("IP") stats

link

- Show link stats

rmon

- Show RMON stats

dump

- Show all port stats

clear

- Clear all port stats

**Table 71** Port Statistics Menu Options (/stats/port)

---

**Command Syntax and Usage**

---

**8021x**

Displays IEEE 802.1x statistics for the port. See [page 166](#) for sample output.

**amp**

Displays Active MultiPath (AMP) statistics for the port. See [page 169](#) for sample output.

**Note:** AMP statistics are available only for an external port (EXTx).

**brg**

Displays bridging (“dot1”) statistics for the port. See [page 170](#) for sample output.

**ether**

Displays Ethernet (“dot3”) statistics for the port. See [page 171](#) for sample output.

**if**

Displays interface statistics for the port. See [page 174](#) for sample output.

**ip**

Displays IP statistics for the port. See [page 177](#) for sample output.

**link**

Displays link statistics for the port. See [page 177](#) for sample output.

---

**Table 71** Port Statistics Menu Options (/stats/port) (continued)

Command Syntax and Usage	
<b>rmon</b>	Displays Remote Monitoring (RMON) statistics for the port. See <a href="#">page 178</a> for sample output.
<b>dump</b>	This command dumps all statistics for the selected port.
<b>clear</b>	This command clears all the statistics on the selected port.

**/stats/port <port alias or number>/8021x**  
**802.1x Authenticator Statistics**

This menu option enables you to display the 802.1x authenticator statistics of the selected port.

Authenticator Statistics:	
eapolFramesRx	= 925
eapolFramesTx	= 3201
eapolStartFramesRx	= 2
eapolLogoffFramesRx	= 0
eapolRespIdFramesRx	= 463
eapolRespFramesRx	= 460
eapolReqIdFramesTx	= 1820
eapolReqFramesTx	= 1381
invalidEapolFramesRx	= 0
eapLengthErrorFramesRx	= 0
lastEapolFrameVersion	= 1
lastEapolFrameSource	= 00:01:02:45:ac:51

**Table 72** 802.1x Authenticator Statistics of a Port (/stats/port/8021x)

Statistics	Description
eapolFramesRx	Total number of EAPOL frames received
eapolFramesTx	Total number of EAPOL frames transmitted
eapolStartFramesRx	Total number of EAPOL Start frames received
eapolLogoffFramesRx	Total number of EAPOL Logoff frames received
eapolRespIdFramesRx	Total number of EAPOL Response Identity frames received
eapolRespFramesRx	Total number of Response frames received
eapolReqIdFramesTx	Total number of Request Identity frames transmitted
eapolReqFramesTx	Total number of Request frames transmitted
invalidEapolFramesRx	Total number of invalid EAPOL frames received
eapLengthErrorFramesRx	Total number of EAP length error frames received
lastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
lastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

`/stats/port <port alias or number>/8021x`  
**802.1x Authenticator Diagnostics**

This menu option enables you to display the 802.1x authenticator diagnostics of the selected port.

Authenticator Diagnostics:	
authEntersConnecting	= 1820
authEapLogoffsWhileConnecting	= 0
authEntersAuthenticating	= 463
authSuccessesWhileAuthenticating	= 5
authTimeoutsWhileAuthenticating	= 0
authFailWhileAuthenticating	= 458
authReauthsWhileAuthenticating	= 0
authEapStartsWhileAuthenticating	= 0
authEapLogoffWhileAuthenticating	= 0
authReauthsWhileAuthenticated	= 3
authEapStartsWhileAuthenticated	= 0
authEapLogoffWhileAuthenticated	= 0
backendResponses	= 923
backendAccessChallenges	= 460
backendOtherRequestsToSupplicant	= 460
backendNonNakResponsesFromSupplicant	= 460
backendAuthSuccesses	= 5
backendAuthFails	= 458

**Table 73** 802.1x Authenticator Diagnostics of a Port (/stats/port/8021x)

Statistics	Description
authEntersConnecting	Total number of times that the state machine transitions to the CONNECTING state from any other state.
authEapLogoffsWhile Connecting	Total number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
authEnters Authenticating	Total number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the Supplicant.
authSuccessesWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant.
authTimeoutsWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout.

**Table 73** 802.1x Authenticator Diagnostics of a Port (/stats/port/8021x)

Statistics	Description
authFailWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure.
authReauthsWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a re-authentication request
authEapStartsWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
authReauthsWhile Authenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a re-authentication request.
authEapStartsWhile Authenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhile Authenticated	Total number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant.
backendResponses	Total number of times that the state machine sends an initial Access-Request packet to the Authentication server. Indicates that the Authenticator attempted communication with the Authentication Server.
backendAccess Challenges	Total number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the Authentication Server has communication with the Authenticator.
backendOtherRequests ToSupplicant	Total number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant. Indicates that the Authenticator chose an EAP-method.

**Table 73** 802.1x Authenticator Diagnostics of a Port (/stats/port/8021x)

Statistics	Description
backendNonNakResponsesFromSupplicant	Total number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK. Indicates that the Supplicant can respond to the Authenticator's chosen EAP-method.
backendAuthSuccesses	Total number of times that the state machine receives an Accept message from the Authentication Server. Indicates that the Supplicant has successfully authenticated to the Authentication Server.
backendAuthFails	Total number of times that the state machine receives a Reject message from the Authentication Server. Indicates that the Supplicant has not authenticated to the Authentication Server.



`/stats/port <port alias or number>/amp`  
**Active MultiPath Statistics**

AMP statistics for port EXT1:		
Keep-alive packets sent:		0
Keep-alive packets rcvd:		0
Fdb-Flush packets sent:		0
Fdb-Flush packets rcvd:		0
Dropped packets	:	0

**Table 74** AMP Statistics of a Port (/stats/port/amp)

Statistics	Description
Keep-alive packets sent	Number of keep-alive packets sent.
Keep-alive packets rcvd	Number of keep-alive packets received.
Fdb-Flush packets sent	Number of FDB-flush packets sent.
Fdb-Flush packets rcvd	Number of FDB-flush packets received.
Dropped packets	Number of invalid AMP packets dropped.

`/stats/port <port alias or number>/brg`  
**Bridging Statistics**

This menu option enables you to display the bridging statistics of the selected port.

Bridging statistics for port INT1:	
dot1PortInFrames:	63242584
dot1PortOutFrames:	63277826
dot1PortInDiscards:	0
dot1TpLearnedEntryDiscards:	0
dot1StpPortForwardTransitions:	0

**Table 75** Bridging Statistics of a Port (/stats/port/brg)

Statistics	Description
dot1PortInFrames	The number of frames that have been received by this port from its segment. A frame received on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.
dot1PortOutFrames	The number of frames that have been transmitted by this port to its segment. Note that a frame transmitted on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.
dot1PortInDiscards	Count of valid frames received which were discarded (that is, filtered) by the Forwarding Process.
dot1TpLearnedEntry Discards	The total number of Forwarding Database entries, which have been or would have been learnt, but have been discarded due to a lack of space to store them in the Forwarding Database. If this counter is increasing, it indicates that the Forwarding Database is regularly becoming full (a condition which has unpleasant performance effects on the subnetwork). If this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent.
dot1StpPortForward Transitions	The number of times this port has transitioned from the Learning state to the Forwarding state.

`/stats/port <port alias or number>/ether`  
**Ethernet Statistics**

This menu option enables you to display the ethernet statistics of the selected port

Ethernet statistics for port INT1:	
dot3StatsAlignmentErrors:	0
dot3StatsFCSErrors:	0
dot3StatsSingleCollisionFrames:	0
dot3StatsMultipleCollisionFrames:	0
dot3StatsLateCollisions:	0
dot3StatsExcessiveCollisions:	0
dot3StatsInternalMacTransmitErrors:	NA
dot3StatsFrameTooLongs:	0
dot3StatsInternalMacReceiveErrors:	0

**Table 76** Ethernet Statistics for Port (/stats/port/ether)

Statistics	Description
dot3StatsAlignmentErrors	<p>A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check.</p> <p>The count represented by an instance of this object is incremented when the <code>alignmentError</code> status is returned by the MAC service to the Logical Link Control (LLC) (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>
dot3StatsFCSErrors	<p>A count of frames received on a particular interface that are an integral number of octets in length but do not pass the Frame Check Sequence (FCS) check.</p> <p>The count represented by an instance of this object is incremented when the <code>frameCheckError</code> status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>

**Table 76** Ethernet Statistics for Port (/stats/port/ether)

Statistics	Description
dot3StatsSingleCollisionFrames	<p>A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.</p> <p>A frame that is counted by an instance of this object is also counted by the corresponding instance of either the <code>ifOutUcastPkts</code>, <code>ifOutMulticastPkts</code>, or <code>ifOutBroadcastPkts</code>, and is not counted by the corresponding instance of the <code>dot3StatsMultipleCollisionFrame</code> object.</p>
dot3StatsMultipleCollisionFrames	<p>A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.</p> <p>A frame that is counted by an instance of this object is also counted by the corresponding instance of either the <code>ifOutUcastPkts</code>, <code>ifOutMulticastPkts</code>, or <code>ifOutBroadcastPkts</code>, and is not counted by the corresponding instance of the <code>dot3StatsSingleCollisionFrames</code> object.</p>
dot3StatsLateCollisions	<p>The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.</p> <p>Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.</p>
dot3StatsExcessiveCollisions	<p>A count of frames for which transmission on a particular interface fails due to excessive collisions.</p>
dot3StatsInternalMacTransmitErrors	<p>A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the <code>dot3StatsLateCollisions</code> object, the <code>dot3StatsExcessiveCollisions</code> object, or the <code>dot3StatsCarrierSenseErrors</code> object.</p> <p>The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.</p>

**Table 76** Ethernet Statistics for Port (/stats/port/ether)

Statistics	Description
dot3StatsFrameTooLongs	<p>A count of frames received on a particular interface that exceed the maximum permitted frame size.</p> <p>The count represented by an instance of this object is incremented when the <code>frameTooLong</code> status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>
dot3StatsInternalMacReceiveErrors	<p>A count of frames for which reception on a particular interface fails due to an internal MAC sub layer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the <code>dot3StatsFrameTooLongs</code> object, the <code>dot3StatsAlignmentErrors</code> object, or the <code>dot3StatsFCSErrors</code> object.</p> <p>The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of received errors on a particular interface that are not otherwise counted.</p>

**/stats/port <port alias or number>/if**  
**Interface Statistics**

This menu option enables you to display the interface statistics of the selected port.

Interface statistics for port EXT1:		
	ifHCIn Counters	ifHCOut Counters
Octets:	51697080313	51721056808
UcastPkts:	65356399	65385714
BroadcastPkts:	0	6516
MulticastPkts:	0	0
FlowCtrlPkts:	0	0
Discards:	0	0
Errors:	0	21187
Ingress Discard reasons for port EXT1:		
VLAN Discards:	0	
Empty Egress Portmap:	0	
Filter Discards:	0	
Policy Discards:	0	
Non-Forwarding State:	0	
IBP/CBP Discards:	0	

**Table 77** Interface Statistics for Port (/stats/port/if)

Statistics	Description
ifInOctets	The total number of octets received on the interface, including framing characters.
ifInUcastPkts	The number of packets, delivered by this sub-layer to a higher sub-layer, which were not addressed to a multicast or broadcast address at this sub-layer.
ifInBroadcastPkts	The number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a broadcast address at this sub-layer.
ifInMulticastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses.
ifInFlowControlPkts	The total number of flow control pause packets received on the interface.

**Table 77** Interface Statistics for Port (/stats/port/if)

Statistics	Description
ifInDiscards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
ifInErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
ifOutOctets	The total number of octets transmitted out of the interface, including framing characters.
ifOutUcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
ifOutBroadcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of <code>ifOutBroadcastPkts</code> .
ifOutMulticastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of <code>ifOutMulticastPkts</code> .
ifOutFlowControlPkts	The total number of flow control pause packets transmitted out of the interface.
ifOutDiscards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
ifOutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

**Table 77** Interface Statistics for Port (/stats/port/if)

Statistics	Description
VLAN Discards	Discarded because the packet was tagged with a VLAN to which this port is not a member.
Empty Egress Portmap	Dropped due to an egress port bitmap of zero condition (no ports in the egress mask). This counter increments whenever the switching decision found that there was no port to send out.
Filter Discards	Dropped by the Content Aware Engine (user-configured filter).
Policy Discards	Dropped due to policy setting. For example, due to a user-configured static entry.
Non-Forwarding State	Discarded because the ingress port is not in the forwarding state.
IBP/CBP Discards	Discarded because of Ingress Back Pressure (flow control), or because the Common Buffer Pool is full (for example, insufficient packet buffering).



**/stats/port <port alias or number>/ip**  
**Interface Protocol Statistics**

This menu option enables you to display the interface statistics of the selected port.

GEA IP statistics for port INT1:		
ipInReceives	:	0
ipInHeaderError:		0
ipInDiscards	:	0

**Table 78** Interface Protocol Statistics (/stats/port/ip)

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHeaderErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch).
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

**/stats/port <port alias or number>/link**  
**Link Statistics**

This menu enables you to display the link statistics of the selected port.

Link statistics for port INT1:		
linkStateChange:		1

**Table 79** Link Statistics (/stats/port/link)

Statistics	Description
linkStateChange	The total number of link state changes.

`/stats/port <port alias or number>/rmon`  
**RMON Statistics**

This menu enables you to display the Remote Monitoring (RMON) statistics of the selected port.

RMON statistics for port EXT2:	
etherStatsDropEvents:	NA
etherStatsOctets:	0
etherStatsPkts:	0
etherStatsBroadcastPkts:	0
etherStatsMulticastPkts:	0
etherStatsCRCAlignErrors:	0
etherStatsUndersizePkts:	0
etherStatsOversizePkts:	0
etherStatsFragments:	NA
etherStatsJabbers:	0
etherStatsCollisions:	0
etherStatsPkts64Octets:	0
etherStatsPkts65to127Octets:	0
etherStatsPkts128to255Octets:	0
etherStatsPkts256to511Octets:	0
etherStatsPkts512to1023Octets:	0
etherStatsPkts1024to1518Octets:	0

**Table 80** RMON Statistics (/stats/port/rmon)

Statistics	Description
etherStatsDropEvents	The total number of packets received that were dropped because of system resource constraints.
etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
etherStatsPkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address.
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address.

**Table 80** RMON Statistics (/stats/port/rmon)

Statistics	Description
etherStatsCRCAAlignErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsUndersizePkts	The total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
etherStatsFragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsJabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
etherStatsCollisions	The best estimate of the total number of collisions on this Ethernet segment.
etherStatsPkts64Octets	The total number of packets (including bad packets) received that were less than or equal to 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts65to127 Octets	The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts128to255 Octets	The total number of packets (including bad packets) received that were greater than 127 octets in length (excluding framing bits but including FCS octets).

**Table 80** RMON Statistics (/stats/port/rmon)

Statistics	Description
etherStatsPkts256to511 Octets	The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts512to1023 Octets	The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518 Octets	The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets).

## /stats/l2

# Layer 2 Statistics Menu

---

```
[Layer 2 Statistics Menu]
  amp      - AMP Stats Menu
  fdb      - Show FDB stats
  lacp     - Show LACP stats
  hotlink  - Show Hot Links stats
  lldp     - Show LLDP port stats
  oam      - Show OAM stats
```

The Layer 2 statistics provided by each menu option are briefly described in [Table 81](#), with pointers to detailed information.

**Table 81** Layer 2 Statistics Menu Options (/stats/l2)

---

### Command Syntax and Usage

---

#### **amp**

Displays Active MultiPath (AMP) statistics. See [page 182](#) for sample output.

---

#### **fdb** [**clear**]

Displays FDB statistics. See [page 184](#) for sample output.

Use the `clear` option to delete all FDB statistics.

---

#### **lacp** [*<port alias or number>*]**clear**

Displays Link Aggregation Control Protocol (LACP) statistics for a specified port, or for all ports if no port is specified. See [page 185](#) for sample output.

Use the `clear` option to delete all LACP statistics.

---

#### **hotlink**

Displays Hotlinks statistics. See [page 186](#) for sample output.

---

#### **lldp** [*<port alias or number>*]**clear**

Displays LLDP port statistics. See [page 187](#) for sample output.

---

#### **oam**

Displays the OAM Statistics menu. See [page 188](#) for sample output.

---

/stats/12/amp

## Active MultiPath Statistics

[AMP Statistics Menu]

group

- Show AMP group stats

dump

- Show all AMP port stats

clear

- Clear AMP stats

The following table describes the AMP statistics commands:

**Table 82** AMP Statistics Options

Command Syntax and Usage	
<b>group</b> [ <i>&lt;AMP group number&gt;</i> ]	Displays AMP statistics for the selected group. See <a href="#">page 183</a> for sample output.
<b>dump</b>	Displays all AMP statistics.
<b>clear</b> [ <i>&lt;AMP group number&gt;</i> ]	Clears AMP statistics.

`/stats/12/amp/group [<AMP group number>]`  
**Active MultiPath Group Statistics**

Group	Link	Keep-alive Sent	Pkts Rcvd	Fdb-Flush Sent	Pkts Rcvd	Pkts Dropped
1	Port EXT1	26	0	0	0	0
	Port EXT2	0	0	0	0	0

This displays shows AMP group statistics for an access switch. AMP statistics are described in the following table:

**Table 83** AMP Statistics

Statistic	Description
Group	AMP group number.
Link	Ports/portchannels (trunks) used for the AMP link.
Keep-alive Pkts Sent	Number of keep-alive packets sent.
Keep-alive Pkts Rcvd	Number of keep-alive packets received.
Fdb-Flush Pkts Sent	Number of FDB-flush packets sent.
Fdb-Flush Pkts Rcvd	Number of FDB-flush packets received.
Packets Dropped	Number of invalid AMP packets dropped.

`/stats/12/fdb [clear]`  
**FDB Statistics**

FDB statistics:			
current:	83	hiwat:	855

This menu option enables you to display statistics regarding the use of the forwarding database, including the number of new entries, finds, and unsuccessful searches.

FDB statistics are described in the following table:

**Table 84** Forwarding Database Statistics (/stats/fdb)

Statistic	Description
current	Current number of entries in the Forwarding Database.
hiwat	Highest number of entries recorded at any given time in the Forwarding Database.

Use the `clear` option to delete all FDB statistics.



`/stats/l2/lacp [<port alias or number>|clear]`  
**LACP Statistics**

Port EXT1:	
-----	
Valid LACPDUs received:	- 870
Valid Marker PDUs received:	- 0
Valid Marker Rsp PDUs received:	- 0
Unknown version/TLV type:	- 0
Illegal subtype received:	- 0
LACPDUs transmitted:	- 6031
Marker PDUs transmitted:	- 0
Marker Rsp PDUs transmitted:	- 0

Link Aggregation Control Protocol (LACP) statistics are described in the following table:

**Table 85** LACP Statistics (/stats/l2/lacp)

Statistic	Description
Valid LACPDUs received	Total number of valid LACP data units received.
Valid Marker PDUs received	Total number of valid LACP marker data units received.
Valid Marker Rsp PDUs received	Total number of valid LACP marker response data units received.
Unknown version/TLV type	Total number of LACP data units with an unknown version or type, length, and value (TLV) received.
Illegal subtype received	Total number of LACP data units with an illegal subtype received.
LACPDUs transmitted	Total number of LACP data units transmitted.
Marker PDUs transmitted	Total number of LACP marker data units transmitted.
Marker Rsp PDUs transmitted	Total number of LACP marker response data units transmitted.

Use the `clear` option to delete all LACP statistics.

`/stats/l2/hotlink`  
**Hotlinks Statistics**

```
Hot Links Trigger Stats:

Trigger 1 statistics:
  Trigger Name: Trigger 1
  Master active:           0
  Backup active:          0
  FDB update:             0   failed: 0
```

The following table describes the Hotlinks statistics:

**Table 86** Hotlinks Statistics (/stats/l2/hotlink)

Statistic	Description
Master active	Total number of times the Master interface transitioned to the Active state.
Backup active	Total number of times the Backup interface transitioned to the Active state.
FDB update	Total number of FDB update requests sent.
failed	Total number of FDB update requests that failed.

`/stats/l2/lldp <port alias or number> | clear`  
**LLDP Port Statistics**

LLDP Port INT1 Statistics	
-----	
Frames Transmitted	: 0
Frames Received	: 0
Frames Received in Errors	: 0
Frames Discarded	: 0
TLVs Unrecognized	: 0
Neighbors Aged Out	: 0
...	

The following table describes the LLDP port statistics:

**Table 87** LLDP port Statistics (/stats/l2/lldp)

Statistic	Description
Frames Transmitted	Total number of LLDP frames transmitted.
Frames Received	Total number of LLDP frames received.
Frames Received in Errors	Total number of LLDP frames that had errors.
Frames Discarded	Total number of LLDP frames discarded.
TLVs Unrecognized	Total number of unrecognized TLV (Type, Length, and Value) fields received.
Neighbors Aged Out	Total number of neighbor devices that have had their LLDP information aged out.

/stats/l2/oam  
OAM Statistics

[OAM statistics Menu]

port

- Show OAM port statistics

dump

- Show all OAM statistics

The following table describes the OAM statistics commands:

**Table 88** OAM Statistics Menu Options (/stats/l2)

Command Syntax and Usage

**port** *<port alias or number>*

Displays OAM statistics for the selected port. See [page 189](#) for sample output.

**dump**

Displays all OAM statistics.

`/stats/12/oam/port` *<port alias or number>*

## OAM Statistics

```
OAM statistics on port INT1
-----
Information OAMPDU Tx :      0
Information OAMPDU Rx :      0
Unsupported OAMPDU Tx :      0
Unsupported OAMPDU Rx :      0

Local faults
-----
    0 Link fault records
    0 Critical events
    0 Dying gasps

Remote faults
-----
    0 Link fault records
    0 Critical events
    0 Dying gasps
```

OAM statistics include the following:

- Total number of OAM Protocol Data Units (OAMPDU) transmitted and received.
- Total number of unsupported OAM Protocol Data Units (OAMPDU) transmitted and received.
- Local faults detected
- Remote faults detected

/stats/l3

## Layer 3 Statistics Menu

```
[Layer 3 Statistics Menu]
geal3      - GEA Layer 3 Stats Menu
ip         - Show IP stats
ip6        - Show IP6 stats
route      - Show route stats
route6     - Show route6 stats
arp        - Show ARP stats
dns        - Show DNS stats
icmp       - Show ICMP stats
tcp        - Show TCP stats
udp        - Show UDP stats
igmp       - Show IGMP stats
ospf       - OSPF stats
ospf3      - OSPFv3 stats
vrrp       - Show VRRP stats
rip        - Show RIP stats
igmpgrps   - Total number of IGMP groups
ipmcgrps   - Total number of IPMC groups
clrigmp    - Clear IGMP stats
ipclear    - Clear IP stats
ip6clear   - Clear IP6 stats
clrvrrp    - Clear VRRP stats
ripclear   - Clear RIP stats
ospfclr    - Clear all OSPF stats
ospf3clr   - Clear all OSPFv3 stats
dump       - Dump layer 3 stats
```

The Layer 3 statistics provided by each menu option are briefly described in [Table 89](#), with pointers to detailed information.

**Table 89** Layer 3 Statistics Menu Options (/stats/l3)

**Command Syntax and Usage**

**geal3**

Displays the Gigabit Ethernet Aggregators (GEA) statistics menu. GEA statistics are used by service and support personnel.

**ip**

Displays IP statistics. See [page 193](#) for sample output.

**ip6**

Displays IPv6 statistics. See [page 196](#) for sample output.

**Table 89** Layer 3 Statistics Menu Options (/stats/l3)

---

**Command Syntax and Usage**

---

**route [clear]**

Displays IPv4 route statistics. See [page 201](#) for sample output.

Use the `clear` option to delete all route statistics.

---

**route6 [clear]**

Displays IPv6 route statistics. See [page 202](#) for sample output.

Use the `clear` option to delete all route statistics.

---

**arp**

Displays Address Resolution Protocol (ARP) statistics. See [page 202](#) for sample output.

---

**dns [clear]**

Displays Domain Name System (DNS) statistics. See [page 203](#) for sample output.

Use the `clear` option to delete all DNS statistics.

---

**icmp [clear]**

Displays ICMP statistics. See [page 204](#) for sample output.

Use the `clear` option to delete all ICMP statistics.

---

**tcp [clear]**

Displays TCP statistics. See [page 206](#) for sample output.

Use the `clear` option to delete all TCP statistics.

---

**udp [clear]**

Displays UDP statistics. See [page 208](#) for sample output.

Use the `clear` option to delete all UDP statistics.

---

**igmp**

Displays IGMP statistics. See [page 209](#) for sample output.

---

**ospf**

Displays OSPF statistics. See [page 210](#) for sample output.

---

**ospf3**

Displays OSPFv3 statistics. See [page 215](#) for sample output.

---

**Table 89** Layer 3 Statistics Menu Options (/stats/l3)**Command Syntax and Usage****vrrp**

When virtual routers are configured, you can display the protocol statistics for VRRP. See [page 221](#) for sample output.

**rip**

Displays Routing Information Protocol (RIP) statistics. See [page 222](#) for sample output.

**igmpgrps**

Displays the total number of IGMP groups that are registered on the switch.

**ipmcgrps**

Displays the total number of current IP multicast groups that are registered on the switch.

**clrigmp**

Clears IGMP statistics.

**ipclear**

Clears IPv4 statistics. Use this command with caution as it will delete all the IPv4 statistics.

**ip6clear**

Clears IPv6 statistics. Use this command with caution as it will delete all the IPv6 statistics.

**clrvrrp**

Clears VRRP statistics.

**ripclear**

Clears Routing Information Protocol (RIP) statistics.

**ospfclr**

Clears Open Shortest Path First (OSPF) statistics.

**ospf3clr**

Clears OSPFv3 statistics.

**dump**

Dumps all Layer 3 statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command.



/stats/l3/ip  
IPv4 Statistics

IP statistics:			
ipInReceives:	3115873	ipInHdrErrors:	1
ipInAddrErrors:	35447	ipForwDatagrams:	0
ipInUnknownProtos:	500504	ipInDiscards:	0
ipInDelivers:	2334166	ipOutRequests:	1010542
ipOutDiscards:	4	ipOutNoRoutes:	4
ipReasmReqds:	0	ipReasmOKs:	0
ipReasmFails:	0	ipFragOKs:	0
ipFragFails:	0	ipFragCreates:	0
ipRoutingDiscards:	0	ipDefaultTTL:	255
ipReasmTimeout:	5		

Table 90 IP Statistics (stats/l3/ip)

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ipForwDatagrams	The number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets, which were Source-Routed via this entity (the switch), and the Source- Route option processing was successful.
ipInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

**Table 90** IP Statistics (stats/l3/ip)

Statistics	Description
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
ipOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
ipOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams, which meet this <i>no-route</i> criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
ipReasmReqds	The number of IP fragments received which needed to be reassembled at this entity (the switch).
ipReasmOKs	The number of IP datagrams successfully re- assembled.
ipReasmFails	The number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
ipFragOKs	The number of IP datagrams that have been successfully fragmented at this entity (the switch).
ipFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their Don't Fragment flag was set.

**Table 90** IP Statistics (stats/l3/ip)

Statistics	Description
ipFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch).
ipRoutingDiscards	The number of routing entries, which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
ipDefaultTTL	The default value inserted into the <code>Time-To-Live</code> (TTL) field of the IP header of datagrams originated at this entity (the switch), whenever a TTL value is not supplied by the transport layer protocol.
ipReasmTimeout	The maximum number of seconds, which received fragments are held while they are awaiting reassembly at this entity (the switch).

/stats/l3/ip6  
IPv6 Statistics

IPv6 Statistics					
*****					
144	Rcvd	0	HdrErrors	0	TooBigErrors
0	AddrErrors	0	FwdDgrams	0	UnknownProtos
0	Discards	144	Delivers	130	OutRequests
0	OutDiscards	0	OutNoRoutes	0	ReasmReqds
0	ReasmOKs	0	ReasmFails		
0	FragOKs	0	FragFails	0	FragCreates
7	RcvdMcastPkt	2	SentMcastPkts	0	TruncatedPkts
0	RcvdRedirects	0	SentRedirects		
ICMP Statistics					
*****					
Received :					
33	ICMPPkts	0	ICMPErrPkt	0	DestUnreach
0	ParmProbs	0	PktTooBigMsg	9	ICMPEchoReq
0	RouterSols	0	RouterAdv	5	NeighSols
0	Redirects	0	AdminProhib	0	ICMPBadCode
Sent					
19	ICMPMsgs	0	ICMPErrMsgs	0	DstUnReach
0	ParmProbs	0	PktTooBig	10	EchoReq
0	RouterSols	0	RouterAdv	11	NeighSols
0	RedirectMsgs	0	AdminProhibMsgs	5	NeighborAdv
UDP statistics					
*****					
Received :					
0	UDPDgrams	0	UDPNoPorts	0	UDPErrPkts
Sent :					
0	UDPDgrams				

The following table describes the IPv6 statistics.

Table 91 IPv6 Statistics (stats/l3/ip6)

Statistics	Description
Rcvd	Number of datagrams received from interfaces, including those received in error.
HdrErrors	Number of datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
TooBigErrors	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.

**Table 91** IPv6 Statistics (stats/l3/ip6)

Statistics	Description
AddrErrors	Number of datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses. For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
FwdDgrams	Number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets, which were Source-Routed via this entity (the switch), and the Source-Route option processing was successful.
UnknownProtos	Number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Discards	Number of IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
Delivers	Number of datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	Number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission.
OutDiscards	Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space).
OutNoRoutes	Number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
ReasmReqds	Number of IP fragments received which needed to be reassembled at this entity (the switch).
ReasmOKs	Number of IP datagrams successfully re- assembled.

**Table 91** IPv6 Statistics (stats/l3/ip6)

Statistics	Description
ReasmFails	Number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
FragOKs	Number of IP datagrams that have been successfully fragmented at this entity (the switch).
FragFails	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their <code>Don't Fragment</code> flag was set.
FragCreates	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch).
RcvdMcastPkt	The number of multicast packets received by the interface.
SentMcastPkts	The number of multicast packets transmitted by the interface.
TruncatedPkts	The number of input datagrams discarded because datagram frame didn't carry enough data.
RcvdRedirects	The number of Redirect messages received by the interface.
SentRedirects	The number of Redirect messages sent.

The following table describes the IPv6 ICMP statistics.

**Table 92** ICMP Statistics (stats/l3/ip6)

Statistics	Description
<b>Received</b>	
ICMPPkts	Number of ICMP messages which the entity (the switch) received.
ICMPErrPkt	Number of ICMP messages which the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so forth).
DestUnreach	Number of ICMP Destination Unreachable messages received.
TimeExcds	Number of ICMP Time Exceeded messages received.
ParmProbs	Number of ICMP Parameter Problem messages received.
PktTooBigMsg	The number of ICMP Packet Too Big messages received by the interface.

**Table 92** ICMP Statistics (stats/l3/ip6)

Statistics	Description
ICMPEchoReq	Number of ICMP Echo (request) messages received.
ICMPEchoReps	Number of ICMP Echo Reply messages received.
RouterSols	Number of Router Solicitation messages received by the switch.
RouterAdv	Number of Router Advertisements received by the switch.
NeighSols	Number of Neighbor Solicitations received by the switch.
NeighAdv	Number of Neighbor Advertisements received by the switch.
Redirects	Number of ICMP Redirect messages received.
AdminProhib	The number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
ICMPBadCode	The number of ICMP Parameter Problem messages received by the interface.
<b>Sent</b>	
ICMPMsgs	Number of ICMP messages which this entity (the switch) attempted to send.
ICMPErrMsgs	Number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
DstUnReach	Number of ICMP Destination Unreachable messages sent.
TimeExcds	Number of ICMP Time Exceeded messages sent.
ParmProbs	Number of ICMP Parameter Problem messages sent.
PktTooBigs	The number of ICMP Packet Too Big messages sent by the interface.
EchoReq	Number of ICMP Echo (request) messages sent.
EchoReply	Number of ICMP Echo Reply messages sent.
RouterSols	Number of Router Solicitation messages sent by the switch.
RouterAdv	Number of Router Advertisements sent by the switch.
NeighSols	Number of Neighbor Solicitations sent by the switch.
NeighAdv	Number of Neighbor Advertisements sent by the switch.

Table 92 ICMP Statistics (stats/l3/ip6)

Statistics	Description
RedirectMsgs	Number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
AdminProhibMsgs	Number of ICMP destination unreachable/communication administratively prohibited messages sent.

The following table describes the UDP statistics.

Table 93 UDP Statistics (stats/l3/ip6)

Statistics	Description
Received	
UDPDgrams	Number of UDP datagrams received by the switch.
UDPNoPorts	Number of received UDP datagrams for which there was no application at the destination port.
UDPErrPkts	Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Sent	
UDPDgrams	Number of UDP datagrams sent from this entity (the switch).

/stats/l3/route [clear]  
IPv4 Route Statistics

Route statistics:			
ipRoutesCur:	11	ipRoutesHighWater:	11
ipRoutesMax:	4096		

Table 94 Route Statistics (/stats/l3/route)

Statistics	Description
ipRoutesCur	The total number of outstanding routes in the route table.
ipRoutesHighWater	The highest number of routes ever recorded in the route table.
ipRoutesMax	The maximum number of routes that are supported.

Use the `clear` option to delete all IPv4 route statistics.



`/stats/l3/route6 [clear]`  
**IPv6 Route Statistics**

```
IPV6 Route statistics:
ipv6RoutesCur:          1  ipv6RoutesHighWater:      1
ipv6RoutesMax:          1880
```

**Table 95** Route Statistics (/stats/l3/route)

Statistics	Description
ipv6RoutesCur	The total number of outstanding routes in the route table.
ipv6RoutesHighWater	The highest number of routes ever recorded in the route table.
ipv6RoutesMax	The maximum number of routes that are supported.

Use the `clear` option to delete all IPv6 route statistics.

`/stats/l3/arp`  
**ARP Statistics**

This menu option enables you to display Address Resolution Protocol statistics.

```
ARP statistics:
arpEntriesCur:          3  arpEntriesHighWater:      4
arpEntriesMax:          4095
```

**Table 96** ARP Statistics (/stats/l3/arp)

Statistics	Description
arpEntriesCur	The total number of outstanding ARP entries in the ARP table.
arpEntriesHighWater	The highest number of ARP entries ever recorded in the ARP table.
arpEntriesMax	The maximum number of ARP entries that are supported.

`/stats/13/dns [clear]`  
**DNS Statistics**

This menu option enables you to display Domain Name System statistics.

DNS statistics:	
dnsOutRequests:	0
dnsBadRequests:	0

**Table 97** DNS Statistics (/stats/dns)

Statistics	Description
dnsOutRequests	The total number of DNS response packets that have been transmitted.
dnsBadRequests	The total number of DNS request packets received that were dropped.

Use the `clear` option to delete all DNS statistics.

`/stats/l3/icmp [clear]`  
**ICMP Statistics**

ICMP statistics:			
icmpInMsgs:	245802	icmpInErrors:	1393
icmpInDestUnreachs:	41	icmpInTimeExcds:	0
icmpInParmProbs:	0	icmpInSrcQuenchs:	0
icmpInRedirects:	0	icmpInEchos:	18
icmpInEchoReps:	244350	icmpInTimestamps:	0
icmpInTimestampReps:	0	icmpInAddrMasks:	0
icmpInAddrMaskReps:	0	icmpOutMsgs:	253810
icmpOutErrors:	0	icmpOutDestUnreachs:	15
icmpOutTimeExcds:	0	icmpOutParmProbs:	0
icmpOutSrcQuenchs:	0	icmpOutRedirects:	0
icmpOutEchos:	253777	icmpOutEchoReps:	18
icmpOutTimestamps:	0	icmpOutTimestampReps:	0
icmpOutAddrMasks:	0	icmpOutAddrMaskReps:	0

**Table 98** ICMP Statistics (/stats/l3/icmp)

Statistics	Description
icmpInMsgs	The total number of ICMP messages which the entity (the switch) received. Note that this counter includes all those counted by icmpInErrors.
icmpInErrors	The number of ICMP messages which the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so forth).
icmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
icmpInTimeExcds	The number of ICMP Time Exceeded messages received.
icmpInParmProbs	The number of ICMP Parameter Problem messages received.
icmpInSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages received.
icmpInRedirects	The number of ICMP Redirect messages received.
icmpInEchos	The number of ICMP Echo (request) messages received.
icmpInEchoReps	The number of ICMP Echo Reply messages received.
icmpInTimestamps	The number of ICMP Timestamp (request) messages received.
icmpInTimestampReps	The number of ICMP Timestamp Reply messages received.

**Table 98** ICMP Statistics (/stats/l3/icmp)

Statistics	Description
icmpInAddrMasks	The number of ICMP Address Mask Request messages received.
icmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
icmpOutMsgs	The total number of ICMP messages which this entity (the switch) attempted to send. Note that this counter includes all those counted by icmpOutErrors.
icmpOutErrors	The number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
icmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
icmpOutSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages sent.
icmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
icmpOutEchos	The number of ICMP Echo (request) messages sent.
icmpOutEchoReps	The number of ICMP Echo Reply messages sent.
icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.
icmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

Use the `clear` option to delete all ICMP statistics.

/stats/l3/tcp [clear]  
TCP Statistics

TCP statistics:			
tcpRtoAlgorithm:	4	tcpRtoMin:	0
tcpRtoMax:	240000	tcpMaxConn:	512
tcpActiveOpens:	252214	tcpPassiveOpens:	7
tcpAttemptFails:	528	tcpEstabResets:	4
tcpInSegs:	756401	tcpOutSegs:	756655
tcpRetransSegs:	0	tcpInErrs:	0
tcpCurBuff:	0	tcpCurConn:	3
tcpOutRsts:	417		

Table 99 TCP Statistics (/stats/l3/tcp)

Statistics	Description
tcpRtoAlgorithm	The algorithm used to determine the <code>timeout</code> value used for retransmitting unacknowledged octets.
tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission <code>timeout</code> , measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission <code>timeout</code> . In particular, when the <code>timeout</code> algorithm is <code>rsre(3)</code> , an object of this type has the semantics of the <code>LBOUND</code> quantity described in RFC 793.
tcpRtoMax	The maximum value permitted by a TCP implementation for the retransmission <code>timeout</code> , measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission <code>timeout</code> . In particular, when the <code>timeout</code> algorithm is <code>rsre(3)</code> , an object of this type has the semantics of the <code>UBOUND</code> quantity described in RFC 793.
tcpMaxConn	The limit on the total number of TCP connections the entity (the switch) can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.
tcpActiveOpens	The number of times TCP connections have made a direct transition to the <code>SYN-SENT</code> state from the <code>CLOSED</code> state.
tcpPassiveOpens	The number of times TCP connections have made a direct transition to the <code>SYN-RCVD</code> state from the <code>LISTEN</code> state.

**Table 99** TCP Statistics (/stats/l3/tcp)

Statistics	Description
tcpAttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
tcpEstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
tcpInSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
tcpInErrs	The total number of segments received in error (for example, bad TCP checksums).
tcpCurBuff	The total number of outstanding memory allocations from heap by TCP protocol stack.
tcpCurConn	The total number of outstanding TCP sessions that are currently opened.
tcpOutRsts	The number of TCP segments sent containing the RST flag.

Use the `clear` option to delete all TCP statistics.

`/stats/l3/udp [clear]`  
**UDP Statistics**

UDP statistics:			
udpInDatagrams:	54	udpOutDatagrams:	43
udpInErrors:	0	udpNoPorts:	1578077

**Table 100** UDP Statistics (/stats/l3/udp)

Statistics	Description
udpInDatagrams	The total number of UDP datagrams delivered to the switch.
udpOutDatagrams	The total number of UDP datagrams sent from this entity (the switch).
udpInErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpNoPorts	The total number of received UDP datagrams for which there was no application at the destination port.

Use the `clear` option to delete all UDP statistics.

`/stats/l3/igmp <VLAN number>`  
**IGMP Statistics**

IGMP Snoop vlan 2 statistics:			
-----			
rxIgmpValidPkts:	0	rxIgmpInvalidPkts:	0
rxIgmpGenQueries:	0	rxIgmpGrpSpecificQueries:	0
rxIgmpGroupSrcSpecificQueries:	0		
rxIgmpLeaves:	0	rxIgmpReports:	0
txIgmpReports:	0	txIgmpGrpSpecificQueries:	0
txIgmpLeaves:	0	rxIgmpV3CurrentStateRecords:	0
rxIgmpV3SourceListChangeRecords:	0	rxIgmpV3FilterChangeRecords:	0

This menu option displays statistics about the use of the IGMP Multicast Groups. IGMP statistics are described in the following table:

**Table 101** IGMP Statistics (/stats/l3/igmp)

Statistic	Description
rxIgmpValidPkts	Total number of valid IGMP packets received
rxIgmpInvalidPkts	Total number of invalid packets received
rxIgmpGenQueries	Total number of General Membership Query packets received
rxIgmpGrpSpecific Queries	Total number of Membership Query packets received from specific groups
rxIgmpGroupSrcSpecific Queries	Total number of Group Source-Specific Queries (GSSQ) received
rxIgmpLeaves	Total number of Leave requests received
rxIgmpReports	Total number of Membership Reports received
txIgmpReports	Total number of Membership reports transmitted
txIgmpGrpSpecific Queries	Total number of Membership Query packets transmitted to specific groups
txIgmpLeaves	Total number of Leave messages transmitted
rxIgmpV3CurrentState Records	Total number of Current State records received
rxIgmpV3SourceList ChangeRecords	Total number of Source List Change records received.
rxIgmpV3FilterChange Records	Total number of Filter Change records received.



/stats/l3/ospf  
OSPF Statistics Menu

[OSPF stats Menu]	
general	- Show global stats
aindex	- Show area(s) stats
if	- Show interface(s) stats

Table 102 OSPF Statistics Menu (/stats/l3/ospf)

---

Command Syntax and Usage

---

**general**

Displays global statistics. See [page 211](#) for sample output.

---

**aindex**

Displays area statistics.

---

**if**

Displays interface statistics.

---

## /stats/13/ospf/general

### OSPF Global Statistics

The OSPF General Statistics contain the sum total of all OSPF packets received on all OSPF areas and interfaces.

OSPF stats			
-----			
Rx/Tx Stats:	Rx	Tx	
	-----	-----	
Pkts	0	0	
hello	23	518	
database	4	12	
ls requests	3	1	
ls acks	7	7	
ls updates	9	7	
Nbr change stats:		Intf change Stats:	
hello	2	hello	4
start	0	down	2
n2way	2	loop	0
adjoint ok	2	unloop	0
negotiation done	2	wait timer	2
exchange done	2	backup	0
bad requests	0	nbr change	5
bad sequence	0		
loading done	2		
nlway	0		
rst_ad	0		
down	1		
Timers kickoff			
hello	514		
retransmit	1028		
lsa lock	0		
lsa ack	0		
dbage	0		
summary	0		
ase export	0		

**Table 103** OSPF General Statistics (stats/l3/ospf/general)

Statistics	Description
<b>Rx/Tx Stats:</b>	
Rx Pkts	The sum total of all OSPF packets received on all OSPF areas and interfaces.
Tx Pkts	The sum total of all OSPF packets transmitted on all OSPF areas and interfaces.
Rx Hello	The sum total of all Hello packets received on all OSPF areas and interfaces.
Tx Hello	The sum total of all Hello packets transmitted on all OSPF areas and interfaces.
Rx Database	The sum total of all Database Description packets received on all OSPF areas and interfaces.
Tx Database	The sum total of all Database Description packets transmitted on all OSPF areas and interfaces.
Rx ls Requests	The sum total of all Link State Request packets received on all OSPF areas and interfaces.
Tx ls Requests	The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces.
Rx ls Acks	The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces.
Tx ls Acks	The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces.
Rx ls Updates	The sum total of all Link State Update packets received on all OSPF areas and interfaces.
Tx ls Updates	The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces.
<b>Nbr Change Stats:</b>	
hello	The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces.
Start	The sum total number of neighbors in this state (that is, an indication that Hello packets should now be sent to the neighbor at intervals of <code>HelloInterval</code> seconds.) across all OSPF areas and interfaces.

**Table 103** OSPF General Statistics (stats/l3/ospf/general) (continued)

Statistics	Description
n2way	The sum total number of bidirectional communication establishment between this router and other neighboring routers.
adjoint ok	The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the neighbor across all OSPF areas and interfaces.
negotiation done	The sum total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces.
exchange done	The sum total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPF areas and interfaces.
bad requests	The sum total number of Link State Requests which have been received for a link state advertisement not contained in the database across all interfaces and OSPF areas.
bad sequence	<p>The sum total number of Database Description packets which have been received that either:</p> <ul style="list-style-type: none"> <li>a. Has an unexpected DD sequence number</li> <li>b. Unexpectedly has the init bit set</li> <li>c. Has an options field differing from the last Options field received in a Database Description packet.</li> </ul> <p>Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.</p>
loading done	The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces.
n1way	The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas.
rst_ad	The sum total number of times the Neighbor adjacency has been reset across all OPSF areas and interfaces.
down	The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation.) across all OSPF areas and interfaces.

**Table 103** OSPF General Statistics (stats/l3/ospf/general) (continued)

Statistics	Description
<b>Intf Change Stats:</b>	
hello	The sum total number of Hello packets sent on all interfaces and areas.
down	The sum total number of interfaces down in all OSPF areas.
loop	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
unloop	The sum total number of interfaces, connected to the attached network in all OSPF areas.
wait timer	The sum total number of times the Wait Timer has been fired, indicating the end of the waiting period that is required before electing a (Backup) Designated Router across all OSPF areas and interfaces.
backup	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
nbr change	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.
<b>Timers Kickoff:</b>	
hello	The sum total number of times the Hello timer has been fired (which triggers the send of a Hello packet) across all OPSF areas and interfaces.
retransmit	The sum total number of times the Retransmit timer has been fired across all OPSF areas and interfaces.
lsa lock	The sum total number of times the Link State Advertisement (LSA) lock timer has been fired across all OSPF areas and interfaces.
lsa ack	The sum total number of times the LSA Ack timer has been fired across all OSPF areas and interfaces.
dbage	The total number of times the data base age (Dbage) has been fired.
summary	The total number of times the Summary timer has been fired.
ase export	The total number of times the Autonomous System Export (ASE) timer has been fired.

/stats/l3/ospf3

## OSPFv3 Statistics Menu

[OSPFV3 stats Menu]

general

- Show global stats

aindex

- Show area(s) stats

if

- Show interface(s) stats

Table 104 OSPFv3 Statistics Menu (/stats/l3/ospf3)

Command Syntax and Usage

general

Displays global statistics. See [page 217](#) for sample output.

aindex

Displays area statistics.

if

Displays interface statistics.

/stats/l3/ospf3

## OSPFv3 Statistics Menu

[OSPFV3 stats Menu]	
general	- Show global stats
aindex	- Show area(s) stats
if	- Show interface(s) stats

**Table 105** OSPFv3 Statistics Menu (/stats/l3/ospf3)

---

**Command Syntax and Usage**

---

**general**

Displays global statistics. See [page 217](#) for sample output.

---

**aindex**

Displays area statistics.

---

**if**

Displays interface statistics.

---

/stats/l3/ospf3/general  
OSPFv3 Global Statistics

OSPFv3 stats			
-----			
Rx/Tx/Disd Stats:	Rx	Tx	Discarded
	-----	-----	-----
Pkts	9695	95933	0
hello	9097	8994	0
database	39	51	6
ls requests	16	8	0
ls acks	172	360	0
ls updates	371	180	0
Nbr change stats:		Intf change Stats:	
down	0	down	5
attempt	0	loop	0
init	1	waiting	6
n2way	1	ptop	0
exstart	1	dr	4
exchange done	1	backup	6
loading done	1	dr other	0
full	1	all events	33
all events	6		
Timers kickoff			
hello	8988		
wait	6		
poll	0		
nbr probe	0		
Number of LSAs			
originated		180	
rcvd newer originations		355	

The OSPFv3 General Statistics contain the sum total of all OSPF packets received on all OSPFv3 areas and interfaces.

Table 106 OSPFv3 General Statistics (stats/l3/ospf3/general)

Statistics	Description
Rx/Tx Stats:	
Rx Pkts	The sum total of all OSPFv3 packets received on all OSPFv3 interfaces.
Tx Pkts	The sum total of all OSPFv3 packets transmitted on all OSPFv3 interfaces.
Discarded Pkts	The sum total of all OSPFv3 packets discarded.



**Table 106** OSPFv3 General Statistics (stats/l3/ospf3/general) (continued)

Statistics	Description
Rx hello	The sum total of all Hello packets received on all OSPFv3 interfaces.
Tx hello	The sum total of all Hello packets transmitted on all OSPFv3 interfaces.
Discarded hello	The sum total of all Hello packets discarded, including packets for which no associated interface has been found.
Rx database	The sum total of all Database Description packets received on all OSPFv3 interfaces.
Tx database	The sum total of all Database Description packets transmitted on all OSPFv3 interfaces.
Discarded database	The sum total of all Database Description packets discarded.
Rx ls requests	The sum total of all Link State Request packets received on all OSPFv3 interfaces.
Tx ls requests	The sum total of all Link State Request packets transmitted on all OSPFv3 interfaces.
Discarded ls requests	The sum total of all Link State Request packets discarded.
Rx ls acks	The sum total of all Link State Acknowledgement packets received on all OSPFv3 interfaces.
Tx ls acks	The sum total of all Link State Acknowledgement packets transmitted on all OSPFv3 interfaces.
Discarded ls acks	The sum total of all Link State Acknowledgement packets discarded.
Rx ls updates	The sum total of all Link State Update packets received on all OSPFv3 interfaces.
Tx ls updates	The sum total of all Link State Update packets transmitted on all OSPFv3 interfaces.
Discarded ls updates	The sum total of all Link State Update packets discarded.
<b>Nbr Change Stats:</b>	
down	The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation.) across all OSPFv3 interfaces.

**Table 106** OSPFv3 General Statistics (stats/l3/ospf3/general) (continued)

Statistics	Description
attempt	The total number of transitions into attempt state of neighboring routers across all OSPFv3 interfaces.
init	The total number of transitions into init state of neighboring routers across all OSPFv3 interfaces.
n2way	The total number of bidirectional communication establishment between this router and other neighboring routers.
exstart	The total number of transitions into exstart state of neighboring routers across all OSPFv3 interfaces
exchange done	The total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPFv3 interfaces.
loading done	The total number of link state updates received for all out-of-date portions of the database across all OSPFv3 interfaces.
full	The total number of transitions into full state of neighboring routers across all OSPFv3 interfaces.
all events	The total number of state transitions of neighboring routers across all OSPFv3 interfaces.

**Table 106** OSPFv3 General Statistics (stats/l3/ospf3/general) (continued)

Statistics	Description
<b>Intf Change Stats:</b>	
down	The total number of transitions into down state of all OSPFv3 interfaces.
loop	The total number of transitions into loopback state of all OSPFv3 interfaces.
waiting	The total number of transitions into waiting state of all OSPFv3 interfaces.
ptop	The total number of transitions into point-to-point state of all OSPFv3 interfaces.
dr	The total number of transitions into Designated Router other state of all OSPFv3 interfaces.
backup	The total number of transitions into backup state of all OSPFv3 interfaces.
all events	The total number of changes associated with any OSPFv3 interface, including changes into internal states.
<b>Timers Kickoff:</b>	
hello	The total number of times the Hello timer has been fired (which triggers the send of a Hello packet) across all OSPFv3 interfaces.
wait	The total number of times the wait timer has been fired (which causes an interface to exit waiting state), across all OPSFv3 interfaces.
poll	The total number of times the timer whose firing causes hellos to be sent to inactive NBMA and Demand Circuit neighbors has been fired, across all OPSFv3 interfaces.
nbr probe	The total number of times the neighbor probe timer has been fired, across all OPSFv3 interfaces.
<b>Number of LSAs:</b>	
originated	The number of LSAs originated by this router.
rcvd newer originations	The number of LSAs received that have been determined to be newer originations.

/stats/l3/vrrp  
VRRP Statistics

Virtual Router Redundancy Protocol (VRRP) support on the Virtual Fabric 10Gb Switch Module (VFSM) provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

When virtual routers are configured, you can display the protocol statistics for VRRP:

VRRP statistics:			
vrrpInAdvers:	0	vrrpBadAdvers:	0
vrrpOutAdvers:	0		
vrrpBadVersion:	0	vrrpBadVrid:	0
vrrpBadAddress:	0	vrrpBadData:	0
vrrpBadPassword:	0	vrrpBadInterval:	0

Table 107 VRRP Statistics (/stats/l3/vrrp)

Statistics	Description
vrrpInAdvers	The total number of valid VRRP advertisements that have been received.
vrrpBadAdvers	The total number of VRRP advertisements received that were dropped.
vrrpOutAdvers	The total number of VRRP advertisements that have been sent.
vrrpBadVersion	The total number of VRRP advertisements received that had a bad version number.
vrrpBadVrid	The total number of VRRP advertisements received that had a bad virtual router ID.
vrrpBadAddress	The total number of VRRP advertisements received that had a bad address.
vrrpBadData	The total number of VRRP advertisements received that had bad data.
vrrpBadPassword	The total number of VRRP advertisements received that had a bad password.
vrrpBadInterval	The total number of VRRP advertisements received that had a bad interval.

`/stats/13/rip`

## Routing Information Protocol Statistics

```
RIP ALL STATS INFORMATION:
    RIP packets received = 12
    RIP packets sent     = 75
    RIP request received = 0
    RIP response received = 12
    RIP request sent     = 3
    RIP reponse sent     = 72
    RIP route timeout    = 0
    RIP bad size packet received = 0
    RIP bad version received = 0
    RIP bad zeros received  = 0
    RIP bad src port received = 0
    RIP bad src IP received = 0
    RIP packets from self received = 0
```

/stats/mp

# Management Processor Statistics Menu

[MP-specific Statistics Menu]	
thr	- Show STEM thread stats
i2c	- Show I2C stats
pkt	- Show Packet stats
tcb	- Show All TCP control blocks in use
ucb	- Show All UDP control blocks in use
cpu	- Show CPU utilization
mem	- Show Memory utilization stats

**Table 108** Management Processor Statistics Menu Options (/stats/mp)

**Command Syntax and Usage**

**thr**

Displays STEM thread statistics. This command is used by Technical Support personnel.

**i2c**

Displays I2C statistics. This command is used by Technical Support personnel.

**pkt**

Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see [page 224](#).

**tcb**

Displays all TCP control blocks that are in use. To view a sample output and a description of the stats, see [page 225](#).

**ucb**

Displays all UDP control blocks that are in use. To view a sample output, see [page 226](#).

**cpu**

Displays CPU utilization for periods of up to 1, 4, and 64 seconds. To view a sample output and a description of the stats, see [page 226](#).

**mem**

Displays system memory statistics.

/stats/mp/pkt  
MP Packet Statistics

Packet counts seen by MP:	
allocs:	859
frees:	859
failures:	0
small packet buffers:	
-----	
current:	0
hi-watermark:	4
hi-water time:	17:56:35 Tue Jul 14, 2009
medium packet buffers:	
-----	
current:	0
hi-watermark:	1
hi-water time:	17:56:16 Tue Jul 14, 2009
jumbo packet buffers:	
-----	
current:	0
hi-watermark:	0

Table 109 Packet Statistics (/stats/mp/pkt)

Statistics	Description
allocs	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
frees	Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack.
failures	Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack.
small packet buffers	
current	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-watermark	The highest number of packet allocation with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.
medium packet buffers	

Table 109 Packet Statistics (/stats/mp/pkt)

Statistics	Description
current	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-watermark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.
<b>jumbo packet buffers</b>	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.

/stats/mp/tcb  
TCP Statistics

All TCP allocated control blocks:			
10ad41e8:	0.0.0.0	0 <=> 0.0.0.0	80 listen
10ad5790:	47.81.27.5	1171 <=> 47.80.23.243	23 established

Table 110 MP Specified TCP Statistics (/stats/mp/tcb)

Statistics	Description
10ad41e8/10ad5790	Memory
0.0.0.0/47.81.27.5	Destination IP address
0/1171	Destination port
0.0.0.0/47.80.23.243	Source IP
80/23	Source port
listen/established	State



`/stats/mp/ucb`  
**UCB Statistics**

```
All UDP allocated control blocks:
161:  listen
```

`/stats/mp/cpu`  
**CPU Statistics**

This menu option enables you to display the CPU utilization statistics.

```
CPU utilization:
cpuUtil1Second:      53%
cpuUtil4Seconds:     54%
cpuUtil64Seconds:    54%
```

**Table 111** CPU Statistics (stats/mp/cpu)

Statistics	Description
cpuUtil1Second	The utilization of MP CPU over 1 second. It shows the percentage.
cpuUtil4Seconds	The utilization of MP CPU over 4 seconds. It shows the percentage.
cpuUtil64Seconds	The utilization of MP CPU over 64 seconds. It shows the percentage.

/stats/acl

## ACL Statistics Menu

[ACL Menu]

acl

- Display ACL stats

dump

- Display all available ACL stats

vmap

- Display VMAP stats

clracl

- Clear ACL stats

clrvmap

- Clear VMAP stats

ACL statistics are described in the following table.

**Table 112** ACL Statistics Menu Options (/stats/acl)

**Command Syntax and Usage**

**acl** <ACL number>

Displays the Access Control List Statistics for a specific ACL. For details, see [page 227](#).

**dump**

Displays all ACL statistics.

**vmap** <VMAP number>

Displays the VLAN Map statistics for a specific VMAP. For details, see [page 228](#).

**clracl**

Clears all ACL statistics.

**clrvmap**

Clears all VMAP statistics.

/stats/acl/acl [<ACL number>]

## ACL Statistics List

This option displays statistics for the selected ACL if an ACL number is specified, or for all ACLs if the option is omitted.

Hits for ACL 1:	26057515
Hits for ACL 2:	26057497

`/stats/acl/vmap [<VMAP number> | all]`  
**VLAN Map Statistics**

This option displays statistics for the selected VLAN Map, or for all VMAPs.

Hits for VMAP 1:	57515
Hits for VMAP 2:	74970

`/stats/fcoe [clear]`

## Fiber Channel over Ethernet Statistics

FCOE statistics:			
FCFAdded:	5	FCFRemoved:	1
FCOEAdded:	81	FCOERemoved:	24

Fiber Channel over Ethernet (FCoE) statistics are described in the following table:

**Table 113** FCoE Statistics (/stats/fcoe)

Statistic	Description
FCFAdded	Total number of FCoE Forwarders (FCF) added.
FCFRemoved	Total number of FCoE Forwarders (FCF) removed.
FCOEAdded	Total number of FCoE connections added.
FCOERemoved	Total number of FCoE connections removed.

The total can accumulate over several FCoE sessions, until the statistics are cleared.

/stats/snmp [clear]  
**SNMP Statistics**

**Note** – You can reset the SNMP counter to zero by using `clear` command, as follows:  
>> Statistics# **snmp clear**

SNMP statistics:			
snmpInPkts:	150097	snmpInBadVersions:	0
snmpInBadC'tyNames:	0	snmpInBadC'tyUses:	0
snmpInASNParseErrs:	0	snmpEnableAuthTraps:	0
snmpOutPkts:	150097	snmpInBadTypes:	0
snmpInTooBigs:	0	snmpInNoSuchNames:	0
snmpInBadValues:	0	snmpInReadOnlys:	0
snmpInGenErrs:	0	snmpInTotalReqVars:	798464
snmpInTotalSetVars:	2731	snmpInGetRequests:	17593
snmpInGetNexts:	131389	snmpInSetRequests:	615
snmpInGetResponses:	0	snmpInTraps:	0
snmpOutTooBigs:	0	snmpOutNoSuchNames:	1
snmpOutBadValues:	0	snmpOutReadOnlys:	0
snmpOutGenErrs:	1	snmpOutGetRequests:	0
snmpOutGetNexts:	0	snmpOutSetRequests:	0
snmpOutGetResponses:	150093	snmpOutTraps:	4
snmpSilentDrops:	0	snmpProxyDrops:	0

**Table 114** SNMP Statistics (/stats/snmp)

Statistics	Description
snmpInPkts	The total number of Messages delivered to the SNMP entity from the transport service.
snmpInBadVersions	The total number of SNMP Messages, which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
snmpInBadC'tyNames	The total number of SNMP Messages delivered to the SNMP entity which used an SNMP community name not known to the said entity (the switch).
snmpInBadC'tyUses	The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message.

**Table 114** SNMP Statistics (/stats/snmp)

Statistics	Description
snmpInASNParseErrs	<p>The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding SNMP Messages received.</p> <p><b>Note:</b> OSI's method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209). ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences. BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.</p>
snmpEnableAuthTraps	An object to enable or disable the authentication traps generated by this entity (the switch).
snmpOutPkts	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
snmpInBadTypes	The total number of SNMP Messages which failed ASN parsing.
snmpInTooBigs	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>too big</i> .
snmpInNoSuchNames	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>noSuchName</i> .
snmpInBadValues	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>badValue</i> .
snmpInReadOnlys	The total number of valid SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>'read-Only'</i> . It should be noted that it is a protocol error to generate an SNMP PDU, which contains the value <i>'read-Only'</i> in the error-status field. As such, this object is provided as a means of detecting incorrect implementations of the SNMP.
snmpInGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>genErr</i> .

**Table 114** SNMP Statistics (/stats/snmp)

Statistics	Description
snmpInTotalReqVars	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as a result of receiving valid SNMP Get-Request and Get-Next Protocol Data Units (PDUs).
snmpInTotalSetVars	The total number of MIB objects, which have been altered successfully by the SNMP protocol entity as a result of receiving valid SNMP Set-Request Protocol Data Units (PDUs).
snmpInGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpOutTooBig	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is <i>too big</i> .
snmpOutNoSuchNames	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status is <i>noSuchName</i> .
snmpOutBadValues	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is <i>badValue</i> .
snmpOutReadOnly	Not in use.
snmpOutGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is <i>genErr</i> .
snmpOutGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.

**Table 114** SNMP Statistics (/stats/snmp)

Statistics	Description
snmpOutGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGet Responses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpSilentDrops	The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMPv2 entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
snmpProxyDrops	The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the transmission of the message to a proxy target failed in a manner such that no Response-PDU could be returned.



/stats/ntp

# NTP Statistics

BLADEOS uses NTP (Network Timing Protocol) version 3 to synchronize the switch’s internal clock with an atomic time calibrated NTP server. With NTP enabled, the switch can accurately update its internal clock to be consistent with other devices on the network and generates accurate syslogs.

```
NTP statistics:
  Primary Server:
    Requests Sent:           17
    Responses Received:      17
    Updates:                 1
  Secondary Server:
    Requests Sent:           0
    Responses Received:      0
    Updates:                 0

Last update based on response from primary/secondary server.
Last update time: 18:04:16 Tue Jul 13, 2009
Current system time: 18:55:49 Tue Jul 13, 2009
```

**Table 115** NTP Statistics Parameters (/stats/ntp)

Field	Description
Primary Server	<ul style="list-style-type: none"><li>■ <b>Requests Sent:</b> The total number of NTP requests the switch sent to the primary NTP server to synchronize time.</li><li>■ <b>Responses Received:</b> The total number of NTP responses received from the primary NTP server.</li><li>■ <b>Updates:</b> The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.</li></ul>
Secondary Server	<ul style="list-style-type: none"><li>■ <b>Requests Sent:</b> The total number of NTP requests the switch sent to the secondary NTP server to synchronize time.</li><li>■ <b>Responses Received:</b> The total number of NTP responses received from the secondary NTP server.</li><li>■ <b>Updates:</b> The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server.</li></ul>

**Table 115** NTP Statistics Parameters (/stats/ntp)

Field	Description
Last update based on response from primary server	Last update of time on the switch based on either primary or secondary NTP response received.
Last update time	The time stamp showing the time when the switch was last updated.
Current system time	The switch system time when the following command was issued: /stats/ntp

**Note –** Use the following command to delete all NTP statistics: /stats/ntp clear

/stats/dump

## Statistics Dump

Use the dump command to dump all switch statistics available from the Statistics Menu (40K or more, depending on your configuration). This data can be used to tune or debug switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

## CHAPTER 6

# The Configuration Menu

---

This chapter discusses how to use the Command Line Interface (CLI) for making, viewing, and saving switch configuration changes. Many of the commands, although not new, display more or different information than in the previous version. Important differences are called out in the text.

### /cfg

## Configuration Menu

---

```
[Configuration Menu]
  sys      - System-wide Parameter Menu
  port     - Port Menu
  stack    - Stacking Menu
  qos      - QOS Menu
  acl      - Access Control List Menu
  pmirr    - Port Mirroring Menu
  l2       - Layer 2 Menu
  l3       - Layer 3 Menu
  cee      - CEE Configuration Menu
  fcoe     - Fiber Channel Over Ethernet Configuration Menu
  rmon     - RMON Menu
  virt     - Virtualization Menu
  setup    - Step by step configuration set up
  dump     - Dump current configuration to script file
  ptcfg    - Backup current configuration to FTP/TFTP server
  gtcfg    - Restore current configuration from FTP/TFTP server
  cur      - Display current configuration
```

Each configuration option is briefly described in [Table 116](#), with pointers to detailed menu commands.

**Table 116** Configuration Menu Options (/cfg)

---

**Command Syntax and Usage**

---

**sys**

Displays the System Configuration Menu. To view menu options, see [page 241](#).

---

**port** *<port alias or number>*

Displays the Port Configuration Menu. To view menu options, see [page 282](#).

---

**stack**

Displays the Stacking Configuration Menu. This menu is visible only if stacking is enabled from the `/boot` menu, and the switch is reset. To view menu options, see [page 291](#).

---

**qos**

Displays the Quality of Service Configuration Menu. To view menu options, see [page 293](#).

---

**acl**

Displays the ACL Configuration Menu. To view menu options, see [page 296](#).

---

**pmirr**

Displays the Mirroring Configuration Menu. To view menu options, see [page 309](#).

---

**12**

Displays the Layer 2 Configuration Menu. To view menu options, see [page 311](#).

---

**13**

Displays the Layer 3 Configuration Menu. To view menu options, see [page 360](#).

---

**cee**

Displays the Converged Ethernet Configuration Menu. To view menu options, see [page 445](#).

---

**fcoe**

Displays the Fiber Channel over Ethernet Configuration Menu. To view menu options, see [page 454](#).

---

**rmon**

Displays the Remote Monitoring (RMON) Configuration Menu. To view menu options, see [page 457](#).

---

**Table 116** Configuration Menu Options (/cfg) (continued)

---

**Command Syntax and Usage**

---

**virt**

Displays the Virtualization Configuration Menu. To view menu options, see [page 462](#).

---

**dump**

Dumps current configuration to a script file. For details, see [page 474](#).

---

**ptcfg** *<FTP/TFTP server host name or IP address> <filename on host>*

Backs up current configuration to TFTP server. For details, see [page 474](#).

---

**gtcfg** *<host name or IP address of TFTP server> <filename on host>*

Restores current configuration from TFTP server. For details, see [page 475](#).

---

**cur**

Displays current configuration parameters.

---

## Viewing, Applying, and Saving Changes

---

As you use the configuration menus to set switch parameters, the changes you make do not take effect immediately. All changes are considered “pending” until you explicitly apply them. Also, any changes are lost the next time the switch boots unless the changes are explicitly saved.

---

**Note** – Some operations can override the settings in the Configuration menu. Therefore, settings you view in the Configuration menu (for example, port status) might differ from run-time information that you view in the Information menu or on the management module. The Information menu displays current run-time information of switch parameters.

---

While configuration changes are in the pending state, you can do the following:

- View the pending changes
- Apply the pending changes
- Save the changes to flash memory

## Viewing Pending Changes

You can view all pending configuration changes by entering **diff** at the menu prompt.

---

**Note** – The **diff** command is a global command. Therefore, you can enter **diff** at any prompt in the CLI.

---

## Applying Pending Changes

To make your configuration changes active, you must apply them. To apply configuration changes, enter **apply** at any prompt in the CLI.

```
# apply
```

---

**Note** – The `apply` command is a global command. Therefore, you can enter **apply** at any prompt in the administrative interface.

---

## Saving the Configuration

In addition to applying the configuration changes, you can save them to flash memory on the Virtual Fabric 10Gb Switch Module (VFSM).

---

**Note** – If you do not save the changes, they will be lost the next time the system is rebooted.

---

To save the new configuration, enter the following command at any CLI prompt:

```
# save
```

When you save configuration changes, the changes are saved to the *active* configuration block. The configuration being replaced by the save is first copied to the *backup* configuration block. If you do not want the previous configuration block copied to the backup configuration block, enter the following instead:

```
# save n
```

You can decide which configuration you want to run the next time you reset the switch. Your options include:

- The active configuration block
- The backup configuration block
- Factory default configuration

You can view all pending configuration changes that have been applied but not saved to flash memory using the `diff flash` command. It is a global command that can be executed from any menu.

For instructions on selecting the configuration to run at the next system reset, see [“Selecting a Configuration Block” on page 503](#).

/cfg/sys

# System Configuration Menu

[System Menu]	
errdis	- ErrDisable Menu
syslog	- Syslog Menu
sshd	- SSH Server Menu
radius	- RADIUS Authentication Menu
tacacs+	- TACACS+ Authentication Menu
ldap	- LDAP Authentication Menu
ntp	- NTP Server Menu
ssnmp	- System SNMP Menu
access	- System Access Menu
dst	- Custom DST Menu
sflow	- sFlow Menu
date	- Set system date
time	- Set system time
timezone	- Set system timezone (daylight savings)
dlight	- Set system daylight savings
idle	- Set timeout for idle CLI sessions
linkscan	- Set linkscan mode
notice	- Set login notice
bannr	- Set login banner
hprompt	- Enable/disable display hostname (sysName) in CLI prompt
reminder	- Enable/disable Reminders
rstctrl	- Enable/disable System reset on panic
cur	- Display current system-wide parameters

This menu provides configuration of switch management parameters such as user and administrator privilege mode passwords, Web-based management settings, and management access lists.

**Table 117** System Configuration Menu Options (/cfg/sys)

**Command Syntax and Usage**

**errdis**

Displays the Error Disable Recovery menu. To view menu options, see [page 244](#).

**syslog**

Displays the Syslog Menu. To view menu options, see [page 245](#).

**sshd**

Displays the SSH Server Menu. To view menu options, see [page 246](#).

**radius**

Displays the RADIUS Authentication Menu. To view menu options, see [page 248](#).

**Table 117** System Configuration Menu Options (/cfg/sys) (continued)

---

**Command Syntax and Usage**

---

**tacacs+**

Displays the TACACS+ Authentication Menu. To view menu options, see [page 250](#).

---

**ldap**

Displays the LDAP Authentication Menu. To view menu options, see [page 254](#).

---

**ntp**

Displays the Network Time Protocol (NTP) Server Menu. To view menu options, see [page 256](#).

---

**ssnmp**

Displays the System SNMP Menu. To view menu options, see [page 257](#).

---

**access**

Displays the System Access Menu. To view menu options, see [page 271](#).

---

**dst**

Displays the Custom Daylight Savings Time menu. To view menu options, see [page 279](#).

---

**sflow**

Displays the sFlow menu. To view menu options, see [page 280](#).

---

**date**

Prompts the user for the system date. The date retains its value when the switch is reset.

---

**time**

Configures the system time using a 24-hour clock format. The time retains its value when the switch is reset.

---

**timezone**

Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Savings Time, etc.

---

**dlight enable|disable**

Disables or enables daylight savings time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock.

The default value is **disabled**.

---



**Table 117** System Configuration Menu Options (/cfg/sys) (continued)

---

**Command Syntax and Usage**

---

**idle** *<idle timeout in minutes>*

Sets the idle timeout for CLI sessions, from 1 to 60 minutes. The default is 10 minutes.

---

**linkscan** {**fast**|**normal**|**slow**}

Configures the link scan interval used to poll the status of ports.

---

**notice** *<maximum 1024 character multi-line login notice>* *<'.' to end>*

Displays login notice immediately before the “Enter password:” prompt. This notice can contain up to 1024 characters and new lines.

---

**bannr** *<string, maximum 80 characters>*

Configures a login banner of up to 80 characters. When a user or administrator logs into the switch, the login banner is displayed. It is also displayed as part of the output from the `/info/sys` command.

---

**hprompt** **disable** | **enable**

Enables or disables displaying of the host name (system administrator’s name) in the Command Line Interface (CLI).

---

**reminder** **disable** | **enable**

Enables or disables reminder messages in the CLI. The default value is `enabled`.

---

**rstctrl** **disable** | **enable**

Enables or disables the reset control flag. When enabled, the switch continues to function after a crash of the main processor, using the last known Layer 2/3 information.

The default value is `enabled`.

---

**cur**

Displays the current system parameters.

---

/cfg/sys/errdis  
Error Disable Configuration

[System ErrDisable Menu]	
timeout	- Set ErrDisable timeout (sec)
ena	- Enable ErrDisable recovery
dis	- Disable ErrDisable recovery
cur	- Display current ErrDisable configuration

The Error Disable and Recovery feature allows the switch to automatically disable a port if an error condition is detected on the port. The port remains in the error-disabled state until it is re-enabled manually, or re-enabled automatically by the switch after a timeout period has elapsed. The error-disabled state of a port does not persist across a system reboot.

Table 118 Error Disable Configuration Options

Command Syntax and Usage

**timeout** <30 - 86400>

Configures the error-recovery timeout, in seconds. After the timer expires, the switch attempts to re-enable the port. The default value is 300.

**Note:** When you change the timeout value, all current error-recovery timers are reset.

**ena**

Globally enables automatic error-recovery for error-disabled ports. The default setting is disabled.

**Note:** Each port must have error-recovery enabled to participate in automatic error recovery (/cfg/port x/errdis/ena).

**dis**

Globally disables error-recovery for error-disabled ports.

**cur**

Displays the current system Error Disable and Recovery configuration.

`/cfg/sys/syslog`  
System Host Log Configuration Menu

```
[Syslog Menu]
  host      - Set IP address of first syslog host
  host2     - Set IP address of second syslog host
  sever     - Set the severity of first syslog host
  sever2    - Set the severity of second syslog host
  facil     - Set facility of first syslog host
  facil2    - Set facility of second syslog host
  console   - Enable/disable console output of syslog messages
  log       - Enable/disable syslogging of features
  cur       - Display current syslog settings
```

**Table 119** Host Log Menu Options (`/cfg/sys/syslog`)

**Command Syntax and Usage**

**host** *<new syslog host IP address>*

Sets the IP address of the first syslog host.

**host2** *<new syslog host IP address>*

Sets the IP address of the second syslog host.

**sever** *<syslog host local severity (0-7)>*

This option sets the severity level of the first syslog host displayed. The default is 7, which means log all severity levels.

**sever2** *<syslog host local severity (0-7)>*

This option sets the severity level of the second syslog host displayed. The default is 7, which means, log all severity levels.

**facil** *<syslog host local facility (0-7)>*

This option sets the facility level of the first syslog host displayed. The default is 0.

**facil2** *<syslog host local facility (0-7)>*

This option sets the facility level of the second syslog host displayed. The default is 0.

**console** **disable** | **enable**

Enables or disables delivering syslog messages to the console. When necessary, disabling `console` ensures the switch is not affected by syslog messages. It is enabled by default.

Table 119 Host Log Menu Options (/cfg/sys/syslog) (continued)

Command Syntax and Usage

**log** <feature | **all**> <**enable** | **disable**>

Displays a list of features for which syslog messages can be generated. You can choose to enable or disable specific features (such as `vlangs`, `stg`, or `ssh`), or to enable or disable syslog on all available features.

**cur**

Displays the current syslog settings.

/cfg/sys/sshd  
SSH Server Configuration Menu

```
[SSHD Menu]
  intrval  - Set Interval for generating the RSA server key
  scpadm   - Set SCP-only admin password
  hkeygen  - Generate the RSA host key
  skeygen  - Generate the RSA server key
  sshport  - Set SSH server port number
  ena      - Enable the SCP apply and save
  dis      - Disable the SCP apply and save
  on       - Turn SSH server ON
  off      - Turn SSH server OFF
  cur      - Display current SSH server configuration
```

For the VFSM, this menu enables Secure Shell access from any SSH client. SSH scripts can be viewed by using the `/cfg/dump` command (see [page 474](#)).

Table 120 SSH Configuration Menu Options (/cfg/sys/sshd)

Command Syntax and Usage

**intrval** <0 - 24>

Set the interval, in hours, for auto-generation of the RSA server key.

**scpadm**

Set the administration password for SCP access.

**hkeygen**

Generate the RSA host key.

**skeygen**

Generate the RSA server key.

**Table 120** SSH Configuration Menu Options (/cfg/sys/sshd) (continued)

Command Syntax and Usage	
<b>sshport</b> <TCP port number>	Sets the SSH server port number.
<b>ena</b>	Enables the SCP apply and save.
<b>dis</b>	Disables the SCP apply and save.
<b>on</b>	Enables the SSH server.
<b>off</b>	Disables the SSH server.
<b>cur</b>	Displays the current SSH server configuration.

/cfg/sys/radius  
RADIUS Server Configuration Menu

```
[RADIUS Server Menu]
  prisrv - Set primary RADIUS server address
  secsrv - Set secondary RADIUS server address
  secret - Set RADIUS secret
  secret2 - Set secondary RADIUS server secret
  port    - Set RADIUS port
  retries - Set RADIUS server retries
  timeout - Set RADIUS server timeout
  bckdoor - Enable/disable RADIUS backdoor for telnet/ssh/http/https
  secbd   - Enable/disable RADIUS secure backdoor for
            telnet/ssh/http/https
  on      - Turn RADIUS authentication ON
  off     - Turn RADIUS authentication OFF
  cur     - Display current RADIUS configuration
```

Table 121 System Configuration Menu Options (/cfg/sys/radius)

Command Syntax and Usage

**prisrv** <IP address>

Sets the primary RADIUS server address.

**secsrv** <IP address>

Sets the secondary RADIUS server address.

**secret** <1-32 character secret>

This is the shared secret between the switch and the RADIUS server(s).

**secret2** <1-32 character secret>

This is the secondary shared secret between the switch and the RADIUS server(s).

**port** <RADIUS port>

Enter the number of the UDP port to be configured, between 1500 - 3000. The default is 1645.

**retries** <RADIUS server retries (1-3)>

Sets the number of failed authentication requests before switching to a different RADIUS server. The default is 3 requests.

**timeout** <RADIUS server timeout seconds (1-10)>

Sets the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed. The default is 3 seconds.

**Table 121** System Configuration Menu Options (/cfg/sys/radius) (continued)

---

**Command Syntax and Usage**

---

**bckdoor disable | enable**

Enables or disables the RADIUS backdoor for Telnet/SSH/HTTP/HTTPS. The default value is disabled.

To obtain the RADIUS backdoor password for your GbESM, contact your Service and Support line.

---

**secbd enable | disable**

Enables or disables the RADIUS back door using secure password for telnet/SSH/HTTP/HTTPS. This command does not apply when backdoor (telnet) is enabled.

---

**on**

Enables the RADIUS server.

---

**off**

Disables the RADIUS server.

---

**cur**

Displays the current RADIUS server parameters.

---

## `/cfg/sys/tacacs+` TACACS+ Server Configuration Menu

TACACS (Terminal Access Controller Access Control system) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. TACACS is not an encryption protocol, and therefore less secure than TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols. (TACACS is described in RFC 1492.)

TACACS+ protocol is more reliable than RADIUS, as TACACS+ uses the Transmission Control Protocol (TCP) whereas RADIUS uses the User Datagram Protocol (UDP). Also, RADIUS combines authentication and authorization in a user profile, whereas TACACS+ separates the two operations.

TACACS+ offers the following advantages over RADIUS as the authentication device:

- TACACS+ is TCP-based, so it facilitates connection-oriented traffic.
- It supports full-packet encryption, as opposed to password-only in authentication requests.
- It supports de-coupled authentication, authorization, and accounting.

```
[TACACS+ Server Menu]
  prisrv   - Set IP address of primary TACACS+ server
  secsrv   - Set IP address of secondary TACACS+ server
  chpass_p - Set new password for primary server
  chpass_s - Set new password for secondary server
  secret   - Set secret for primary TACACS+ server
  secret2  - Set secret for secondary TACACS+ server
  port     - Set TACACS+ port number
  retries  - Set number of TACACS+ server retries
  attempts - Set number of TACACS+ login attempts
  timeout  - Set timeout value of TACACS+ server retries
  usermap  - Set user privilege mappings
  bckdoor  - Enable/disable TACACS+ backdoor for telnet/ssh/http/https
  secbd    - Enable/disable TACACS+ secure backdoor
  cmap     - Enable/disable TACACS+ new privilege level mapping
  passsch  - Enable/disable TACACS+ password change
  cauth    - Enable/disable TACACS+ command authorization
  clog     - Enable/disable TACACS+ command logging
  dreq     - Enable/disable TACACS+ directed request
  on       - Enable TACACS+ authentication
  off      - Disable TACACS+ authentication
  cur      - Display current TACACS+ settings
```



**Table 122** TACACS+ Server Menu Options (/cfg/sys/tacacs)

---

**Command Syntax and Usage**

---

**prisrv** *<IP address>*

Defines the primary TACACS+ server address.

---

**secsrv** *<IP address>*

Defines the secondary TACACS+ server address.

---

**chpass\_p**

Configures the password for the primary TACACS+ server. The CLI will prompt you for input.

---

**chpass\_s**

Configures the password for the secondary TACACS+ server. The CLI will prompt you for input.

---

**secret** *<1-32 character secret>*

This is the shared secret between the switch and the TACACS+ server(s).

---

**secret2** *<1-32 character secret>*

This is the secondary shared secret between the switch and the TACACS+ server(s).

---

**port** *<TACACS port>*

Enter the number of the TCP port to be configured, between 1 - 65000. The default is 49.

---

**retries** *<TACACS server retries, 1-3>*

Sets the number of failed authentication requests before switching to a different TACACS+ server. The default is 3 requests.

---

**attempts** *<1-10>*

Sets the number of failed login attempts before disconnecting the user. The default is 2 attempts.

---

**timeout** *<TACACS server timeout seconds, 4-15>*

Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The default is 5 seconds.

---

**usermap** *<0-15>* **user|oper|admin|none**

Maps a TACACS+ authorization level to a switch user level. Enter a TACACS+ authorization level (0-15), followed by the corresponding switch user level.

---

**Table 122** TACACS+ Server Menu Options (/cfg/sys/tacacs) (continued)

---

**Command Syntax and Usage**

---

**bckdoor disable | enable**

Enables or disables the TACACS+ back door for Telnet, SSH/SCP, or HTTP/HTTPS.

Enabling this feature allows you to bypass the TACACS+ servers. It is recommended that you use Secure Backdoor to ensure the switch is secured, because Secure Backdoor disallows access through the back door when the TACACS+ servers are responding.

The default setting is `disabled`.

To obtain the TACACS+ backdoor password for your GbESM, contact your IBM Service and Support line.

---

**secbd enable | disable**

Enables or disables TACACS+ secure back door access through Telnet, SSH/SCP, or HTTP/HTTPS only when the TACACS+ servers are not responding.

This feature is recommended to permit access to the switch when the TACACS+ servers become unresponsive. If no back door is enabled, the only way to gain access when TACACS+ servers are unresponsive is to use the back door via the console port.

The default setting is `disabled`.

---

**cmmap enable | disable**

Enables or disables TACACS+ privilege-level mapping.

The default value is `disabled`.

---

**passch enable | disable**

Enables or disables TACACS+ password change.

The default setting is `disabled`.

---

**cauth disable | enable**

Enables or disables TACACS+ command authorization.

---

**clog disable | enable**

Enables or disables TACACS+ command logging.

---

**Table 122** TACACS+ Server Menu Options (/cfg/sys/tacacs) (continued)

---

**Command Syntax and Usage**

---

**dreq disable | enable**

Enables or disables TACACS+ directed request, which uses a specified TACACS+ server for authentication, authorization, accounting. When enabled, When directed-request is enabled, each user must add a configured TACACS+ server hostname to the username (for example, username@hostname) during login.

This command allows the following options:

- ☐ **Restricted:** Only the username is sent to the specified TACACS+ server.
- ☐ **No-truncate:** The entire login string is sent to the TACACS+ server.

---

**on**

Enables the TACACS+ server. This is the default setting.

---

**off**

Disables the TACACS+ server.

---

**cur**

Displays current TACACS+ configuration parameters.

---

/cfg/sys/ldap

## LDAP Server Configuration Menu

LDAP (Lightweight Directory Access Protocol) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system.

[LDAP Server Menu]	
prisrv	- Set IP address of primary LDAP server
secsrv	- Set IP address of secondary LDAP server
port	- Set LDAP port number
retries	- Set number of LDAP server retries
timeout	- Set timeout value of LDAP server retries
domain	- Set domain name
bckdoor	- Enable/disable LDAP backdoor for telnet/ssh/http/https
on	- Enable LDAP authentication
off	- Disable LDAP authentication
cur	- Display current LDAP settings

Table 123 LDAP Server Menu Options (/cfg/sys/ldap)

Command Syntax and Usage	
<b>prisrv</b> <IP address>	Defines the primary LDAP server address.
<b>secsrv</b> <IP address>	Defines the secondary LDAP server address.
<b>port</b> <LDAP port>	Enter the number of the TCP port to be configured, between 1 - 65000. The default is 389.
<b>retries</b> <LDAP server retries, 1-3>	Sets the number of failed authentication requests before switching to a different LDAP server. The default is 3 requests.
<b>timeout</b> <LDAP server timeout seconds, 4-15>	Sets the amount of time, in seconds, before a LDAP server authentication attempt is considered to have failed. The default is 5 seconds.
<b>domain</b> <domain name (1-128 characters)>   none	Sets the domain name for the LDAP server. Enter the full path for your organization. For example:  ou=people,dc=mydomain,dc=com

**Table 123** LDAP Server Menu Options (/cfg/sys/ldap) (continued)

Command Syntax and Usage	
<b>bckdoor</b>	<b>disable</b>   <b>enable</b>
Enables or disables the LDAP back door for Telnet, SSH/SCP, or HTTP/HTTPS. The default setting is disabled.	
To obtain the LDAP back door password for your GbESM, contact your Service and Support line.	
<b>on</b>	
Enables the LDAP server.	
<b>off</b>	
Disables the LDAP server. This is the default setting.	
<b>cur</b>	
Displays current LDAP configuration parameters.	

**/cfg/sys/ntp**  
**NTP Server Configuration Menu**

[NTP Server Menu]

prisrv

- Set primary NTP server address

secsrv

- Set secondary NTP server address

intrval

- Set NTP server resync interval

on

- Turn NTP service ON

off

- Turn NTP service OFF

cur

- Display current NTP configuration

This menu enables you to synchronize the switch clock to a Network Time Protocol (NTP) server. By default, this option is disabled.

**Table 124** NTP Configuration Menu Options (/cfg/sys/ntp)

**Command Syntax and Usage**

**prisrv** <IP address>

Prompts for the IP addresses of the primary NTP server to which you want to synchronize the switch clock.

**secsrv** <IP address>

Prompts for the IP addresses of the secondary NTP server to which you want to synchronize the switch clock.

**intrval** <5-44640>

Specifies the time interval, in minutes, to re-synchronize the switch clock with the NTP server.

**on**

Enables the NTP synchronization service.

**off**

Disables the NTP synchronization service.

**cur**

Displays the current NTP service settings.

## /cfg/sys/ssnmp

# System SNMP Configuration Menu

```
[System SNMP Menu]
snmpv3    - SNMPv3 Menu
name      - Set SNMP "sysName"
locn      - Set SNMP "sysLocation"
cont      - Set SNMP "sysContact"
rcomm     - Set SNMP read community string
wcomm     - Set SNMP write community string
trsrc     - Set SNMP trap source interface for SNMPv1
timeout   - Set timeout for the SNMP state machine
auth      - Enable/disable SNMP "sysAuthenTrap"
linkt     - Enable/disable SNMP link up/down trap
cur       - Display current SNMP configuration
```

BLADEOS supports SNMP-based network management. In SNMP model of network management, a management station (client/manager) accesses a set of variables known as MIBs (Management Information Base) provided by the managed device (agent). If you are running an SNMP network management station on your network, you can manage the switch using the following standard SNMP MIBs:

- MIB II (RFC 1213)
- Ethernet MIB (RFC 1643)
- Bridge MIB (RFC 1493)

An SNMP agent is a software process on the managed device that listens on UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to retrieve or to modify.

SNMP parameters that can be modified include:

- System name
- System location
- System contact
- Use of the SNMP system authentication trap function
- Read community string
- Write community string
- Trap community strings

**Table 125** System SNMP Menu Options (/cfg/sys/ssnmp)**Command Syntax and Usage****snmpv3**

Displays SNMPv3 menu. To view menu options, see [page 259](#).

**name** <1-64 characters>

Configures the name for the system.

**locn** <1-64 characters>

Configures the name of the system location.

**cont** <1-64 characters>

Configures the name of the system contact.

**rcomm** <1-32 characters>

Configures the SNMP read community string. The read community string controls SNMP “get” access to the switch. The default read community string is *public*.

**wcomm** <1-32 characters>

Configures the SNMP write community string. The write community string controls SNMP “set” and “get” access to the switch. The default write community string is *private*.

**trsrc** <interface number>

Configures the source interface for SNMP traps. The default value is interface 1.

To send traps through the management ports, specify interface 128.

**timeout** <1-30>

Set the timeout value for the SNMP state machine, in minutes.

**auth** **disable** | **enable**

Enables or disables the use of the system authentication trap facility. The default setting is disabled.

**linkt** <port> {**disable** | **enable**}

Enables or disables the sending of SNMP link up and link down traps. The default setting is enabled.

**cur**

Displays the current SNMP configuration.



**/cfg/sys/ssnmp/snmpv3**  
**SNMPv3 Configuration Menu**

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please refer to RFC3411 to RFC3418.

[SNMPv3 Menu]	
usm	- usmUser Table menu
view	- vacmViewTreeFamily Table menu
access	- vacmAccess Table menu
group	- vacmSecurityToGroup Table menu
comm	- community Table menu
taddr	- targetAddr Table menu
tparam	- targetParams Table menu
notify	- notify Table menu
v1v2	- Enable/disable V1/V2 access
cur	- Display current SNMPv3 configuration

**Table 126** SNMPv3 Configuration Menu Options (/cfg/sys/ssnmp/snmpv3)

**Command Syntax and Usage**

**usm** <usmUser number (1-16)>

Defines a user security model (USM) entry for an authorized user.  
You can also configure this entry through SNMP. To view menu options, see [page 261](#).

**view** <vacmViewTreeFamily number (1-128)>

Allows you to create different MIB views. To view menu options, see [page 262](#).

**access** <vacmAccess number (1-32)>

Configures the access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity. To view menu options, see [page 263](#).

**Table 126** SNMPv3 Configuration Menu Options (/cfg/sys/ssnmp/snmpv3)

---

**group** <*vacmSecurityToGroup number (1-16)*>

Maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group. To view menu options, see [page 265](#).

---

**comm** <*snmpCommunity number (1-16)*>

The community table contains objects for mapping community strings and version-independent SNMP message parameters. To view menu options, see [page 266](#).

---

**taddr** <*snmpTargetAddr number (1-16)*>

Allows you to configure destination information, consisting of a transport domain and a transport address. This is also termed as transport endpoint. The SNMP MIB provides a mechanism for performing source address validation on incoming requests, and for selecting community strings based on target addresses for outgoing notifications. To view menu options, see [page 267](#).

---

**tparam** <*target params index (1-16)*>

Allows you to configure SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters. To view menu options, see [page 268](#).

---

**notify** <*notify index (1-16)*>

A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions. To view menu options, see [page 269](#).

---

**v1v2** **disable** | **enable**

Allows you to enable or disable the access to SNMP version 1 and version 2. The default setting is enabled.

---

**cur**

Displays the current SNMPv3 configuration.

---

*/cfg/sys/ssnmp/snmpv3/usm*  
*User Security Model Configuration Menu*

You can make use of a defined set of user identities using this Security Model. An SNMP engine must have the knowledge of applicable attributes of a user.

This menu helps you create a user security model entry for an authorized user. You need to provide a security name to create the USM entry.

```
[SNMPv3 usmUser 1 Menu]
name      - Set USM user name
auth      - Set authentication protocol
authpw    - Set authentication password
priv      - Set privacy protocol
privpw    - Set privacy password
del        - Delete usmUser entry
cur        - Display current usmUser configuration
```

**Table 127** User Security Model Configuration Menu Options  
(/cfg/sys/ssnmp/snmpv3/usm)

**Command Syntax and Usage**

**name** <1-32 characters>

Defines a string that represents the name of the user. This is the login name that you need in order to access the switch.

**auth** {md5 | sha | none}

Configures the authentication protocol between HMAC-MD5-96 or HMAC-SHA-96. The default algorithm is none.

**authpw**

Allows you to create or change your password for authentication. If you selected an authentication algorithm using the above command, you need to provide a password, otherwise you will get an error message during validation.

**priv** des | none

Configures the type of privacy protocol on your switch. The privacy protocol protects messages from disclosure. The options are des (CBC-DES Symmetric Encryption Protocol) or none. If you specify des as the privacy protocol, then make sure that you have selected one of the authentication protocols (MD5 or HMAC-SHA-96). If you select none as the authentication protocol, you will get an error message.

**privpw**

Defines the privacy password.

**Table 127** User Security Model Configuration Menu Options  
(/cfg/sys/ssnmp/snmpv3/usm) (continued)

**Command Syntax and Usage**

**del**

Deletes the selected USM user entries.

**cur**

Displays the selected USM user entries.

**/cfg/sys/ssnmp/snmpv3/view**  
*SNMPv3 View Configuration Menu*

```
[SNMPv3 vacmViewTreeFamily 1 Menu]
name      - Set view name
tree      - Set MIB subtree(OID) which defines a family of view subtrees
mask      - Set view mask
type      - Set view type
del       - Delete vacmViewTreeFamily entry
cur       - Display current vacmViewTreeFamily configuration
```

Note that the first five default `vacmViewTreeFamily` entries cannot be removed, and their names cannot be changed.

**Table 128** SNMPv3 View Menu Options (/cfg/sys/ssnmp/snmpv3/view)

**Command Syntax and Usage**

**name** <1-32 characters>

Defines the name for a family of view subtrees.

**tree** <object identifier, such as 1.3.6.1.2.1.1.1.0 (1-32 characters)>

Defines the MIB tree which, when combined with the corresponding mask, defines a family of view subtrees.

**mask** <bitmask, 1-32 characters>

Configures the bit mask, which in combination with the corresponding tree, defines a family of view subtrees.

**type** **included**|**excluded**

This command indicates whether the corresponding instances of `vacmViewTreeFamilySubtree` and `vacmViewTreeFamilyMask` define a family of view subtrees, which is included in or excluded from the MIB view.

**Table 128** SNMPv3 View Menu Options (/cfg/sys/ssnmp/snmpv3/view)

**Command Syntax and Usage**

**del**

Deletes the vacmViewTreeFamily group entry.

**cur**

Displays the current vacmViewTreeFamily configuration.

**/cfg/sys/ssnmp/snmpv3/access**  
*View-Based Access Control Model Configuration Menu*

The view-based Access Control Model defines a set of services that an application can use for checking access rights of the user. Access control is needed when the user has to process SNMP retrieval or modification request from an SNMP entity.

```
[SNMPv3 vacmAccess 1 Menu]
name      - Set group name
prefix    - Set content prefix
model     - Set security model
level     - Set minimum level of security
match     - Set prefix only or exact match
rview     - Set read view index
wview     - Set write view index
nview     - Set notify view index
del       - Delete vacmAccess entry
cur       - Display current vacmAccess configuration
```

**Table 129** View-based Access Control Model Menu Options  
(/cfg/sys/ssnmp/snmpv3/access)

**Command Syntax and Usage**

**name** <1-32 characters>

Defines the name of the group.

**prefix** <1-32 characters>

Defines the name of the context. An SNMP context is a collection of management information that an SNMP entity can access. An SNMP entity has access to many contexts. For more information on naming the management information, see RFC2571, the SNMP Architecture document.

The view-based Access Control Model defines a table that lists the locally available contexts by contextName.

**Table 129** View-based Access Control Model Menu Options  
(/cfg/sys/ssnmp/snmpv3/access) (continued)

---

**Command Syntax and Usage**

---

**model** *usm* | *snmpv1* | *snmpv2*

Allows you to select the security model to be used.

---

**level** *noAuthNoPriv* | *authNoPriv* | *authPriv*

Defines the minimum level of security required to gain access rights. The level *noAuthNoPriv* means that the SNMP message will be sent without authentication and without using a privacy protocol. The level *authNoPriv* means that the SNMP message will be sent with authentication but without using a privacy protocol. The *authPriv* means that the SNMP message will be sent both with authentication and using a privacy protocol.

---

**match** *exact* | *prefix*

If the value is set to *exact*, then all the rows whose *contextName* exactly matches the prefix are selected. If the value is set to *prefix* then the all the rows where the starting octets of the *contextName* exactly match the prefix are selected.

---

**rview** *<1-32 characters>*

Defines a read view name that allows you read access to a particular MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.

---

**wview** *<1-32 characters>*

Defines a write view name that allows you write access to the MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.

---

**nview** *<1-32 characters>*

Defines a long notify view name that allows you notify access to the MIB view.

---

**del**

Deletes the View-based Access Control entry.

---

**cur**

Displays the View-based Access Control configuration.

---

*/cfg/sys/ssnmp/snmpv3/group*  
*SNMPv3 Group Configuration Menu*

[SNMPv3 vacmSecurityToGroup 1 Menu]	
model	- Set security model
uname	- Set USM user name
gname	- Set group gname
del	- Delete vacmSecurityToGroup entry
cur	- Display current vacmSecurityToGroup configuration

**Table 130** SNMPv3 Group Menu Options (/cfg/sys/ssnmp/snmpv3/group)

**Command Syntax and Usage**

**model usm | snmpv1 | snmpv2**

Defines the security model.

**uname** *<1-32 characters>*

Sets the user name as defined in /cfg/sys/ssnmp/snmpv3/usm/name on [page 261](#).

**gname** *<1-32 characters>*

The name for the access group as defined in  
/cfg/sys/ssnmp/snmpv3/access/name on [page 263](#).

**del**

Deletes the vacmSecurityToGroup entry.

**cur**

Displays the current vacmSecurityToGroup configuration.

*/cfg/sys/ssnmp/snmpv3/comm*  
*SNMPv3 Community Table Configuration Menu*

This command is used for configuring the community table entry. The configured entry is stored in the community table list in the SNMP engine. This table is used to configure community strings in the Local Configuration Datastore (LCD) of SNMP engine.

```
[SNMPv3 snmpCommunityTable 1 Menu]
  index      - Set community index
  name       - Set community string
  uname      - Set USM user name
  tag        - Set community tag
  del        - Delete communityTable entry
  cur        - Display current communityTable configuration
```

**Table 131** SNMPv3 Community Table Configuration Menu Options  
(/cfg/sys/ssnmp/snmpv3/comm)

**Command Syntax and Usage**

<b>index</b> <1-32 characters>	Configures the unique index value of a row in this table.
<b>name</b> <1-32 characters>	Defines the user name as defined in the /cfg/sys/ssnmp/snmpv3/usm/name command.
<b>uname</b> <1-32 characters>	Defines a readable text string that represents the corresponding value of an SNMP community name in a security model.
<b>tag</b> <1-255 characters>	Configures a tag that specifies a set of transport endpoints to which a command responder application sends an SNMP trap.
<b>del</b>	Deletes the community table entry.
<b>cur</b>	Displays the community table configuration.



*/cfg/sys/ssnmp/snmpv3/taddr*  
*SNMPv3 Target Address Table Configuration Menu*

This command is used to configure the target transport entry. The configured entry is stored in the target address table list in the SNMP engine. This table of transport addresses is used in the generation of SNMP messages.

```
[SNMPv3 snmpTargetAddrTable 1 Menu]
  name      - Set target address name
  addr      - Set target transport address IP
  port      - Set target transport address port
  taglist   - Set tag list
  pname     - Set targetParams name
  del       - Delete targetAddrTable entry
  cur       - Display current targetAddrTable configuration
```

**Table 132** Target Address Table Menu Options (/cfg/sys/ssnmp/snmpv3/taddr)

**Command Syntax and Usage**

**name** <1-32 characters>

Defines the locally arbitrary, but unique identifier, target address name associated with this entry.

**addr** <transport IP address>

Configures a transport IPv4/IPv6 address that can be used in the generation of SNMP traps.  
IPv6 addresses are not displayed in the configuration, but they do receive traps.

**port** <transport address port>

Configures a transport address port that can be used in the generation of SNMP traps.

**taglist** <1-255 characters>

Allows you to configure a list of tags that are used to select target addresses for a particular operation.

**pname** <1-32 characters>

Defines the name as defined in the /cfg/sys/ssnmp/snmpv3/tparam/name command on [page 268](#).

**del**

Deletes the Target Address Table entry.

**cur**

Displays the current Target Address Table configuration.

*/cfg/sys/ssnmp/snmpv3/tparam*  
*SNMPv3 Target Parameters Table Configuration Menu*

You can configure the target parameters entry and store it in the target parameters table in the SNMP engine. This table contains parameters that are used to generate a message. The parameters include the message processing model (for example: SNMPv3, SNMPv2c, SNMPv1), the security model (for example: USM), the security name, and the security level (noAuthnoPriv, authNoPriv, or authPriv).

[SNMPv3 snmpTargetParamsTable 1 Menu]	
name	- Set target params name
mpmodel	- Set message processing model
model	- Set security model
uname	- Set USM user name
level	- Set minimum level of security
del	- Delete targetParamsTable entry
cur	- Display current targetParamsTable configuration

**Table 133** Target Parameters Table Configuration Menu Options  
(/cfg/sys/ssnmp/snmpv3/tparam)

<b>Command Syntax and Usage</b>	
<b>name</b> <1-32 characters>	Defines the locally arbitrary, but unique identifier that is associated with this entry.
<b>mpmodel</b> snmpv1   snmpv2c   snmpv3	Configures the message processing model that is used to generate SNMP messages.
<b>model</b> usm   snmpv1   snmpv2	Allows you to select the security model to be used when generating the SNMP messages.
<b>uname</b> <1-32 characters>	Defines the name that identifies the user in the USM table (page 261) on whose behalf the SNMP messages are generated using this entry.
<b>level</b> noAuthNoPriv   authNoPriv   authPriv	Allows you to select the level of security to be used when generating the SNMP messages using this entry. The level noAuthNoPriv means that the SNMP message will be sent without authentication and without using a privacy protocol. The level authNoPriv means that the SNMP message will be sent with authentication but without using a privacy protocol. The authPriv means that the SNMP message will be sent both with authentication and using a privacy protocol.

**Table 133** Target Parameters Table Configuration Menu Options  
(/cfg/sys/ssnmp/snmpv3/tparam) (continued)

<b>Command Syntax and Usage</b>	
<b>del</b>	Deletes the targetParamsTable entry.
<b>cur</b>	Displays the current targetParamsTable configuration.

**/cfg/sys/ssnmp/snmpv3/notify**  
*SNMPv3 Notify Table Configuration Menu*

SNMPv3 uses Notification Originator to send out traps. A notification typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.

[SNMPv3 snmpNotifyTable 1 Menu]	
name	- Set notify name
tag	- Set notify tag
del	- Delete notifyTable entry
cur	- Display current notifyTable configuration

**Table 134** Notify Table Menu Options (/cfg/sys/ssnmp/snmpv3/notify)

<b>Command Syntax and Usage</b>	
<b>name</b> <1-32 characters>	Defines a locally arbitrary but unique identifier associated with this SNMP notify entry.
<b>tag</b> <1-255 characters>	Allows you to configure a tag that contains a tag value which is used to select entries in the Target Address Table. Any entry in the snmpTargetAddrTable, that matches the value of this tag is selected.
<b>del</b>	Deletes the notify table entry.
<b>cur</b>	Displays the current notify table configuration.

/cfg/sys/access

## System Access Configuration Menu

[System Access Menu]	
mgmt	- Management Network Definition Menu
user	- User Access Control Menu (passwords)
https	- HTTPS Web Access Menu
snmp	- Set SNMP access control
tnport	- Set Telnet server port number
tport	- Set the TFTP Port for the system
wport	- Set HTTP (Web) server port number
http	- Enable/disable HTTP (Web) access
tnet	- Enable/disable Telnet access
tsbbi	- Enable/disable Telnet/SSH configuration from BBI
userbbi	- Enable/disable user configuration from BBI
cur	- Display current system access configuration

**Table 135** System Access Menu Options (/cfg/sys/access)

**Command Syntax and Usage**

**mgmt**

Displays the Management Configuration Menu. To view menu options, see [page 273](#).

**user**

Displays the User Access Control Menu. To view menu options, see [page 274](#).

**https**

Displays the HTTPS Menu. To view menu options, see [page 277](#).

**snmp {disable | read-only | read-write}**

Disables or provides read-only/write-read SNMP access.

**tnport** <TCP port number>

Sets an optional telnet server port number for cases where the server listens for telnet sessions on a non-standard port.

**tport** <TFTP port number (1-65535)>

Sets the TFTP port for the switch. The default is port 69.

**wport** <TCP port number (1-65535)>

Sets the switch port used for serving switch Web content. The default is HTTP port 80. If Global Server Load Balancing is to be used, set this to a different port (such as 8080).

**Table 135** System Access Menu Options (/cfg/sys/access) (continued)

Command Syntax and Usage	
<b>http</b> <b>disable</b>   <b>enable</b>	Enables or disables HTTP (Web) access to the Browser-Based Interface. It is enabled by default.
<b>tnet</b> <b>enable</b>   <b>disable</b>	Enables or disables Telnet access. This command is enabled by default.
<b>tsbbi</b> <b>enable</b>   <b>disable</b>	Enables or disables Telnet/SSH configuration access through the Browser-Based Interface (BBI).
<b>userbbi</b> <b>enable</b>   <b>disable</b>	Enables or disables user configuration access through the Browser-Based Interface (BBI).
<b>cur</b>	Displays the current system access parameters.

## /cfg/sys/access/mgmt

### Management Networks Configuration Menu

```
[Management Networks Menu]
  add      - Add mgmt network definition
  rem      - Remove mgmt network definition
  cur      - Display current mgmt network definitions
  clear    - Clear current mgmt network definitions
```

This menu is used to define IP address ranges which are allowed to access the switch for management purposes.

**Table 136** Management Network Menu Options (/cfg/sys/access/mgmt)

---

#### Command Syntax and Usage

---

**add** *<mgmt network address> <mgmt network mask>*

Adds a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the Browser-Based Interface. A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation.

**Note:** If you configure the management network without including the switch interfaces, the configuration causes the Firewall Load Balancing health checks to fail and creates a “Network Down” state on the network.

---

**rem** *<mgmt network address> <mgmt network mask>*

Removes a defined network, which consists of a management network address and a management network mask address.

---

**cur**

Displays the current configuration.

---

**clear**

Removes all defined management networks.

---

**/cfg/sys/access/user**  
User Access Control Configuration Menu

[User Access Control Menu]

uid

- User ID Menu

eject

- Eject user

usrpw

- Set user password (user)

opw

- Set operator password (oper)

admpw

- Set administrator password (admin)

strongpw

- Strong password menu

cur

- Display current user status

**Note** – Passwords can be a maximum of 128 characters.

**Table 137** User Access Control Menu Options (/cfg/sys/access/user)

**Command Syntax and Usage**

**uid** <User ID (1-10)>

Displays the User ID Menu. To view menu options, see [page 275](#).

**eject user** | **oper** | **admin** | <user name>

Ejects the specified user from the VFSM.

**usrpw** <1-128 characters>

Sets the user (user) password. The user has no direct responsibility for switch management. He or she can view switch status information and statistics, but cannot make any configuration changes.

**opw** <1-128 characters>

Sets the operator (oper) password. The operator manages all functions of the switch. He or she can view all switch information and statistics and can reset ports or the entire switch.

**admpw** <1-128 characters>

Sets the administrator (admin) password. The super user administrator has complete access to all menus, information, and configuration commands on the VFSM, including the ability to change both the user and administrator passwords.

Access includes “oper” functions.

**Table 137** User Access Control Menu Options (/cfg/sys/access/user)

**Command Syntax and Usage**

**strongpw**

Displays the Strong User Password Menu. To view menu options, see [page 276](#).

**cur**

Displays the current user status.

**/cfg/sys/access/user/uid <1-10>**  
*System User ID Configuration Menu*

```
[User ID 1 Menu]
cos      - Set class of service
name     - Set user name
pswd     - Set user password
ena      - Enable user ID
dis      - Disable user ID
del      - Delete user ID
cur      - Display current user configuration
```

**Table 138** User ID Configuration Menu Options (/cfg/sys/access/user/uid)

**Command Syntax and Usage**

**cos** <user | oper | admin>

Sets the Class-of-Service to define the user’s authority level. BLADEOS defines these levels as: User, Operator, and Administrator, with User being the most restricted level.

**name** <1-8 characters>

Sets the user name (maximum of eight characters).

**pswd** <1-128 characters>

Sets the user password.

**ena**

Enables the user ID.

**dis**

Disables the user ID.



**Table 138** User ID Configuration Menu Options (/cfg/sys/access/user/uid)

**Command Syntax and Usage**

**del**

Deletes the user ID.

**cur**

Displays the current user ID configuration.

**/cfg/sys/access/user/strongpw**  
*Strong Password Configuration Menu*

```
[Strong Pwd Menu]
  ena      - Enable usage of strong passwords
  dis      - Disable usage of strong passwords
  expiry   - Set password validity
  warning  - Set warning days before pswd expiry
  faillog  - Set number of failed logins for security notification
  cur      - Display current strong password configuration
```

**Table 139** Strong Password Menu Options (/cfg/sys/access/user/strongpw)

**Command Syntax and Usage**

**ena**

Enables Strong Password requirement.

**dis**

Disables Strong Password requirement.

**expiry** <1-365>

Configures the number of days allowed before the password must be changed. The default value is 60 days.

**warning** <1-365>

Configures the number of days before password expiration, that a warning is issued to users. The default value is 15 days.

**Table 139** Strong Password Menu Options (/cfg/sys/access/user/strongpw)

**Command Syntax and Usage**

**faillog** <1-255>

Configures the number of failed login attempts allowed before a security notification is logged. The default value is 3 login attempts.

**cur**

Displays the current Strong Password configuration.

**/cfg/sys/access/https**  
**HTTPS Access Configuration**

```
[https Menu]
  access    - Enable/Disable HTTPS Web access
  port      - HTTPS WebServer port number
  generate  - Generate self-signed HTTPS server certificate
  certSave  - save HTTPS certificate
  cur       - Display current SSL Web Access configuration
```

**Table 140** HTTPS Access Configuration Menu Options (/cfg/sys/access/https)

**Command Syntax and Usage**

**access** **ena** | **dis**

Enables or disables BBI access (Web access) using HTTPS.

**port** <TCP port number>

Defines the HTTPS Web server port number. The default port is 443.

**Table 140** HTTPS Access Configuration Menu Options (/cfg/sys/access/https)

---

**Command Syntax and Usage**

---

**generate**

Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example:

- ☐ Country Name (2 letter code) []: CA
- ☐ State or Province Name (full name) []: Ontario
- ☐ Locality Name (for example, city) []: Ottawa
- ☐ Organization Name (for example, company) []: Blade
- ☐ Organizational Unit Name (for example, section) []: Datacenter
- ☐ Common Name (for example, user's name) []: Mr Smith
- ☐ Email (for example, email address) []: info@bladenetwork.net

You will be asked to confirm if you want to generate the certificate. It will take approximately 30 seconds to generate the certificate. Then the switch will restart SSL agent.

---

**certSave**

Allows the client, or the Web browser, to accept the certificate and save the certificate to Flash to be used when the switch is rebooted.

---

**cur**

Displays the current SSL Web Access configuration.

---

/cfg/sys/dst  
Custom Daylight Savings Time Configuration Menu

[Custom DST Menu]

dststart

- Set the DST start day

dstend

- Set the DST stop day

ena

- Enable custom DST

dis

- Disable custom DST

cur

- Display custom DST configuration

Use this menu to configure custom Daylight Savings Time. The DST will be defined by two rules, the start rule and end rule. The rules specify the date and time when the DST starts and finishes. These dates are represented as specific calendar dates or as relative offsets in a month (for example, 'the second Sunday of September').

Relative offset example:  
2070901 = Second Sunday of September, at 1:00 a.m.

Calendar date example:  
0070901 = September 7, at 1:00 a.m.

Table 141 Custom DST Configuration Menu Options (/cfg/sys/dst)

Command Syntax and Usage

**dststart** {<WDDMMhh>}

Configures the start date for custom DST, as follows:

WDDMMhh

W = week (0-5, where 0 means use the calendar date)  
D = day of the week (01-07, where 01 is Monday)  
MM = month (1-12)  
hh = hour (0-23)

**Note:** Week 5 is always considered to be the last week of the month.

**dstend** {<WDDMMhh>}

Configures the end date for custom DST, as follows:

WDDMMhh

W = week (0-5, where 0 means use the calendar date)  
D = day of the week (01-07, where 01 is Monday)  
MM = month (1-12)  
hh = hour (0-23)

**Note:** Week 5 is always considered to be the last week of the month.

**Table 141** Custom DST Configuration Menu Options (/cfg/sys/dst) (continued)

**Command Syntax and Usage**

**ena**

Enables the Custom Daylight Savings Time settings.

**dis**

Disables the Custom Daylight Savings Time settings.

**cur**

Displays the current Custom DST configuration.

**/cfg/sys/sflow**  
**sFlow Configuration Menu**

```
[sFlow Menu]
  ena      - Enable sFlow
  dis      - Disable sFlow
  saddress - Set the sFlow Analyzer IP address
  sport    - Set the sFlow Analyzer port
  port     - sFlow port Menu
  cur      - Display sFlow configuration
```

BLADEOS supports sFlow version 5. sFlow is a sampling method used for monitoring high speed switched networks. Use this menu to configure the sFlow agent on the switch.

**Table 142** sFlow Configuration Menu Options (/cfg/sys/sflow)

**Command Syntax and Usage**

**ena**

Enables the sFlow agent.

**dis**

Disables the sFlow agent.

**saddress** <IP address>

Defines the sFlow server address.

**sport** <1-65535>

Configures the UDP port for the sFlow server. The default value is 6343.

**Table 142** sFlow Configuration Menu Options (/cfg/sys/sflow) (continued)

**Command Syntax and Usage**

**port** <port alias or number>  
Configures the sFlow interface port.

**cur**  
Displays the current sFlow configuration.

**/cfg/sys/sflow/port** <port alias or number>  
**sFlow Port Configuration Menu**

```
[sFlow Port Menu]
  polling - Set the sFlow polling interval
  sampling - Set the sFlow sampling rate
  cur      - Display sFlow port configuration
```

Use this menu to configure the sFlow port on the switch.

**Table 143** sFlow Port Configuration Menu Options (/cfg/sys/sflow/port)

**Command Syntax and Usage**

**polling** <5-60> | 0  
Configures the sFlow polling interval, in seconds. The default value is 0 (disabled).

**sampling** <256-65536> | 0  
Configures the sFlow sampling rate, in packets per sample. The default value is 0 (disabled).

**cur**  
Displays the current sFlow port configuration.

*/cfg/port <port alias or number>*  
**Port Configuration Menu**

```
[Port INT1 Menu]
errdis    - ErrDisable Menu
gig        - Gig Phy Menu
udld      - UDLD Menu
oam        - OAM Menu
aclqos    - Acl/Qos Configuration Menu
stp        - STP Menu
8021ppri  - Set default 802.1p priority
pvid      - Set default port VLAN id
name       - Set port name
bpdugrd   - Enable/disable BPDU Guard
dscpmrk   - Enable/disable DSCP remarking for port
rmon       - Enable/disable RMON for port
learn      - Enable/Disable FDB Learning for port
tag        - Enable/disable VLAN tagging for port
tagpvid    - Enable/disable tagging on pvid
fastfwd    - Enable/disable Port Fast Forwarding mode
floodblk   - Enable/disable Port flood blocking
brate      - Set BroadCast Threshold
mrate      - Set MultiCast Threshold
drate      - Set Dest. Lookup Fail Threshold
ena         - Enable port
dis         - Disable port
cur         - Display current port configuration
```

Use the Port Configuration menu to configure settings for internal ports (INTx) and external ports (EXTx).

**Table 144** Port Configuration Menu (/cfg/port)

**Command Syntax and Usage**

**errdis**

Displays the Error Disable and Recovery menu. To view menu options, see [page 285](#).

**gig**

If a port is configured to support Gigabit Ethernet, this option displays the Gigabit Ethernet Physical Link Menu. To view menu options, see [page 286](#).

**udld**

Displays the Unidirectional Link Detection (UDLD) Menu. To view menu options, see [page 287](#).

**Table 144** Port Configuration Menu (/cfg/port) (continued)**Command Syntax and Usage****oam**

Displays the OAM Discovery Configuration Menu. To view menu options, see [page 288](#).

**aclqos**

Displays the ACL/QoS Configuration Menu. To view menu options, see [page 289](#).

**stp**

Displays the Spanning Tree Port menu. To view menu options, see [page 290](#).

**8021ppri** <0-7>

Configures the port's 802.1p priority level.

**pvid** <VLAN number>

Sets the default VLAN number which will be used to forward frames which are not VLAN tagged. The default number is 1 for non-management ports.

**name** <1-64 characters> | **none**

Sets a name for the port. The assigned port name appears next to the port number on some information and statistics screens. The default setting is **none**.

**bpdugrd** **e** | **d**

Enables or disables BPDU guard, to avoid spanning-tree loops on ports with Port Fast Forwarding enabled.

**dscpmark**

Enables or disables DSCP re-marking on a port.

**rmon** **e** | **d**

Enables or disables Remote Monitoring for the port. RMON must be enabled for any RMON configurations to function.

**learn** **disable** | **enable**

Enables or disables FDB learning on the port.

**tag** **disable** | **enable**

Disables or enables VLAN tagging for this port. The default setting is disabled for external ports (EXTx) and enabled for internal server ports (INTx).



**Table 144** Port Configuration Menu (/cfg/port) (continued)

---

**Command Syntax and Usage**

---

**tagpvid disable | enable**

Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default setting is `disabled` for external (EXTx) ports and internal server ports (INTx), and `enabled` for MGT ports.

---

**fastfwd disable | enable**

Disables or enables Port Fast Forwarding, which permits a port that participates in Spanning Tree to bypass the Listening and Learning states and enter directly into the Forwarding state. While in the Forwarding state, the port listens to the BPDUs to learn if there is a loop and, if dictated by normal STG behavior (following priorities, etc.), the port transitions into the Blocking state. This feature permits the VFSM to interoperate well within Rapid Spanning Tree networks.

---

**floodblk disable | enable**

Enables or disables port Flood Blocking. When enabled, unicast and multicast packets with unknown destination MAC addresses are blocked from the port.

---

**brate <0-262143> | dis**

Limits the number of broadcast packets per second to the specified value. If disabled (`dis`), the port forwards all broadcast packets.

---

**mrate <0-262143> | dis**

Limits the number of multicast packets per second to the specified value. If disabled (`dis`), the port forwards all multicast packets.

---

**drate <0-262143> | dis**

Limits the number of unknown unicast packets per second to the specified value. If disabled (`dis`), the port forwards all unknown unicast packets.

---

**ena**

Enables the port.

---

**dis**

Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to [“Temporarily Disabling a Port” on page 285.](#))

---

**cur**

Displays current port parameters.

---

## Temporarily Disabling a Port

To temporarily disable a port without changing its stored configuration attributes, enter the following command at any prompt:

Main# **/oper/port** *<port alias or number>* **/dis**

Because this configuration sets a temporary state for the port, you do not need to use `apply` or `save`. The port state will revert to its original configuration when the VFSM is reset. See the “Operations Menu” on page 477 for other operations-level commands.

## `/cfg/port` *<port alias or number>* `/errdis` Port Error Disable and Recovery Configuration

[Port 2 ErrDisable Menu]  
ena        - Enable ErrDisable recovery  
dis        - Disable ErrDisable recovery  
cur        - Display current ErrDisable configuration

The Error Disable and Recovery feature allows the switch to automatically disable a port if an error condition is detected on the port. The port remains in the error-disabled state until it is re-enabled manually, or re-enabled automatically by the switch after a timeout period has elapsed. The error-disabled state of a port does not persist across a system reboot.

**Table 145** Port Error Disable Configuration Options

---

### Command Syntax and Usage

---

#### **ena**

Enables automatic error-recovery for the port. The default setting is `enabled`.

**Note:** Error-recovery must be enabled globally before port-level commands become active (`/cfg/sys/errdis/ena`).

---

#### **dis**

Enables automatic error-recovery for the port.

---

#### **cur**

Displays current port Error Disable parameters.

---

`/cfg/port` *<port alias or number>* `/gig`  
**Port Link Configuration Menu**

[Gigabit Link Menu]	
speed	- Set link speed
mode	- Set full or half duplex mode
fctl	- Set flow control
auto	- Set autonegotiation
cl73	- Enable/disable Clause 73 auto-negotiation mode
cur	- Display current gig link configuration

Link menu options are described in the following table.

**Table 146** Port Link Configuration Menu Options (`/cfg/port/gig`)

---

**Command Syntax and Usage**

---

**speed** `10|100|1000|10000|any`

Sets the link speed. Some options are not valid on all ports. The choices include:

- ☐ 10 Mbps
- ☐ 100 Mbps
- ☐ 1000 Mbps
- ☐ 10000 Mps
- ☐ any (auto negotiate port speed)

**Note:** External 1/10Gb port speed becomes fixed when a transceiver is plugged into the port.

---

**mode** `full|half|any`

Sets the operating mode. Some options are not valid on all ports. The choices include:

- ☐ Full-duplex
- ☐ Half-duplex
- ☐ “Any,” for auto negotiation (default)

---

**fctl** `rx|tx|both|none`

Sets the flow control. The choices include:

- ☐ Receive flow control
- ☐ Transmit flow control
- ☐ Both receive and transmit flow control (default)
- ☐ No flow control

---

**auto** `on|off`

Turns auto-negotiation on or off.

---

Table 146 Port Link Configuration Menu Options (/cfg/port/gig) (continued)

Command Syntax and Usage

c173 e|d

Enables or disables 802.3 Clause 73 for high-speed backplane autonegotiation. The default setting is enabled.

**Note:** This command applies only to internal ports (INTx).

cur

Displays current port parameters.

/cfg/port <port alias or number> /udld  
UniDirectional Link Detection Configuration Menu

[UDLD Menu]	
mode	- Set UDLD mode
ena	- Enable UDLD
dis	- Disable UDLD
cur	- Display current port UDLD configuration

UDLD menu options are described in the following table.

Table 147 Port UDLD Configuration Menu Options (/cfg/port/udld)

Command Syntax and Usage

mode normal|aggressive

Configures the UDLD mode for the selected port, as follows:

- **Normal:** Detect unidirectional links that have mis-connected interfaces. The port is disabled if UDLD determines that the port is mis-connected.
- **Aggressive:** In addition to the normal mode, the aggressive mode disables the port if the neighbor stops sending UDLD probes for 7 seconds.

ena

Enables UDLD on the port.

dis

Disables UDLD on the port.

cur

Displays current port UDLD parameters.

**/cfg/port** *<port alias or number>* /oam  
**Port OAM Configuration Menu**

[OAM Menu]	
ena	- Enable OAM Discovery process
dis	- Disable OAM Discovery process
mode	- Set OAM mode
cur	- Display current port OAM configuration

Operation, Administration, and Maintenance (OAM) protocol allows the switch to detect faults on the physical port links. OAM is described in the IEEE 802.3ah standard.

OAM menu options are described in the following table.

**Table 148** Port OAM Configuration Menu Options (/cfg/port/oam)

<b>Command Syntax and Usage</b>	
<b>ena</b>	Enables OAM discovery on the port.
<b>dis</b>	Disables OAM discovery on the port.
<b>mode active passive</b>	Configures the OAM discovery mode, as follows: <ul style="list-style-type: none"><li>□ Active: This port link initiates OAM discovery.</li><li>□ Passive: This port allows its peer link to initiate OAM discovery.</li></ul> If OAM determines that the port is in an anomalous condition, the port is disabled.
<b>cur</b>	Displays current port OAM parameters.

**/cfg/port** *<port alias or number>* /aclqos  
**Port ACL Configuration Menu**

[Port INT2 ACL Menu]	
add	- Add ACL or ACL group to this port
rem	- Remove ACL or ACL group from this port
cur	- Display current ACLs for this port

**Table 149** Port ACL Menu Options (/cfg/port/aclqos)

**Command Syntax and Usage**

**add acl | grp** *<1-256>*

Adds the specified ACL or ACL Group to the port. You can add multiple ACL Groups to a port.

**rem acl | grp** *<1-256>*

Removes the specified ACL or ACL Group from the port.

**cur**

Displays current ACL QoS parameters.

`/cfg/port <port alias or number> /stp`  
**Port Spanning Tree Configuration Menu**

[Port INT1 STP Menu]	
edge	- Enable/disable edge port (for PVRST only)
link	- Set port link type (auto, p2p, or shared; default: auto)
cur	- Display current port stp configuration

**Table 150** Port STP Menu Options (/cfg/port/stp)

**Command Syntax and Usage**

**edge e|d**

Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled).

**Note:** After you configure the port as an edge port, you must disable the port (**/oper/port x/dis**) and then re-enable the port (**/oper/port x/ena**) for the change to take effect.

**link auto|p2p|shared**

Defines the type of link connected to the port, as follows:

- ☐ auto: Configures the port to detect the link type, and automatically match its settings.
- ☐ p2p: Configures the port for Point-To-Point protocol.
- ☐ shared: Configures the port to connect to a shared medium (usually a hub).

The default link type is auto.

**cur**

Displays current STP parameters for the port.

/cfg/stack

# Stacking Configuration Menu

---

[Stacking Menu]	
swnum	- Switch Number Menu
name	- Set stack name
backup	- Set backup switch number
cur	- Display current stacking configuration

A *stack* is a group of switches that work together as a unified system. The network views a stack of switches as a single entity, identified by a single network IP address. The Stacking Configuration menu is used to configure a stack, and to define the Master and Backup interface that represents the stack on the network.

The Stacking Configuration menu is available only after Stacking is enabled and the switch is reset. For more information, see “[Stacking Boot Menu](#)” on page 493.

**Table 151** Stacking Menu Options (/cfg/stack)

---

**Command Syntax and Usage**

---

**swnum** <switch number (1-8)>

Displays the Stacking Switch menu. To view menu options, see [page 292](#).

---

**name** <1-32 characters>

Defines a name for the stack.

---

**backup** <1-8> | 0

Defines the backup switch in the stack, based on its configured switch number (csnum).

---

**cur**

Displays the current stacking parameters.

---



`/cfg/stack/swnum <1-8>`  
**Stacking Switch Menu**

[Switch 1 Menu]	
uuid	- Set Switch Chassis UUID
bay	- Set Switch Bay Number
bind	- Bind UUID/Bay to switch in stack
del	- Delete switch
cur	- Display current Switch configuration

**Table 152** Stacking Switch Menu Options (/cfg/stack/swnum)

---

**Command Syntax and Usage**

---

**uuid** *<UUID>*

Binds the selected switch to the stack, based on the UUID of the chassis in which the switch resides. You also must enter the bay number to specify a switch within the chassis. Following is an example UUID:

**uuid 49407441b1a511d7b95df58f4b6f99fe**

---

**bay** *<1-10>*

Binds the selected switch to the stack, based on its bay number in the chassis. You also must enter the UUID to specify the chassis in which the switch resides.

---

**bind** *<asnum (1-8)>*

Binds the selected switch to the stack, based on its attached switch number (asnum).

---

**del**

Deletes the selected switch from the stack.

---

**cur**

Displays the current stacking switch parameters.

---

/cfg/qos

## Quality of Service Configuration Menu

---

[QOS Menu]	
8021p	- 802.1p Menu
dscp	- Dscp Menu
cur	- Display current QOS configuration

Use the Quality of Service (QoS) menus to configure the 802.1p priority value and DiffServ Code Point (DSCP) value of incoming packets. This allows you to differentiate between various types of traffic, and provide different priority levels.

**Table 153** Quality of Service Menu Options (/cfg/qos)

---

**Command Syntax and Usage**

---

**8021p**

Displays 802.1p configuration menu. To view menu options, see [page 294](#).

---

**dscp**

Displays DSCP configuration menu. To view menu options, see [page 295](#).

---

**cur**

Displays QoS configuration parameters.

---

/cfg/qos/8021p  
802.1p Configuration Menu

[802.1p Menu]

priq

- Set priority to COS queue mapping

qweight

- Set weight to a COS queue

numcos

- Set number of COS queue

cur

- Display current 802.1p configuration

This feature provides the capability to filter IP packets based on the 802.1p bits in the packet's VLAN header. The 802.1p bits specify the priority that you should give to the packets while forwarding them. The packets with a higher (non-zero) priority bits are given forwarding preference over packets with numerically lower priority bits value.

Table 154 802.1p Menu Options (/cfg/qos/8021p)

Command Syntax and Usage

**priq** <priority (0-7)> <COSq number>

Maps the 802.1p priority to the Class of Service queue (COSq) priority. Enter the 802.1p priority value (0-7), followed by the COSq that handles the matching traffic. The valid range of the COSq number is set using the `numcos` command.

**Note:** Priority value 7 is reserved for Stacking.

**qweight** <COSq number> <weight (0-15)>

Configures the weight of the selected COSq. Enter the COSq number, followed by the scheduling weight (0-15). The valid range of the COSq number is set using the `numcos` command.

**numcos** 2 | 8

Sets the number of Class of Service queues (COSq) for switch ports. Depending on the `numcos` setting, the valid COSq range for the `priq` and `qweight` commands is as follows:

- ☐ If `numcos` is 2 (the default), the COSq range is 0-1.
- ☐ If `numcos` is 8, the COSq range is 0-7.

You must apply, save, and reset the switch to activate the new configuration.

**Note:** In Stacking mode, the number of COS queues available is 1 or 7, because one COS queue is reserved for Stacking.

**cur**

Displays the current 802.1p parameters.

/cfg/qos/dscp  
DSCP Configuration Menu

[dscp Menu]	
dscp	- Remark DSCP value to a new DSCP value
prio	- Remark DSCP value to a 802.1p priority
on	- Globally turn DSCP remarking ON
off	- Globally turn DSCP remarking OFF
cur	- Display current DSCP remarking configuration

Use this menu map the DiffServ Code Point (DSCP) value of incoming packets to a new value, or to an 802.1p priority value.

Table 155 DSCP Menu Options (/cfg/qos/dscp)

Command Syntax and Usage

**dscp** <DSCP (0-63)> <new DSCP (0-63)>

Maps the initial DiffServ Code Point (DSCP) value to a new value. Enter the DSCP value (0-63) of incoming packets, followed by the new value.

**prio** <DSCP (0-63)> <priority (0-7)>

Maps the DiffServ Code point value to an 802.1p priority value. Enter the DSCP value, followed by the corresponding 802.1p value.

**on**

Turns on DSCP re-marking globally.

**off**

Turns off DSCP re-marking globally.

**cur**

Displays the current DSCP parameters.

/cfg/acl

# Access Control List Configuration Menu

---

[ACL Menu]	
acl	- Access Control List Item Config Menu
group	- Access Control List Group Config Menu
vmap	- Vlan Map Config Menu
cur	- Display current ACL configuration

Use this menu to create Access Control Lists (ACLs) and ACL Groups. ACLs define matching criteria used for IP filtering and Quality of Service functions.

For information about assigning ACLs to ports, see [“Port ACL Configuration Menu” on page 289](#).

**Table 156** ACL Menu Options (/cfg/acl)

---

**Command Syntax and Usage**

---

- acl** <1-256>

Displays Access Control List configuration menu. To view menu options, see [page 297](#).
- group** <1-256>

Displays ACL Group configuration menu. To view menu options, see [page 308](#).
- vmap** <1-128>

Displays ACL VLAN Map configuration menu. To view menu options, see [page 307](#).
- cur**

Displays the current ACL parameters.
-

*/cfg/acl/acl <ACL number>*  
**ACL Configuration Menu**

[ACL 1 Menu]	
ethernet	- Ethernet Header Options Menu
ipv4	- IP Header Options Menu
tcpudp	- TCP/UDP Header Options Menu
meter	- ACL Metering Configuration Menu
re-mark	- ACL Re-mark Configuration Menu
pktfmt	- Set to filter specific packet format types
egrport	- Set to filter for packets egressing this port
action	- Set filter action
stats	- Enable/disable statistics for this acl
reset	- Reset filtering parameters
cur	- Display current filter configuration

These menus allow you to define filtering criteria for each Access Control List (ACL).

**Table 157** ACL Menu Options (/cfg/acl/acl x)

**Command Syntax and Usage**

**ethernet**

Displays the ACL Ethernet Header menu. To view menu options, see [page 298](#).

**ipv4**

Displays the ACL IP Header menu. To view menu options, see [page 299](#).

**tcpudp**

Displays the ACL TCP/UDP Header menu. To view menu options, see [page 301](#).

**meter**

Displays the ACL Metering menu. To view menu options, see [page 302](#).

**re-mark**

Displays the ACL Re-mark menu. To view menu options, see [page 303](#).

**pktfmt** *<packet format>*

Displays the ACL Packet Format menu. To view menu options, see [page 306](#).

**egrport** *<port alias or number>*

Configures the ACL to function on egress packets.

Table 157 ACL Menu Options (/cfg/acl/acl x) (continued)

Command Syntax and Usage

**action** **permit** | **deny** | **setprio** <0-7>

Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7).

**stats** **e** | **d**

Enables or disables the statistics collection for the Access Control List.

**reset**

Resets the ACL parameters to their default values.

**cur**

Displays the current ACL parameters.

/cfg/acl/acl <ACL number>/ethernet  
Ethernet Filtering Configuration Menu

smac	- Set to filter on source MAC
dmac	- Set to filter on destination MAC
vlan	- Set to filter on VLAN ID
etype	- Set to filter on ethernet type
pri	- Set to filter on priority
reset	- Reset all fields
cur	- Display current parameters

This menu allows you to define Ethernet matching criteria for an ACL.

Table 158 Ethernet Filtering Menu Options (/cfg/acl/acl x/ethernet)

Command Syntax and Usage

**smac** <MAC address (such as 00:60:cf:40:56:00)> <mask (FF:FF:FF:FF:FF:FF)>

Defines the source MAC address for this ACL.

**dmac** <MAC address (such as 00:60:cf:40:56:00)> <mask (FF:FF:FF:FF:FF:FF)>

Defines the destination MAC address for this ACL.

**vlan** <VLAN number> <VLAN mask (0xfff)>

Defines a VLAN number and mask for this ACL.

**Table 158** Ethernet Filtering Menu Options (/cfg/acl/acl x/ethernet) (continued)

**Command Syntax and Usage**

**etype** [ARP | IP | IPv6 | MPLS | RARP | any | none | <other (0x600-0xFFFF)>]

Defines the Ethernet type for this ACL.

**pri** <0-7>

Defines the Ethernet priority value for the ACL.

**reset**

Resets Ethernet parameters for the ACL to their default values.

**cur**

Displays the current Ethernet parameters for the ACL.

**/cfg/acl/acl <ACL number>/ipv4**  
**IP version 4 Filtering Configuration Menu**

[Filtering IPv4 Menu]  
sip - Set to filter on source IP address  
dip - Set to filter on destination IP address  
proto - Set to filter on prototype  
tos - Set to filter on TOS  
reset - Reset all fields  
cur - Display current parameters

This menu allows you to define IPv4 matching criteria for an ACL.

**Table 159** IP version 4 Filtering Menu Options (/cfg/acl/acl x/ipv4)

**Command Syntax and Usage**

**sip** <IP address> <mask (such as 255.255.255.0)>

Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation.

**dip** <IP address> <mask (such as 255.255.255.0)>

Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.



**Table 159** IP version 4 Filtering Menu Options (/cfg/acl/acl x/ipv4) (continued)

---

**Command Syntax and Usage**

---

**proto** <0-255>

Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols.

**Number    Name**

1	icmp
2	igmp
6	tcp
17	udp
89	ospf
112	vrrp

---

**tos** <0-255>

Defines a Type of Service (ToS) value for the ACL. For more information on ToS, refer to RFC 1340 and 1349.

---

**reset**

Resets the IPv4 parameters for the ACL to their default values.

---

**cur**

Displays the current IPV4 parameters.

---

/cfg/acl/acl <ACL number>/tcpudp  
TCP/UDP Filtering Configuration Menu

[Filtering TCP/UDP Menu]	
sport	- Set to filter on TCP/UDP source port
dport	- Set to filter on TCP/UDP destination port
flags	- Set to filter TCP/UDP flags
reset	- Reset all fields
cur	- Display current parameters

This menu allows you to define TCP/UDP matching criteria for an ACL.

Table 160 TCP/UDP Filtering Menu Options (/cfg/acl/acl x/tcpudp)

Command Syntax and Usage

**sport** <source port (1-65535)> <mask (0xFFFF)>

Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed below are some of the well-known ports:

Number Name

20	ftp-data
21	ftp
22	ssh
23	telnet
25	smtp
37	time
42	name
43	whois
53	domain
69	tftp
70	gopher
79	finger
80	http

**dport** <destination port (1-65535)> <mask (0xFFFF)>

Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with **sport** above.

**flags** <value (0x0-0x3f)> <mask (0x0-0x3f)>

Defines a TCP/UDP flag for the ACL.

**Table 160** TCP/UDP Filtering Menu Options (/cfg/acl/acl x/tcpudp) (continued)

**Command Syntax and Usage**

**reset**

Resets the TCP/UDP parameters for the ACL to their default values.

**cur**

Displays the current TCP/UDP Filtering parameters.

**/cfg/acl/acl <ACL number>/meter**  
**ACL Metering Configuration Menu**

[Metering Menu]	
cir	- Set committed rate in KiloBits/s
mbsize	- Set maximum burst size in KiloBits
enable	- Enable/disable port metering
dpass	- Set to Drop or Pass out of profile traffic
reset	- Reset meter parameters
cur	- Display current settings

This menu defines the metering profile for the selected ACL.

**Table 161** ACL Metering Menu Options (/cfg/acl/acl x/meter)

**Command Syntax and Usage**

**cir <64-10000000>**

Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64.

**mbsize <32-4096>**

Configures the maximum burst size, in Kilobits. Enter one of the following values for mbsize: 32, 64, 128, 256, 512, 1024, 2048, 4096

**enable e|d**

Enables or disables metering on the ACL.

**dpass drop|pass**

Configures the ACL Meter to either drop or pass out-of-profile traffic.

**Table 161** ACL Metering Menu Options (/cfg/acl/acl x/meter) (continued)

**Command Syntax and Usage**

**reset**

Reset ACL Metering parameters to their default values.

**cur**

Displays current ACL Metering parameters.

**/cfg/acl/acl <ACL number>/re-mark  
Re-Mark Configuration Menu**

[Re-mark Menu]	
inprof	- In Profile Menu
outprof	- Out Profile Menu
uplp	- Set Update User Priority Menu
reset	- Reset re-mark settings
cur	- Display current settings

You can choose to re-mark IP header data for the selected ACL. You can configure different re-mark values, based on whether packets fall within the ACL Metering profile, or out of the ACL Metering profile.

**Table 162** ACL Re-mark Menu Options (/cfg/acl/acl x/re-mark)

**Command Syntax and Usage**

**inprof**

Displays the re-mark In-Profile Menu. To view menu options, see [page 304](#).

**outprof**

Displays the re-mark Out-of-Profile Menu. To view menu options, see [page 305](#).

**uplp**

Displays the Re-Mark In-Profile Update User Priority Menu. To view menu options, see [page 305](#).

**reset**

Reset ACL re-mark parameters to their default values.

**cur**

Displays current re-mark parameters.

**/cfg/acl/acl <ACL number>/re-mark/inprof**  
Re-Marking In-Profile Configuration Menu

[Re-marking - In Profile Menu]	
updscp	- Set the update DSCP
reset	- Reset update DSCP settings
cur	- Display current settings

**Table 163** ACL Re-Mark In-Profile Menu (/cfg/acl/acl x/re-mark/inprof)

**Command Syntax and Usage**

**updscp** <0-63>

Sets the DiffServ Code Point (DSCP) of In-Profile packets to the selected value.

**reset**

Resets the update DSCP parameters to their default values.

**cur**

Displays current Re-Mark In-Profile parameters.

**/cfg/acl/acl <ACL number>/re-mark/outprof**  
Re-Marking Out-of-Profile Configuration Menu

[Re-marking - Out Of Profile Menu]	
updscp	- Set the update DSCP
reset	- reset update DSCP setting
cur	- Display current settings

**Table 164** ACL Re-Mark Out-of-Profile Menu (/cfg/acl/acl x/re-mark/outprof)

**Command Syntax and Usage**

**updscp** <0-63>

Sets the DiffServ Code Point (DSCP) of Out-of-Profile packets to the selected value. The switch sets the DSCP value on Out-of-Profile packets.

**reset**

Resets the update DSCP parameters for Out-of-Profile packets to their default values.

**cur**

Displays current Re-Mark Out-of-Profile parameters.

**/cfg/acl/acl <ACL number>/re-mark/up1p**  
Update User Priority Configuration Menu

[Update User Priority Menu]	
value	- Set the update user priority
utosp	- Enable/Disable use of TOS precedence
reset	- Reset in profile up1p settings
cur	- Display current settings

**Table 165** ACL Re-Mark User Priority Menu (/cfg/acl/acl x/re-mark/inprof/up1p)

**Command Syntax and Usage**

**value** <0-7>

Defines the 802.1p value. The value is the priority bits information in the packet structure.

**utosp enable | disable**

Enable or disable mapping of TOS (Type of Service) priority to 802.1p priority for In-Profile packets. When enabled, the TOS value is used to set the 802.1p value.

**Table 165** ACL Re-Mark User Priority Menu (/cfg/acl/acl x/  
re-mark/inprof/up1p) (continued)

Command Syntax and Usage	
<b>reset</b>	Resets UP1P settings to their default values.
<b>cur</b>	Displays current Re-Mark In-Profile User Priority parameters.

**/cfg/acl/acl <ACL number>/pktfmt**  
**Packet Format Filtering Configuration Menu**

[Filtering Packet Format Menu]	
ethfmt	- Set to filter on ethernet format
tagfmt	- Set to filter on ethernet tagging format
ipfmt	- Set to filter on IP format
reset	- Reset all fields
cur	- Display current parameters

This menu allows you to define Packet Format matching criteria for an ACL.

**Table 166** ACL Packet Format Filtering Menu Options (/cfg/acl/acl x/pktfmt)

Command Syntax and Usage	
<b>ethfmt {none eth2 SNAP LLC}</b>	Defines the Ethernet format for the ACL.
<b>tagfmt {disabled any none tagged}</b>	Defines the tagging format for the ACL.
<b>ipfmt {none v4 v6}</b>	Defines the IP format for the ACL.
<b>reset</b>	Resets Packet Format parameters for the ACL to their default values.
<b>cur</b>	Displays the current Packet Format parameters for the ACL.

## /cfg/acl/vmap <1-128> VMAP Configuration

```
[VMAP 1 Menu]
  ethernet - Ethernet Header Options Menu
  ipv4     - IP Header Options Menu
  tcpudp   - TCP/UDP Header Options Menu
  meter    - ACL Metering Configuration Menu
  re-mark  - ACL Re-mark Configuration Menu
  pktfmt   - Set to filter specific packet format types
  egrport  - Set to filter for packets egressing this port
  action   - Set filter action
  stats    - Enable/disable statistics
  reset    - Reset filtering parameters
  cur      - Display current filter configuration
```

A VLAN Map is an Access Control List (ACL) that can be assigned to a VLAN or a VM group instead of a port. In a virtualized environment where Virtual Machines move between physical servers, VLAN Maps allow you to create traffic filtering and metering policies associated with a VM's VLAN.

For more information about VLAN Map configuration commands, see [“Access Control List Configuration Menu” on page 296](#).

For more information about assigning VLAN Maps to a VLAN, see [“VLAN Configuration Menu” on page 355](#).

For more information about assigning VLAN Maps to a VM group, see [“VM Group Configuration” on page 469](#).



**/cfg/acl/group** *<ACL group number>*  
**ACL Group Configuration Menu**

[ACL Group 1 Menu]

add	- Add ACL to group
rem	- Remove ACL from group
cur	- Display current ACL items in ACL group

This menu allows you to compile one or more ACLs into an ACL Group. Once you create an ACL Group, you can assign the ACL Group to one or more ports.

**Table 167** ACL Group Menu Options (/cfg/acl/group x)

Command Syntax and Usage	
<b>add acl</b> <i>&lt;1-256&gt;</i>	Adds the selected ACL to the ACL Group.
<b>rem acl</b> <i>&lt;1-256&gt;</i>	Removes the selected ACL from the ACL Group.
<b>cur</b>	Displays the current ACL group parameters.

/cfg/pmirr

# Port Mirroring Configuration

```
[Port Mirroring Menu]
monport - Monitoring Port based PM Menu
mirror   - Enable/Disable Mirroring
cur      - Display All Mirrored and Monitoring Ports
```

Port mirroring is disabled by default. For more information about port mirroring on the VFSM, see “Appendix A: Troubleshooting” in the *BLADEOS Application Guide*.

**Note** – Traffic on VLAN 4095 is not mirrored to the external ports.

The Port Mirroring Menu is used to configure, enable, and disable the monitor port. When enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitor port. By attaching a network analyzer to the monitor port, you can collect detailed information about your network performance and usage.

**Table 168** Port Mirroring Menu Options (/cfg/pmirr)

### Command Syntax and Usage

**monport** <port alias or number>

Displays port-mirroring menu. To view menu options, see [page 310](#).

**mirror disable | enable**

Enables or disables port mirroring

**cur**

Displays current settings of the mirrored and monitoring ports.

*/cfg/pmirr/monport <port alias or number>*  
**Port-Mirroring Configuration Menu**

[Port EXT1 Menu]	
add	- Add "Mirrored" port
rem	- Rem "Mirrored" port
delete	- Delete this "Monitor" port
cur	- Display current Port-based Port Mirroring configuration

**Table 169** Port Mirroring Monitor Port Menu Options (/cfg/pmirr/monport)

---

**Command Syntax and Usage**

---

**add** *<mirrored port (port to mirror from)> <direction (in, out, or both)>*

Adds the port to be mirrored. This command also allows you to enter the direction of the traffic. It is necessary to specify the direction because:

If the source port of the frame matches the mirrored port and the mirrored direction is ingress or both (ingress and egress), the frame is sent to the monitoring port.

If the destination port of the frame matches the mirrored port and the mirrored direction is egress or both, the frame is sent to the monitoring port.

---

**rem** *<mirrored port (port to mirror from)>*

Removes the mirrored port.

---

**delete**

Deletes this monitor port.

---

**cur**

Displays the current settings of the monitoring port.

---

/cfg/12

# Layer 2 Configuration Menu

[Layer 2 Menu]	
8021x	- 802.1x Menu
amp	- Active Multipath Menu
mrst	- Multiple Spanning Tree/Rapid Spanning Tree Menu
nostp	- Disable Spanning Tree
stg	- Spanning Tree Menu
fdb	- FDB Menu
lldp	- LLDP Menu
trunk	- Trunk Group Menu
thash	- IP Trunk Hash Menu
lacp	- Link Aggregation Control Protocol Menu
failovr	- Failover Menu
hotlink	- Hot Links Menu
vlan	- VLAN Menu
pvstcomp	- Enable/disable PVST+ compatibility mode
macnotif	- Enable/disable MAC address notification
upfast	- Enable/disable Uplink Fast
update	- UplinkFast station update rate
cur	- Display current layer 2 parameters

Table 170 Layer 2 Configuration Menu (/cfg/l2)

Command Syntax and Usage

8021x

Displays the 802.1X Configuration Menu. To view menu options, see [page 313](#).

amp

Displays the Active MultiPath Protocol (AMP) Configuration menu. To view menu options, see [page 319](#).

mrst

Displays the Rapid Spanning Tree/Multiple Spanning Tree Protocol Configuration Menu. To view menu options, see [page 323](#).

nostp enable|disable

When enabled, globally turns Spanning Tree off. All ports are placed into forwarding state. Any BPDU's received are flooded. BPDU Guard is not affected by this command.

stg <group number (1-128)>

Displays the Spanning Tree Configuration Menu. To view menu options, see [page 328](#).

**Table 170** Layer 2 Configuration Menu (/cfg/l2) (continued)**Command Syntax and Usage****fdb**

Displays the Forwarding Database Menu. To view menu options, see [page 332](#).

**lldp**

Displays the LLDP Menu. To view menu options, see [page 335](#).

**trunk** <trunk number>

Displays the Trunk Group Configuration Menu. To view menu options, see [page 339](#).

**thash**

Displays the IP Trunk Hash Menu. To view menu options, see [page 340](#).

**lACP**

Displays the Link Aggregation Control Protocol Menu. To view menu options, see [page 343](#).

**failover**

Displays the Failover Configuration Menu. To view menu options, see [page 345](#).

**hotlink**

Displays the Hot Links Configuration menu. To view menu options, see [page 351](#).

**vlan** <VLAN number (1-4095)>

Displays the VLAN Configuration Menu. To view menu options, see [page 355](#).

**pvstcomp enable|disable**

Enables or disables VLAN tagging of Spanning Tree BPDUs. The default setting is **enabled**.

**macnotif enable|disable**

Enables or disables MAC Address Notification. With MAC Address Notification enabled, the switch generates a syslog message when a MAC address is added or removed from the MAC address table.

**upfast enable|disable**

Enables or disables Fast Uplink Convergence, which provides rapid Spanning Tree convergence to an upstream switch during failover.

**Note:** When enabled, this feature increases bridge priorities to 65535 for all STGs and path cost by 3000 for all external STP ports.

Table 170 Layer 2 Configuration Menu (/cfg/l2) (continued)

Command Syntax and Usage

**update** <10-200>

Configures the station update rate. The default value is 40.

**cur**

Displays current Layer 2 parameters.

/cfg/l2/8021x  
802.1X Configuration Menu

```
[802.1x Configuration Menu]
global      - Global 802.1x configuration menu
port        - Port 802.1x configuration menu
ena         - Enable 802.1x access control
dis         - Disable 802.1x access control
cur         - Show 802.1x configuration
```

This feature allows you to configure the VFSM as an IEEE 802.1X Authenticator, to provide port-based network access control.

Table 171 802.1X Configuration Menu (/cfg/l2/8021x)

Command Syntax and Usage

**global**

Displays the global 802.1X Configuration Menu. To view menu options, see [page 314](#).

**port** <port alias or number>

Displays the 802.1X Port Menu. To view menu options, see [page 317](#).

**ena**

Globally enables 802.1X.

**dis**

Globally disables 802.1X.

**cur**

Displays current 802.1X parameters.

## /cfg/12/8021x/global

### 802.1X Global Configuration Menu

```
[802.1X Global Configuration Menu]
  gvlan      - 802.1X Guest VLAN configuration menu
  mode       - Set access control mode
  qtperiod   - Set EAP-Request/Identity quiet time interval
  txperiod   - Set EAP-Request/Identity retransmission timeout
  suptmout   - Set EAP-Request retransmission timeout
  svrtmout   - Set server authentication request timeout
  maxreq     - Set max number of EAP-Request retransmissions
  raperiod   - Set reauthentication time interval
  reauth     - Set reauthentication status to on or off
  vassign    - Set dynamic VLAN assignment status to on or off
  default    - Restore default 802.1X configuration
  cur        - Display current 802.1X configuration
```

The global 802.1X menu allows you to configure parameters that affect all ports in the VFSM.

**Table 172** 802.1X Global Configuration Menu Options (/cfg/12/8021x/global)

---

#### Command Syntax and Usage

---

##### **gvlan**

Displays the 802.1X Guest VLAN Configuration Menu. To view menu options, see [page 316](#).

---

##### **mode force-unauth | auto | force-auth**

Sets the type of access control for all ports:

- ☐ **force-unauth**: the port is unauthorized unconditionally.
- ☐ **auto**: the port is unauthorized until it is successfully authorized by the RADIUS server.
- ☐ **force-auth**: the port is authorized unconditionally, allowing all traffic.

The default value is **force-auth**.

---

##### **qtperiod <0-65535>**

Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.

---

##### **txperiod <1-65535>**

Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.

---

**Table 172** 802.1X Global Configuration Menu Options (/cfg/l2/8021x/global)**Command Syntax and Usage****suptmout** <1-65535>

Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet to the authentication server. The default value is 30 seconds.

**svrtmout** <1-65535>

Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds.

The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of /cfg/sys/radius/timeout (default is 3 seconds).

**maxreq** <1-10>

Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.

**raperiod** <1-604800>

Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.

**reauth** on|off

Sets the re-authentication status to on or off. The default value is off.

**vassign** on|off

Sets the dynamic VLAN assignment status to on or off. The default value is off.

**default**

Resets the global 802.1X parameters to their default values.

**cur**

Displays current global 802.1X parameters.



**/cfg/12/8021x/global/gvlan**  
**802.1X Guest VLAN Configuration Menu**

[802.1X Guest VLAN Configuration Menu]	
vlan	- Set 8021.x Guest VLAN number
ena	- Enable 8021.xGuest VLAN
dis	- Disable 8021.x Guest VLAN
cur	- Display current Guest VLAN configuration

The 802.1X Guest VLAN menu allows you to configure a Guest VLAN for unauthenticated ports. The Guest VLAN provides limited access to switch functions.

**Table 173** 802.1X Guest VLAN Configuration Menu  
(/cfg/12/8021x/global/gvlan)

---

**Command Syntax and Usage**

---

**vlan** <VLAN number>

Configures the Guest VLAN number.

---

**ena**

Enables the 802.1X Guest VLAN.

---

**dis**

Disables the 802.1X Guest VLAN.

---

**cur**

Displays current 802.1X Guest VLAN parameters.

---

## `/cfg/12/8021x/port` *<port alias or number>* 802.1X Port Configuration Menu

```
[802.1X Port Configuration Menu]
mode      - Set access control mode
qtperiod  - Set EAP-Request/Identity quiet time interval
txperiod  - Set EAP-Request/Identity retransmission timeout
suptmout  - Set EAP-Request retransmission timeout
svrtmout  - Set server authentication request timeout
maxreq    - Set max number of EAP-Request retransmissions
raperiod  - Set reauthentication time interval
reauth    - Set reauthentication status to on or off
vassign   - Set dynamic VLAN assignment status to on or off
default   - Restore default 802.1X configuration
global    - Apply current global 802.1X configuration to this port
cur       - Display current 802.1X configuration
```

The 802.1X port menu allows you to configure parameters that affect the selected port in the VFSM. These settings override the global 802.1X parameters.

**Table 174** 802.1X Port Configuration Menu Options (`/cfg/12/8021x/port`)

---

### Command Syntax and Usage

---

**mode** **force-unauth** | **auto** | **force-auth**

Sets the type of access control for the port:

- ☐ **force-unauth** - the port is unauthorized unconditionally.
- ☐ **auto** - the port is unauthorized until it is successfully authorized by the RADIUS server.
- ☐ **force-auth** - the port is authorized unconditionally, allowing all traffic.

The default value is `force-auth`.

---

**qtperiod** *<0-65535>*

Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.

---

**txperiod** *<1-65535>*

Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.

---

**Table 174** 802.1X Port Configuration Menu Options (/cfg/l2/8021x/port)

---

**Command Syntax and Usage**

---

**suptmout** <1-65535>

Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet to the authentication server. The default value is 30 seconds.

---

**svrtmout** <1-65535>

Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds.

The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of /cfg/sys/radius/timeout (default is 3 seconds).

---

**maxreq** <1-10>

Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.

---

**raperiod** <1-604800>

Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.

---

**reauth** on|off

Sets the re-authentication status to on or off. The default value is off.

---

**vassign** on|off

Sets the dynamic VLAN assignment status to on or off. The default value is off.

---

**default**

Resets the 802.1X port parameters to their default values.

---

**global**

Applies current global 802.1X configuration parameters to the port.

---

**cur**

Displays current 802.1X port parameters.

---

/cfg/12/amp

## Active MultiPath Protocol Configuration

[Active Multipath Menu]	
group	- Active Multipath Group Configuration Menu
agglacp	- Set active multipath aggregator LACP trunk
aggport	- Set active multipath aggregator port
aggtrk	- Set active multipath aggregator static trunk
interval	- Set active multipath packet interval
priority	- Set active multipath switch priority
timeout	- Set active multipath timeout count to detect unhealthy links
type	- Set active multipath switch type
on	- Globally turn active multipath ON
off	- Globally turn active multipath OFF
default	- Default active multipath parameters
cur	- Display current active multipath configuration

Use the following commands to configure Active Multipath (AMP) for the VFSM.

**Table 175** AMP Configuration Options

---

**Command Syntax and Usage**

---

**group** <1-22>

Displays the AMP group menu. To view menu options, see [page 321](#).

---

**agglacp** <1-65535> | 0

Configures an LACP *admin key* to be used as the AMP Aggregator link. LACP trunks formed with this *admin key* will be used to link the two AMP Aggregators. Enter 0 (zero) to clear the Aggregator link.

**Note:** This command does not apply to AMP Access switches.

---

**aggport** <port alias or number> | 0

Configures a port to be used as the AMP Aggregator link. Enter 0 (zero) to clear the Aggregator link.

**Note:** This command does not apply to AMP Access switches.

---

**aggtrk** <trunk number> | 0

Configures a trunk to be used as the AMP Aggregator link. Enter 0 (zero) to clear the Aggregator link.

**Note:** This command does not apply to AMP Access switches.

---

Table 175 AMP Configuration Options

Command Syntax and Usage	
<b>interval</b> <10-10000>	Configures the time interval between AMP <i>keep alive</i> messages, in centiseconds. The default value is 50.
<b>priority</b> <1-255>	<p>Configures the AMP priority for the switch. The default value is 255.</p> <p>A lower priority value denotes a higher precedence (so priority 1 is the highest priority.) It is recommended that aggregator switches be configured with lower priority values than access switches.</p>
<b>timeout</b> <1-20>	Configures the timeout count, which is the number of unreceived keep-alive packets the switch waits before declaring a timeout due to loss of connectivity with the peer. The default value is 4.
<b>type</b> access aggregator	<p>Defines the AMP switch type, as follows:</p> <ul style="list-style-type: none"><li>❑ <b>Access:</b> Connects to downstream servers. Only one AMP group can be configured on an access switch.</li><li>❑ <b>Aggregator:</b> Connects to upstream routers. Multiple AMP groups can be configured on an Aggregator switch.</li></ul> <p>The default switch type is <code>access</code>.</p> <p><b>Note:</b> It is recommended to configure the Virtual Fabric 10Gb Switch Module only as an access switch.</p>
<b>on</b>	Globally turns Active MultiPath on.
<b>off</b>	Globally turns Active MultiPath off.
<b>default</b>	Resets Active MultiPath parameters to their default values, and optionally delete all AMP groups.
<b>cur</b>	Displays the current AMP parameters.

/cfg/12/amp/group </-22>  
AMP Group Configuration

[AMP Group 1 Menu]

port

- Add port to AMP group

port2

- Add second port to AMP group

lACP

- Add LACP trunk to AMP group

lACP2

- Add second LACP trunk to AMP group

trunk

- Add static trunk to AMP group

trunk2

- Add second static trunk to AMP group

ena

- Enable AMP group

dis

- Disable AMP group

del

- Delete AMP group

cur

- Display current AMP group configuration

Use the following commands to configure an AMP group.

Table 176 AMP Group Configuration Options

Command Syntax and Usage

**port** <port alias or number> | 0

Adds the port as the first port in the AMP group. Enter 0 (zero) to clear the port.

**port2** <port alias or number> | 0

Adds the port as the second port in the AMP group. Enter 0 (zero) to clear the port.

**lACP** </-65535> | 0

Adds the first LACP *admin key* to the AMP group. LACP trunks formed with this *admin key* will be used for AMP communication. Enter 0 (zero) to clear the *admin key*.

**lACP2** </-65535> | 0

Adds the second LACP *admin key* to the AMP group. LACP trunks formed with this *admin key* will be used for AMP communication. Enter 0 (zero) to clear the *admin key*.

**trunk** <trunk number> | 0

Adds the first trunk group to the AMP group. Enter 0 (zero) to clear the trunk group.

**trunk2** <trunk number> | 0

Adds the second trunk group to the AMP group. Enter 0 (zero) to clear the trunk group.

**ena**

Enables the AMP group.

**Table 176** AMP Group Configuration Options

Command Syntax and Usage	
<b>dis</b>	Disables the AMP group.
<b>del</b>	Deletes the AMP group.
<b>cur</b>	Displays the current AMP group configuration.

/cfg/12/mrst

## RSTP/MSTP/PVRST Configuration Menu

[Multiple Spanning Tree Menu]	
cist	- Common and Internal Spanning Tree menu
name	- Set MST region name
rev	- Set revision level of this MST region
maxhop	- Set Maximum Hop Count for MST (4 - 60)
mode	- Spanning Tree Mode
on	- Globally turn Multiple Spanning Tree (MSTP/RSTP/PVRST) ON
off	- Globally turn Multiple Spanning Tree (MSTP/RSTP/PVRST) OFF
cur	- Display current MST parameters

BLADEOS supports the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), and Per VLAN Rapid Spanning Tree Protocol (PVRST). MSTP allows you to map many VLANs to a small number of Spanning Tree Groups (STGs), each with its own topology.

Up to 32 Spanning Tree Groups can be configured in **mstp** mode. MRST is turned on by default and the default STP mode is RSTP.

**Note** – When Multiple Spanning Tree is turned on, VLAN 4095 is moved from Spanning Tree Group 128 to the Common Internal Spanning Tree (CIST). When Multiple Spanning Tree is turned off, VLAN 4095 is moved back to Spanning Tree Group 128.

**Table 177** MSTP/RSTP/PVRST Configuration Menu Options (/cfg/12/mrst)

**Command Syntax and Usage**

**cist**

Displays the Common Internal Spanning Tree (CIST) Menu. To view menu options, see [page 325](#).

**name** <1-32 characters>

Configures a name for the MSTP region. All devices within a MSTP region must have the same region name.

**rev** <0-65535>

Configures a version number for the MSTP region. The version is used as a numerical identifier for the region. All devices within a MSTP region must have the same version number.



**Table 177** MSTP/RSTP/PVRST Configuration Menu Options (/cfg/l2/mrst)

---

**Command Syntax and Usage**

---

**maxhop** <4-60>

Configures the maximum number of bridge hops a packet may traverse before it is dropped.  
The default is 20.

---

**mode rstp|mstp|pvrst**

Selects the Spanning Tree mode, as follows: Per VLAN Rapid Spanning Tree Plus (**pvrst**), Rapid Spanning Tree (**rstp**), Multiple Spanning Tree (**mstp**).

The default mode is RSTP.

---

**on**

Globally turns RSTP/MSTP/PVRST ON.

**Note:** When RSTP is turned on, the configuration parameters for STG 1 apply to RSTP.

---

**off**

Globally turns RSTP/MSTP/PVRST OFF.

---

**cur**

Displays the current RSTP/MSTP/PVRST configuration.

---

/cfg/l2/mrst/cist  
Common Internal Spanning Tree Configuration Menu

[Common Internal Spanning Tree Menu]	
brg	- CIST Bridge parameter menu
port	- CIST Port parameter menu
add	- Add VLAN(s) to CIST
default	- Default Common Internal Spanning Tree and Member parameters
cur	- Display current CIST parameters

Table 178 describes the commands used to configure Common Internal Spanning Tree (CIST) parameters. The CIST provides compatibility with different MSTP regions and with devices running different Spanning Tree instances. It is equivalent to Spanning Tree Group 0.

Table 178 CIST Menu Options (/cfg/l2/mrst/cist)

Command Syntax and Usage

**brg**

Displays the CIST Bridge Menu. To view menu options, see [page 326](#).

**port** <port alias or number>

Displays the CIST Port Menu. To view menu options, see [page 327](#).

**add** <VLAN numbers>

Adds selected VLANs to the CIST.

**default**

Resets all CIST parameters to their default values.

**cur**

Displays the current CIST configuration.

/cfg/l2/mrst/cist/brg  
CIST Bridge Configuration Menu

[CIST Bridge Menu]

prior

- Set CIST bridge Priority (0-65535)

mxage

- Set CIST bridge Max Age (6-40 secs)

fwd

- Set CIST bridge Forward Delay (4-30 secs)

cur

- Display current CIST bridge parameters

CIST bridge parameters are used only when the switch is in MSTP mode. CIST parameters do not affect operation of STP/PVST+.

**Table 179** CIST Bridge Configuration Menu Options (/cfg/l2/mrst/cist/brg)

**Command Syntax and Usage**

**prior** <0-65535>

Configures the CIST bridge priority. The bridge priority parameter controls which bridge on the network is the MSTP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority.

The range is 0 to 65535, in steps of 4096 (0, 4096, 8192...). The default value is 61440.

**mxage** <6-40 seconds>

Configures the CIST bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the MSTP network. The range is 6 to 40 seconds, and the default is 20 seconds.

**fwd** <4-30 seconds>

Configures the CIST bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds.

**cur**

Displays the current CIST bridge configuration.

## `/cfg/l2/mrst/cist/port` *<port alias or number>* CIST Port Configuration Menu

```
[CIST Port 1 Menu]
prior   - Set port Priority (0-240)
cost    - Set port Path Cost (1-200000000, 0 for auto)
hello   - Set CIST port Hello Time (1-10 secs)
on       - Turn port's Spanning Tree ON
off      - Turn port's Spanning Tree OFF
cur      - Display current port Spanning Tree parameters
```

CIST port parameters are used to modify MRST operation on an individual port basis. CIST parameters do not affect operation of STP/PVST+, RSTP, or PVRST. For each port, RSTP/MSTP is turned on by default.

**Table 180** CIST Port Configuration Menu Options (`/cfg/l2/mrst/cist/port`)

---

### Command Syntax and Usage

---

#### **prior** *<0-240>*

Configures the CIST port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 240, in steps of 16 (0, 16, 32...), and the default is 128.

---

#### **cost** *<0-200000000>*

Configures the CIST port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows:

- 100Mbps = 200000
- 1Gbps = 20000
- 10Gbps = 2000

The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed.

---

#### **hello** *<1-10 seconds>*

Configures the CIST port Hello time. The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds, and the default is 2 seconds.

---

#### **on**

Enables MRST on the port.

---

**Table 180** CIST Port Configuration Menu Options (/cfg/l2/mrst/cist/port)

Command Syntax and Usage	
<b>off</b>	Disables MRST on the port.
<b>cur</b>	Displays the current CIST port configuration.

**/cfg/l2/stg** *<STP group index>*  
**Spanning Tree Configuration Menu**

[Spanning Tree Group 1 Menu]	
brg	- Bridge parameter menu
port	- Port parameter menu
add	- Add VLAN(s) to Spanning Tree Group
remove	- Remove VLAN(s) from Spanning Tree Group
clear	- Remove all VLANs from Spanning Tree Group
on	- Globally turn Spanning Tree ON
off	- Globally turn Spanning Tree OFF
default	- Default Spanning Tree and Member parameters
cur	- Display current bridge parameters

BLADEOS supports the IEEE 802.1D Spanning Tree Protocol (STP). STP is used to prevent loops in the network topology. Up to 128 Spanning Tree Groups can be configured on the switch (STG 128 is reserved for management).

**Note** – When VRRP is used for active/active redundancy, STG must be enabled.

**Table 181** Spanning Tree Configuration Menu (/cfg/l2/stg)

Command Syntax and Usage	
<b>brg</b>	Displays the Bridge Spanning Tree Menu. To view menu options, see <a href="#">page 329</a> .
<b>port</b> <i>&lt;port alias or number&gt;</i>	Displays the Spanning Tree Port Menu. To view menu options, see <a href="#">page 331</a> .
<b>add</b> <i>&lt;VLAN number&gt;</i>	Associates a VLAN with a Spanning Tree and requires a VLAN ID as a parameter.

**Table 181** Spanning Tree Configuration Menu (/cfg/l2/stg) (continued)

**Command Syntax and Usage**

<b>remove</b> <VLAN number>
Breaks the association between a VLAN and a Spanning Tree and requires a VLAN ID as a parameter.
<b>clear</b>
Removes all VLANs from a Spanning Tree.
<b>on</b>
Globally enables Spanning Tree Protocol. STG is turned on by default.
<b>off</b>
Globally disables Spanning Tree Protocol.
<b>default</b>
Restores a Spanning Tree instance to its default configuration.
<b>cur</b>
Displays current Spanning Tree Protocol parameters.

**/cfg/l2/stg** <STP group number> **/brg**  
Spanning Tree Bridge Configuration Menu

[Bridge Spanning Tree Menu]	
prior	- Set bridge Priority [0-65535]
hello	- Set bridge Hello Time [1-10 secs]
mxage	- Set bridge Max Age (6-40 secs)
fwd	- Set bridge Forward Delay (4-30 secs)
cur	- Display current bridge parameters

Spanning Tree bridge parameters affect the global STG operation of the switch. STG bridge parameters include:

- Bridge priority
- Bridge hello time
- Bridge maximum age
- Forwarding delay

**Table 182** Spanning Tree Bridge Menu Options (/cfg/l2/stg/brg)

---

**Command Syntax and Usage**

---

**prior** *<new bridge priority (0-65535)>*

Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STG root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The default value is 65534.

**RSTP/MSTP:** The range is 0 to 61440, in steps of 4096 (0, 4096, 8192...), and the default is 61440.

---

**hello** *<new bridge hello time (1-10 secs)>*

Configures the bridge hello time. The hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. The range is 1 to 10 seconds, and the default is 2 seconds.

This command does not apply to MSTP (see CIST on [page 325](#)).

---

**mxage** *<new bridge max age (6-40 secs)>*

Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it re configures the STG network. The range is 6 to 40 seconds, and the default is 20 seconds.

This command does not apply to MSTP (see CIST on [page 325](#)).

---

**fwd** *<new bridge Forward Delay (4-30 secs)>*

Configures the bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds.

This command does not apply to MSTP (see CIST on [page 325](#)).

---

**cur**

Displays the current bridge STG parameters.

---

When configuring STG bridge parameters, the following formulas must be used:

- $2*(fwd-1) \geq mxage$
- $2*(hello+1) \leq mxage$

*/cfg/l2/stg <STP group index>/port <port alias or number>*  
Spanning Tree Port Configuration Menu

[Spanning Tree Port EXT1 Menu]

prior

- Set port Priority (0-255)

cost

- Set port Path Cost (1-65535 (802.1D) /  
1-200000000 (MSTP/RSTP) /0 for auto)

on

- Turn port's Spanning Tree ON

off

- Turn port's Spanning Tree OFF

cur

- Display current port Spanning Tree parameters

By default for STP/PVST+, Spanning Tree is turned off for internal ports and management ports, and turned on for external ports. By default for RSTP/MSTP, Spanning Tree is turned off for internal ports and management ports, and turned on for external ports, with internal ports configured as edge ports. STG port parameters include:

- Port priority
- Port path cost

For more information about port Spanning Tree commands, see “[Port Spanning Tree Configuration Menu](#)” on page 290.

**Table 183** Spanning Tree Port Menu Options (/cfg/l2/stg/port)

**Command Syntax and Usage**

**prior** *<new port Priority (0-255)>*

Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The default value is 128.

**RSTP/MSTP:** The range is 0 to 240, in steps of 16 (0, 16, 32...).

**Note:** In Stacking mode, the range is 0-255, in steps of 4 (0, 4, 8, 12...).

**cost** *<1-65535, 0 for default>*

Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows:

- 100Mbps = 19
- 1Gbps = 4
- 10Gbps = 2

The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed.



**Table 183** Spanning Tree Port Menu Options (/cfg/l2/stg/port) (continued)

Command Syntax and Usage	
<b>on</b>	Enables STG on the port.
<b>off</b>	Disables STG on the port.
<b>cur</b>	Displays the current STG port parameters.

**/cfg/l2/fdb**  
**Forwarding Database Configuration Menu**

[FDB Menu]	
mcast	- Static Multicast Menu
static	- Static FDB Menu
aging	- Configure FDB aging value
cur	- Display current FDB configuration

Use the following commands to configure the Forwarding Database (FDB) for the VFSM.

**Table 184** FDB Menu Options (/cfg/l2/fdb)

Command Syntax and Usage	
<b>mcast</b>	Displays the static Multicast menu. To view menu options, see <a href="#">page 333</a> .
<b>static</b>	Displays the static FDB menu. To view menu options, see <a href="#">page 334</a> .
<b>aging</b> <0-65535>	Configures the aging value for FDB entries, in seconds. The default value is 300.
<b>cur</b>	Displays the current FDB parameters.

/cfg/l2/fdb/mcast

## Static Multicast MAC Configuration Menu

[Static Multicast Menu]	
add	- Add a Multicast Address entry
del	- Delete a Multicast Address entry
clear	- Clear all Multicast Address entries
cur	- Display current Multicast Address configuration

The following options are available to control the forwarding of known and unknown multicast packets:

- All multicast packets are flooded to the entire VLAN. This is the default switch behavior.
- Known multicast packets are forwarded only to those ports specified. Unknown multicast packets are flooded to the entire VLAN. To configure this option, define the Multicast MAC address for the VLAN and specify ports that are to receive multicast packets (**/cfg/l2/fdb/mcast/add**).
- Known multicast packets are forwarded only to those ports specified. Unknown multicast packets are dropped. To configure this option:
  - Define the Multicast MAC address for the VLAN and specify ports that are to receive multicast packets (**/cfg/l2/fdb/mcast/add**).
  - Enable Flood Blocking on ports that are not to receive multicast packets (**/cfg/port x/floodblk ena**).

Use the following commands to configure static Multicast MAC entries in the Forwarding Database (FDB).

**Table 185** Static Multicast MAC Menu Options (/cfg/l2/fdb/mcast)

**Command Syntax and Usage**

<b>add</b> <MAC address> <VLAN number> <port alias or number>
Adds a static multicast entry. You can list ports separated by a space, or enter a range of ports separated by a hyphen ( - ). For example:  <b>add 01:00:00:23:3f:01 200 int1-int4</b>
<b>del</b> <MAC address> <VLAN number> <port alias or number>
Deletes a static multicast entry.

**Table 185** Static Multicast MAC Menu Options (/cfg/l2/fdb/mcast) (continued)

**Command Syntax and Usage**

**clear** {**all**|**mac** <MAC address>|**vlan** <VLAN number>|  
    **port** <port alias or number>}

Clears static multicast entries.

**cur**

Display current static multicast entries.

**/cfg/l2/fdb/static**  
**Static FDB Configuration Menu**

[Static FDB Menu]

add	- Add a permanent FDB entry
del	- Delete a static FDB entry
clear	- Clear static FDB entries
cur	- Display current static FDB configuration

Use the following commands to configure static entries in the Forwarding Database (FBD).

**Table 186** Static FDB Menu Options (/cfg/l2/fdb/static)

**Command Syntax and Usage**

**add** <MAC address> <VLAN number> <port number>

Adds a permanent FDB entry. Enter the MAC address using the following format:

xx:xx:xx:xx:xx:xx

For example, 08:00:20:12:34:56

You can also enter the MAC address as follows:

xxxxxxxxxxxx

For example, 080020123456

**del** <MAC address> <VLAN number>

Deletes a permanent FDB entry.

**clear** <MAC address>|**all** {**mac**|**vlan**|**port**}

Clears static FDB entries.

**cur**

Display current static FDB configuration.

/cfg/l2/lldp  
LLDP Configuration Menu

[LLDP configuration Menu]  
port - LLDP Port Menu  
msgtxint - Set transmission interval for LLDPDU  
msgtxhld - Set holdtime multiplier for LLDP advertisement  
notifint - Set minimum interval for successive trap notification  
txdelay - Set delay interval between LLDP advertisements  
redelay - Set reinitialization delay interval  
on - Globally turn LLDP On  
off - Globally turn LLDP Off  
cur - Show current LLDP parameters

Use the following commands to configure Link Layer Detection Protocol (LLDP).

Table 187 LLDP Menu Options (/cfg/l2/lldp)

Command Syntax and Usage	
<b>port</b> <port alias or number>	Displays the LLDP Port Configuration menu. To view menu options, see <a href="#">page 336</a> .
<b>msgtxint</b> <5-32768>	Configures the message transmission interval, in seconds. The default value is 30.
<b>msgtxhld</b> <2-10>	Configures the message hold time multiplier. The hold time is configured as a multiple of the message transmission interval.  The default value is 4.
<b>notifint</b> <1-3600>	Configures the trap notification interval, in seconds. The default value is 5.
<b>txdelay</b> <1-8192>	Configures the transmission delay interval. The transmit delay timer represents the minimum time permitted between successive LLDP transmissions on a port.  The default value is 2.
<b>redelay</b> <1-10>	Configures the re-initialization delay interval, in seconds. The re-initialization delay allows the port LLDP information to stabilize before transmitting LLDP messages.  The default value is 2.

Table 187 LLDP Menu Options (/cfg/l2/lldp) (continued)

Command Syntax and Usage	
<b>on</b>	Globally turns LLDP on. The default setting is <b>on</b> .
<b>off</b>	Globally turns LLDP off.
<b>cur</b>	Display current LLDP configuration.

**/cfg/l2/lldp/port** *<port alias or number>*  
LLDP Port Configuration Menu

[LLDP Port EXT2 Menu]

admstat - Set LLDP admin-status of this port

snmptrap - Enable/disable SNMP trap notification of this port

tlv - Optional TLVs Menu

cur - Show current LLDP port parameters

Use the following commands to configure LLDP port options.

Table 188 LLDP Port Menu Options (/cfg/l2/lldp/port)

Command Syntax and Usage	
<b>admstat disabled tx_only rx_only tx_rx</b>	
	Configures the LLDP transmission type for the port, as follows:
	<ul style="list-style-type: none"><li><input type="checkbox"/> Transmit only</li><li><input type="checkbox"/> Receive only</li><li><input type="checkbox"/> Transmit and receive</li><li><input type="checkbox"/> Disabled</li></ul>
	The default value is tx_rx.
<b>snmptrap e d</b>	
	Enables or disables SNMP trap notification for LLDP messages.

Table 188 LLDP Port Menu Options (/cfg/l2/lldp/port) (continued)

Command Syntax and Usage

**tlv**

Displays the Optional TLV menu for the selected port. To view menu options, see [page 337](#).

**cur**

Display current LLDP configuration.

**/cfg/l2/lldp/port** *<port alias or number>* **/tlv**  
LLDP Optional TLV Configuration Menu

[Optional TLVs Menu]	
portdesc	- Enable/disable Port Description TLV for this port
sysname	- Enable/disable System Name TLV for this port
sysdescr	- Enable/disable System Description TLV for this port
syscap	- Enable/disable System Capabilities TLV for this port
mgmtaddr	- Enable/disable Management Address TLV for this port
portvid	- Enable/disable Port VLAN ID TLV for this port
portprot	- Enable/disable Port and Protocol VLAN ID TLV for this port
vlanname	- Enable/disable VLAN Name TLV for this port
protid	- Enable/disable Protocol Identity TLV for this port
macphy	- Enable/disable MAC/PHY Configuration/Status TLV for this port
powermdi	- Enable/disable Power Via MDI TLV for this port
linkaggr	- Enable/disable Link Aggregation TLV for this port
framesz	- Enable/disable Maximum Frame Size TLV for this port
all	- Enable/disable all the Optional TLVs for this port
cur	- Display current Optional TLVs configuration

Use the following commands to configure LLDP port TLV (Type, Length, Value) options for the selected port.

Table 189 Optional TLV Menu Options (/cfg/l2/lldp/port x/tlv)

Command Syntax and Usage

**portdesc d|e**

Enables or disables the Port Description information type.

**sysname d|e**

Enables or disables the System Name information type.

**sysdescr d|e**

Enables or disables the System Description information type.

**Table 189** Optional TLV Menu Options (/cfg/l2/ldp/port x/tlv) (continued)**Command Syntax and Usage****syscap d|e**

Enables or disables the System Capabilities information type.

**mgmtaddr d|e**

Enables or disables the Management Address information type.

**portvid d|e**

Enables or disables the Port VLAN ID information type.

**portprot d|e**

Enables or disables the Port and VLAN Protocol ID information type.

**vlanname d|e**

Enables or disables the VLAN Name information type.

**protid d|e**

Enables or disables the Protocol ID information type.

**macphy d|e**

Enables or disables the MAC/Phy Configuration information type.

**powermdi d|e**

Enables or disables the Power via MDI information type.

**linkaggr d|e**

Enables or disables the Link Aggregation information type.

**framesz d|e**

Enables or disables the Maximum Frame Size information type.

**all d|e**

Enables or disables all optional TLV information types.

**cur**

Display current Optional TLV configuration.

**/cfg/l2/trunk** *<trunk group number>*  
**Trunk Configuration Menu**

[Trunk group 1 Menu]	
add	- Add port to trunk group
rem	- Remove port from trunk group
ena	- Enable trunk group
dis	- Disable trunk group
del	- Delete trunk group
cur	- Display current Trunk Group configuration

Trunk groups can provide super-bandwidth connections between VFSMs or other trunk capable devices. A *trunk* is a group of ports that act together, combining their bandwidth to create a single, larger port. Up to 18 trunk groups can be configured on the VFSM, with the following restrictions:

- Any physical switch port can belong to no more than one trunk group.
- Up to 8 ports can belong to the same trunk group.
- Configure all ports in a trunk group with the same properties (speed, duplex, flow control, STG, VLAN, and so on).
- Trunking from non-BLADE devices must comply with Cisco® EtherChannel® technology.

By default, each trunk group is empty and disabled.

**Table 190** Trunk Configuration Menu Options (/cfg/l2/trunk)

**Command Syntax and Usage**

**add** *<port alias or number>*

Adds a physical port to the current trunk group.

**rem** *<port alias or number>*

Removes a physical port from the current trunk group.

**ena**

Enables the current trunk group.

**dis**

Disables the current trunk group.

**del**

Removes the current trunk group configuration.

**cur**

Displays current trunk group parameters.



/cfg/l2/thash

## IP Trunk Hash Configuration Menu

[IP Trunk Hash Menu]

l2thash

- L2 Trunk Hash Control

l3thash

- L3 Trunk Hash Control

ingress

- Enable/disable ingress port hash

L4port

- Enable/disble L4 port hash

cur

- Display current Trunk Hash configuration

Use the following commands to configure IP trunk hash settings for the VFSM. Trunk hash parameters are set globally for the VFSM. The trunk hash settings affect both static trunks and LACP trunks.

To achieve the most even traffic distribution, select options that exhibit a wide range of values for your particular network. You may use the configuration settings listed in [Table 191](#) combined with the hash parameters listed in [Table 192](#) and [Table 193](#).

**Table 191** Trunk Hash Settings (/cfg/l2/thash)

---

**Command Syntax and Usage**

---

**l2thash**

Displays the Layer 2 Trunk Hash Settings menu. To view menu options, see [page 341](#).

**l3thash**

Displays the Layer 3 Trunk Hash Settings menu. To view menu options, see [page 342](#).

**ingress e|d**

Enables or disables trunk hash computation based on the ingress port. The default setting is disabled.

**L4port e|d**

Enables or disables use of Layer 4 service ports (TCP, UDP, and so on) to compute the hash value. The default setting is disabled.

**cur**

Display current trunk hash configuration.

---

/cfg/l2/thash/l2thash  
Layer 2 Trunk Hash Menu

```
[L2 Trunk Hash Menu]
  smac      - Enable/disable smac hash
  dmac      - Enable/disable dmac hash
  cur       - Display current trunk hash setting for L2 traffic
```

Layer 2 trunk hash parameters are set globally. You can enable one or both parameters, to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SMAC and DMAC

Use the following commands to configure Layer 2 trunk hash parameters for the switch.

**Table 192** Layer 2 Trunk Hash Options (/cfg/l2/thash/l2thash)

Command Syntax and Usage	
<b>smac enable disable</b>	Enables or disable Layer 2 trunk hashing on the source MAC.
<b>dmac enable disable</b>	Enables or disable Layer 2 trunk hashing on the destination MAC.
<b>cur</b>	Displays current Layer 2 trunk hash settings.

**/cfg/l2/thash/l3thash**  
**Layer 3 Trunk Hash Menu**

```
[L3 Trunk Hash Menu]
  useL2    - Enable/disable L2 hash for IP packet
  sip      - Enable/disable sip hash for IP packet
  dip      - Enable/disable dip hash for IP packet
  cur      - Display current trunk hash setting for L3 traffic
```

Layer 3 trunk hash parameters are set globally. You can enable one or both parameters, to configure any of the following valid combinations:

- SIP (source IP only)
- DIP (destination IP only)
- SIP and DIP

Use the following commands to configure Layer 3 trunk hash parameters for the switch.

**Table 193** Layer 3 Trunk Hash Options (/cfg/l2/thash/l3thash)

**Command Syntax and Usage**

**usel2 enable|disable**

Enables or disables use of Layer 2 hash parameters only. When enabled, Layer 3 hashing parameters are cleared.

**sip enable|disable**

Enables or disables Layer 3 trunk hashing on the source IP address.

**dip enable|disable**

Enables or disables Layer 3 trunk hashing on the destination IP address.

**cur**

Displays current Layer 3 trunk hash settings.

/cfg/l2/lacp  
LACP Configuration Menu

[LACP Menu]	
port	- LACP Port Menu
sysprio	- Set LACP system priority
timeout	- Set LACP system timeout scale for timing out partner info
delete	- Delete an LACP trunk
default	- Restore default LACP system configuration
cur	- Display current LACP configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the VFSM.

Table 194 LACP Menu Options (/cfg/l2/lacp)

Command Syntax and Usage	
port <port alias or number>	Displays the LACP Port menu. To view menu options, see <a href="#">page 344</a> .
sysprio <1-65535>	Defines the priority value (1 through 65535) for the VFSM. Lower numbers provide higher priority. The default value is 32768.
timeout short long	Defines the timeout period before invalidating LACP data from a remote partner. Choose <b>short</b> (3 seconds) or <b>long</b> (90 seconds). The default value is <b>long</b> . <b>Note:</b> It is recommended that you use a timeout value of <b>long</b> , to reduce LACPDU processing. If your VFSM's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP.
delete <1-65535>	Deletes a selected LACP trunk, based on its <i>admin key</i> . This command is equivalent to disabling LACP on each of the ports configured with the same <i>admin key</i> .
default sysprio timeout	Restores the selected parameters to their default values.
cur	Display current LACP configuration.

**/cfg/l2/lacp/port** *<port alias or number>*  
LACP Port Configuration Menu

```
[LACP Port EXT1 Menu]
mode      - Set LACP mode
prio      - Set LACP port priority
adminkey  - Set LACP port admin key
default   - Restore default LACP port configuration
cur       - Display current LACP port configuration
```

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the selected port.

**Table 195** LACP Port Menu Options (/cfg/l2/lacp/port)

---

**Command Syntax and Usage**

---

**mode** **off** | **active** | **passive**

Set the LACP mode for this port, as follows:

- ☐ **off**: Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is **off**.
- ☐ **active**: Turn LACP on and set this port to active. Active ports initiate LACPDUs.
- ☐ **passive**: Turn LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports.

---

**prio** *<1-65535>*

Sets the priority value for the selected port. Lower numbers provide higher priority. The default value is 32768.

---

**adminkey** *<1-65535>*

Set the admin key for this port. Only ports with the same *admin key* and *oper key* (operational state generated internally) can form a LACP trunk group.

---

**default** **adminkey** | **mode** | **prio**

Restores the selected parameters to their default values.

---

**cur**

Displays the current LACP configuration for this port.

---

/cfg/l2/failovr  
Layer 2 Failover Configuration Menu

[Failover Menu]	
trigger	- Trigger Menu
vlan	- Globally turn VLAN Monitor ON/OFF
on	- Globally turn Failover ON
off	- Globally turn Failover OFF
cur	- Display current Failover configuration

Use this menu to configure Layer 2 Failover. For more information about Layer 2 Failover, see “High Availability” in the *BLADEOS Application Guide*.

Table 196 Layer 2 Failover Menu Options (/cfg/l2/failovr)

Command Syntax and Usage

**trigger** <1-8>

Displays the Failover Trigger menu. To view menu options, see [page 346](#).

**vlan on|off**

Globally turns VLAN monitor **on** or **off**. When the VLAN Monitor is **on**, the switch automatically disables only internal ports that belong to the same VLAN as ports in the failover trigger. The default value is **off**.

**on**

Globally turns Layer 2 Failover **on**.

**off**

Globally turns Layer 2 Failover **off**.

**cur**

Displays current Layer 2 Failover parameters.

`/cfg/l2/failovr/trigger </-8>`  
Failover Trigger Configuration Menu

[Trigger 1 Menu]	
amon	- Auto Monitor Menu
mmon	- Manual Monitor Menu
limit	- Limit of Trigger
ena	- Enable Trigger
dis	- Disable Trigger
del	- Delete Trigger
cur	- Display current Trigger configuration

**Table 197** Failover Trigger Menu Options (/cfg/l2/failovr/trigger)

**Command Syntax and Usage**

**amon**

Displays the Auto Monitor menu for the selected trigger. To view menu options, see [page 347](#).

**mmon**

Displays the Manual Monitor menu for the selected trigger. To view menu options, see [page 348](#).

**limit** *<0-1024>*

Configures the minimum number of operational links allowed within each trigger before the trigger initiates a failover event. If you enter a value of zero (0), the switch triggers a failover event only when no links in the trigger are operational.

**ena**

Enables the selected trigger.

**dis**

Disables the selected trigger.

**del**

Deletes the selected trigger.

**cur**

Displays the current failover trigger settings.

**/cfg/l2/failovr/trigger <l-8>/amon**  
*Auto Monitor Configuration Menu*

[Auto Monitor Menu]

- addtrnk - Add trunk to Auto Monitor
- remtrnk - Remove trunk from Auto Monitor
- addkey - Add LACP port adminkey to Auto Monitor
- remkey - Remove LACP port adminkey from Auto Monitor
- cur - Display current Auto Monitor configuration

**Table 198** Auto Monitor Menu Options (/cfg/l2/failovr/trigger/amon)

**Command Syntax and Usage**

**addtrnk** <trunk group number>

Adds a trunk group to the Auto Monitor.

**remtrnk** <trunk group number>

Removes a trunk group from the Auto Monitor.

**addkey** <l-65535>

Adds an LACP *admin key* to the Auto Monitor. LACP trunks formed with this *admin key* will be included in the Auto Monitor.

**remkey** <l-65535>

Removes an LACP admin key from the Auto Monitor.

**cur**

Displays the current Auto Monitor settings.



**/cfg/l2/failovr/trigger </-8>/mmon**  
*Manual Monitor Configuration Menu*

```
[Manual Monitor Menu]
  monitor - Monitor Menu
  control - Control Menu
  cur      - Display current Manual Monitor configuration
```

Use this menu to configure Failover Manual Monitor. These menus allow you to manually define both the monitor and control ports that participate in failover teaming.

---

**Note** – AMON and MMON configurations are mutually exclusive.

---

**Table 6-1** Failover Manual Monitor options (/cfg/l2/failovr/trigger/mmon)

---

**Command Syntax and Usage**

---

**monitor**

Displays the Manual Monitor - Monitor menu for the selected trigger.

---

**control**

Displays the Manual Monitor - Control menu for the selected trigger.

---

**cur**

Displays the current Manual Monitor settings.

---

*/cfg/l2/failovr/trigger <1-8>/mmon/monitor*  
*Manual Monitor Port Configuration Menu*

[Monitor Menu]

addport

-

Add port to Monitor

remport

-

Remove port from Monitor

addtrnk

-

Add trunk to Monitor

remtrnk

-

Remove trunk from Monitor

addkey

-

Add LACP port adminkey to Monitor

remkey

-

Remove LACP port adminkey from Monitor

cur

-

Display current Monitor configuration

Use this menu to define the port link(s) to monitor. The Manual Monitor Port configuration accepts only external uplink ports.

**Table 199** Failover Manual Monitor Port Options  
(/cfg/l2/failovr/trigger/mmon/monitor)

**Command Syntax and Usage**

**addport** *<port alias or number>*

Adds the selected port to the Manual Monitor Port configuration.

**remport** *<port alias or number>*

Removes the selected port from the Manual Monitor Port configuration.

**addtrnk** *<trunk number>*

Adds a trunk group to the Manual Monitor Port configuration.

**remtrnk** *<trunk number>*

Removes a trunk group from the Manual Monitor Port configuration.

**addkey** *<1-65535>*

Adds an LACP *admin key* to the Manual Monitor Port configuration. LACP trunks formed with this *admin key* will be included in the Manual Monitor Port configuration.

**remkey** *<1-65535>*

Removes an LACP admin key from the Manual Monitor Port configuration.

**cur**

Displays the current Manual Monitor Port configuration.

**/cfg/l2/failovr/trigger <1-8>/mmon/control**  
*Manual Monitor Control Configuration Menu*

[Control Menu]

addport

- Add port to Control

remport

- Remove port from Control

addtrnk

- Add trunk to Control

remtrnk

- Remove trunk from Control

addkey

- Add LACP port adminkey to Control

remkey

- Remove LACP port adminkey from Control

cur

- Display current Control configuration

Use this menu to define the port link(s) to control. The Manual Monitor Control configuration accepts internal and external ports, but not management ports.

**Table 200** Failover Manual Monitor Control Options  
(/cfg/l2/failovr/trigger/mmon/control)

**Command Syntax and Usage**

**addport** <port alias or number>

Adds the selected port to the Manual Monitor Control configuration.

**remport** <port alias or number>

Removes the selected port from the Manual Monitor Control configuration.

**addtrnk** <trunk number>

Adds a trunk group to the Manual Monitor Control configuration.

**remtrnk** <trunk number>

Removes a trunk group from the Manual Monitor Control configuration.

**addkey** <1-65535>

Adds an LACP *admin key* to the Manual Monitor Control configuration. LACP trunks formed with this *admin key* will be included in the Manual Monitor Control configuration.

**remkey** <1-65535>

Removes an LACP *admin key* from the Manual Monitor Control configuration.

**cur**

Displays the current Manual Monitor Control configuration.

/cfg/l2/hotlink  
Hot Links Configuration Menu

[Hot Links Menu]	
trigger	- Trigger Menu
bpdu	- Enable/disable BPDU flood
sndfdb	- Enable/disable FDB update
on	- Globally turn Hot Links ON
off	- Globally turn Hot Links OFF
cur	- Display current Hot Links configuration

Table 201 describes the Hot Links menu options.

Table 201 Hot Links Menu Options (/cfg/l2/hotlink)

Command Syntax and Usage

**trigger** <1-200>

Displays the Hot Links Trigger menu. To view menu options, see [page 352](#).

**bpdu enable|disable**

Enables or disables the ability to flood BPDUs on the active Hot Links interface when the interface belongs to a Spanning Tree group that is globally turned `off`.

The default setting is `disabled`.

**sndfdb enable|disable**

Enables or disables FDB Update, which allows the switch to send FDB and MAC update packets over the active interface.

The default setting is `disabled`.

**on**

Globally turns Hot Links `on`. The default value is `off`.

**off**

Globally turns Hot Links `off`.

**cur**

Displays current Hot Links configuration.

`/cfg/l2/hotlink/trigger <1-200>`  
Hot Links Trigger Configuration Menu

```
[Trigger 2 Menu]
  master    - Master Menu
  backup    - Backup Menu
  fdelay    - Set Forward Delay (secs)
  name      - Set Trigger Name
  preempt   - Enable/disable Preemption
  ena       - Enable Trigger
  dis       - Disable Trigger
  del       - Delete Trigger
  cur       - Display current Trigger configuration
```

**Table 202** Hot Links Trigger Menu Options (/cfg/l2/hotlink/trigger)

**Command Syntax and Usage**

**master**

Displays the Master interface menu for the selected trigger. To view menu options, see [page 353](#).

**backup**

Displays the Backup interface menu for the selected trigger. To view menu options, see [page 354](#).

**fdelay <0-3600>**

Configures the Forward Delay interval, in seconds. The default value is 1.

**name <1-32 characters>**

Configures a name for the trigger.

**preempt e|d**

Enables or disables pre-emption, which allows the Master interface to transition to the Active state whenever it becomes available.

The default setting is *enabled*.

**ena**

Enables the Hot Links trigger.

**dis**

Disables the Hot Links trigger.

**Table 202** Hot Links Trigger Menu Options (/cfg/l2/hotlink/trigger) (continued)

**Command Syntax and Usage**

**del**

Deletes the Hot Links trigger.

**cur**

Displays the current Hot Links Trigger configuration.

**/cfg/l2/hotlink/trigger <1-200>/master**  
Hot Links Trigger Master Configuration Menu

[Master Menu]  
port - Set port in Master  
trunk - Set trunk in Master  
adminkey - Set adminkey in Master  
cur - Display current Master configuration

**Table 203** Hot Links Trigger Master menu (/cfg/l2/hotlink/trigger/master)

**Command Syntax and Usage**

**port** <port alias or number>

Adds the selected port to the Master interface. Enter 0 (zero) to clear the port.

**trunk** <trunk number> | 0

Adds the selected trunk group to the Master interface. Enter 0 (zero) to clear the trunk group.

**adminkey** <0-65535>

Adds an LACP *admin key* to the Master interface. LACP trunks formed with this *admin key* will be included in the Master interface. Enter 0 (zero) to clear the *admin key*.

**cur**

Displays the current Hot Links Master interface configuration.

**/cfg/l2/hotlink/trigger <1-200>/backup**  
Hot Links Trigger Backup Configuration Menu

[Backup Menu]

- port - Set port in Backup
- trunk - Set trunk in Backup
- adminkey - Set adminkey in Backup
- cur - Display current Backup configuration

**Table 204** Hot Links Trigger Backup menu (/cfg/l2/hotlink/trigger/backup)

**Command Syntax and Usage**

**port** <port alias or number>

Adds the selected port to the Backup interface. Enter 0 (zero) to clear the port.

**trunk** <trunk number> | 0

Adds the selected trunk to the Backup interface. Enter 0 (zero) to clear the trunk group.

**adminkey** <0-65535>

Adds an LACP *admin key* to the Backup interface. LACP trunks formed with this *admin key* will be included in the Backup interface. Enter 0 (zero) to clear the *admin key*.

**cur**

Displays the current Hot Links Backup interface settings.

`/cfg/l2/vlan` *<VLAN number>*  
VLAN Configuration Menu

[VLAN 1 Menu]	
pvlan	- Protocol VLAN Menu
privlan	- Private-VLAN Menu
name	- Set VLAN name
stg	- Assign VLAN to a Spanning Tree Group
vmap	- Set VMAP for this vlan
add	- Add port to VLAN
rem	- Remove port from VLAN
def	- Define VLAN as list of ports
mgmt	- Enable/Disable this VLAN as additional management VLAN
ena	- Enable VLAN
dis	- Disable VLAN
del	- Delete VLAN
cur	- Display current VLAN configuration

The commands in this menu configure VLAN attributes, change the status of each VLAN, change the port membership of each VLAN, and delete VLANs.

By default, VLAN 1 is the only VLAN configured on the switch. Internal server ports and external uplink ports are members of VLAN 1 by default. Up to 1024 VLANs can be configured on the VFSM.

VLANs can be assigned any number between 1 and 4094. VLAN 4095 is reserved for switch management.

**Table 205** VLAN Configuration Menu Options (`/cfg/l2/vlan`)

Command Syntax and Usage

**pvlan** *<1-8>*

Displays the Protocol-based VLAN menu. To view menu options, see [page 357](#).

**privlan**

Displays the Private VLAN menu. To view menu options, see [page 359](#).

**name**

Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one.

**stg** *<Spanning Tree Group index>*

Assigns a VLAN to a Spanning Tree Group.



**Table 205** VLAN Configuration Menu Options (/cfg/l2/vlan) (continued)

**Command Syntax and Usage**

**vmap** {**add**|**rem**} <1-128> [**extports**|**intports**]

Adds or removes a VLAN Map to the VLAN membership. You can choose to limit operation of the VLAN Map to internal ports only or external ports only. If you do not select a port type, the VMAP is applied to the entire VLAN.

**add** <port alias or number>

Adds port(s) to the VLAN membership.

**rem** <port alias or number>

Removes port(s) from this VLAN.

**def** <list of port numbers>

Defines which ports are members of this VLAN. Every port must be a member of at least one VLAN. By default, internal server ports (INTx) and external ports (EXTx) are in VLAN 1.

**mgmt enable|disable**

Configures this VLAN as a management VLAN. You must add the management ports (MGT1 and MGT2) to each new management VLAN. External ports cannot be added to management VLANs.

**ena**

Enables this VLAN.

**dis**

Disables this VLAN without removing it from the configuration.

**del**

Deletes this VLAN.

**cur**

Displays the current VLAN configuration.

**Note** – All ports must belong to at least one VLAN. Any port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN 1. You cannot remove a port from VLAN 1 if the port has no membership in any other VLAN. Also, you cannot add a port to more than one VLAN unless the port has VLAN tagging turned on (see the `tag` command on [page 282](#)).

## `/cfg/l2/vlan/pvlan` *<protocol number>* Protocol-Based VLAN Configuration Menu

```
[VLAN 1 Protocol 1 Menu]
  pty      - Set protocol type
  protocol - Select a predefined protocol
  prio     - Set priority to protocol
  add      - Add port to PVLAN
  rem      - Remove port from PVLAN
  ports    - Add/Remove a list of ports to/from PVLAN
  tagpvl   - Enable/Disable port tagging for PVLAN
  taglist  - Enable tagging a port list for PVLAN
  ena      - Enable protocol
  dis      - Disable protocol
  del      - Delete protocol
  cur      - Display current PVLAN configuration
```

Use this menu to configure Protocol-based VLAN (PVLAN) for the selected VLAN.

**Table 206** PVLAN Menu Options (`/cfg/l2/vlan/pvlan`)

---

### Command Syntax and Usage

---

**pty** *<(Ether2|SNAP|LLC)>* *<Ethernet type>*

Configures the frame type and the Ethernet type for the selected protocol. Ethernet type consists of a 4-digit (16 bit) hex code, such as 0080 (IPv4).

---

**protocol** *<Protocol type>*

Selects a pre-defined protocol, as follows:

- ☐ decEther2: DEC Local Area Transport
  - ☐ ipv4Ether2: Internet IP (IPv4)
  - ☐ ipv6Ether2: IPv6
  - ☐ ipx802.2: Novell IPX 802.2
  - ☐ ipx802.3: Novell IPX 802.3
  - ☐ ipxEther2: Novell IPX
  - ☐ ipxSnap: Novell IPX SNAP
  - ☐ netbios: NetBIOS 802.2
  - ☐ rarpEther2: Reverse ARP
  - ☐ sna802.2: SNA 802.2
  - ☐ snaEther2: IBM SNA Service on Ethernet
  - ☐ vinesEther2: Banyan VINES
  - ☐ xnsEther2: XNS Compatibility
-

**Table 206** PVLAN Menu Options (/cfg/l2/vlan/pvlan) (continued)**Command Syntax and Usage****prio** <0-7>

Configures the priority value for this PVLAN.

**add** <port alias or number>

Adds a port to the selected PVLAN.

**rem** <port alias or number>

Removes a port from the selected PVLAN.

**ports** <port alias or number; or a list or range of ports>

Defines a list of ports that belong to the selected protocol on this VLAN. Enter 0 (zero) to remove all ports.

**tagpvl enable | disable**

Enables or disables port tagging on this PVLAN.

**taglist** {<port alias or number; or a list or range of ports> | **empty**}Defines a list of ports that will be tagged by the selected protocol on this VLAN. Enter **empty** to disable tagging on all ports by this PVLAN.**ena**

Enables the selected protocol on the VLAN.

**dis**

Disables the selected protocol on the VLAN.

**del**

Deletes the selected protocol configuration from the VLAN.

**cur**

Displays current parameters for the selected PVLAN.

/cfg/l2/vlan/privlan  
Private VLAN Configuration Menu

[privlan Menu]	
type	- Set Private-VLAN type
map	- Associate secondary VLAN with a primary VLAN
ena	- Enable Private-VLAN
dis	- Disable Private-VLAN
cur	- Display current Private-VLAN configuration

Use this menu to configure a Private VLAN.

Table 207 Private VLAN Menu Options (/cfg/l2/vlan/privlan)

Command Syntax and Usage

**type {none|primary|isolated|community}**

Defines the VLAN type, as follows:

- ☐ none: Clears the Private VLAN type.
- ☐ primary: A Private VLAN must have only one primary VLAN. The primary VLAN carries unidirectional traffic to ports on the isolated VLAN or to community VLAN.
- ☐ isolated: The isolated VLAN carries unidirectional traffic from host ports. A Private VLAN may have only one isolated VLAN.
- ☐ community: Community VLANs carry upstream traffic from host ports. A Private VLAN may have multiple community VLANs.

**map <2-4094> | none**

Configures Private VLAN mapping between a secondary VLAN (isolated or community) and a primary VLAN. Enter the primary VLAN ID.

**ena**

Enables the Private VLAN.

**dis**

Disables the Private VLAN.

**cur**

Displays current parameters for the selected Private VLAN.

/cfg/13

# Layer 3 Configuration Menu

[Layer 3 Menu]	
if	- Interface Menu
gw	- Default Gateway Menu
route	- Static Route Menu
mroute	- Static IP Multicast Route Menu
arp	- ARP Menu
frwd	- Forwarding Menu
nwf	- Network Filters Menu
rmap	- Route Map Menu
rip	- Routing Information Protocol Menu
ospf	- Open Shortest Path First (OSPF) Menu
bgp	- Border Gateway Protocol Menu
igmp	- IGMP Menu
dns	- Domain Name System Menu
bootp	- Bootstrap Protocol Relay Menu
vrrp	- Virtual Router Redundancy Protocol Menu
gw6	- IP6 Default Gateway Menu
route6	- Static IP6 Route Menu
nbrcache	- IP6 Static Neighbor Cache Menu
ospf3	- Open Shortest Path First v3 (OSPFv3) Menu
loopif	- Loopback Interface Menu
rtrid	- Set router ID
cur	- Display current IP configuration

Table 208 Layer 3 Configuration Menu (/cfg/l3)

Command Syntax and Usage

**if** <interface number (1-128)>

Displays the IP Interface Menu. To view menu options, see [page 363](#).

**gw** <default gateway number (1-132)>

Displays the IP Default Gateway Menu. To view menu options, see [page 367](#).

**route**

Displays the IP Static Route Menu. To view menu options, see [page 368](#).

**mroute**

Displays the Static IP Multicast Route Menu. To view menu options, see [page 370](#).

**arp**

Displays the Address Resolution Protocol Menu. To view menu options, see [page 372](#).

**Table 208** Layer 3 Configuration Menu (/cfg/l3) (continued)**Command Syntax and Usage****frwd**

Displays the IP Forwarding Menu. To view menu options, see [page 374](#).

**nwf** *<network filter number (1-256)>*

Displays the Network Filter Configuration Menu. To view menu options see [page 375](#).

**rmap** *<route map number (1-32)>*

Displays the Route Map Menu. To view menu options see [page 376](#).

**rip**

Displays the Routing Interface Protocol Menu. To view menu options, see [page 380](#).

**ospf**

Displays the OSPF Menu. To view menu options, see [page 384](#).

**bgrp**

Displays the Border Gateway Protocol Menu. To view menu options, see [page 395](#).

**igmp**

Displays the IGMP Menu. To view menu options, see [page 402](#).

**dns**

Displays the IP Domain Name System Menu. To view menu options, see [page 413](#).

**bootp**

Displays the Bootstrap Protocol Menu. To view menu options, see [page 415](#).

**vrrp**

Displays the Virtual Router Redundancy Configuration Menu. To view menu options, see [page 416](#).

**gw6** *<gateway number (1, 132)>*

Displays the IPv6 Gateway Configuration Menu. To view menu options, see [page 427](#).

**route6**

Displays the IPv6 Routing Configuration Menu. To view menu options, see [page 428](#).

**Table 208** Layer 3 Configuration Menu (/cfg/l3) (continued)

---

**Command Syntax and Usage**

---

**nbrcache**

Displays the IPv6 Neighbor Discovery Cache Configuration Menu. To view menu options, see [page 429](#).

---

**ospf3**

Displays the OSPFv3 Configuration Menu. To view menu options, see [page 430](#).

---

**loopif**

Displays the IP Loopback Interface Menu. To view menu options, see [page 444](#).

---

**rtrid** *<IP address (such as, 192.4.17.101)>*

Sets the router ID.

---

**cur**

Displays the current IP configuration.

---

**/cfg/l3/if** *<interface number>*  
**IP Interface Configuration Menu**

[IP Interface 1 Menu]	
ip6nd	- IP6 Neighbor Discovery Menu
addr	- Set IP address
secaddr6	- Set Secondary IPv6 address on IPv6 interface
maskplen	- Set subnet mask/prefix len
vlan	- Set VLAN number
relay	- Enable/disable BOOTP relay
ip6host	- Enable/disable IPv6 host mode
ena	- Enable IP interface
dis	- Disable IP interface
del	- Delete IP interface
cur	- Display current interface configuration

The VFSM can be configured with up to 128 IP interfaces. Each IP interface represents the VFSM on an IP subnet on your network. The Interface option is disabled by default.

**Note –** Interface 128 is reserved for switch management. If the IPv6 feature is enabled, interface 127 is also reserved. To maintain connectivity between the management module and the VFSM, use the management module interface to change the IP address of the switch.

**Table 209** IP Interface Menu Options (/cfg/l3/if)

**Command Syntax and Usage**

**ip6nd**

Displays the IPv6 Neighbor Discovery menu. To view menu options, see [page 365](#).

**addr** *<IPv4 address (such as 192.4.17.101)>*

**IPv4:** Configures the IPv4 address of the switch interface, using dotted decimal notation.

**addr** *<IPv6 address (such as 3001:0:0:0:0:abcd:12)>* [**anycast**]

**IPv6:** Configures the IPv6 address of the switch interface, using hexadecimal format with colons.

**secaddr6** *<IPv6 address (such as 3001:0:0:0:0:abcd:12)>*|*<prefix length>* [**anycast**]

Configures the secondary IPv6 address of the switch interface, using hexadecimal format with colons.



Table 209 IP Interface Menu Options (/cfg/l3/if) (continued)

Command Syntax and Usage	
<b>maskplen</b> <IPv4 subnet mask (such as 255.255.255.0)>	
IPv4: Configures the IPv4 subnet address mask for the interface, using dotted decimal notation.	
<b>maskplen</b> <IPv6 prefix length (1-128)>	
IPv6: Configures the subnet IPv6 prefix length. The default value is 0 (zero).	
<b>vlan</b> <VLAN number>	
Configures the VLAN number for this interface. Each interface can belong to only one VLAN.	
IPv4: Each VLAN can contain multiple IPv4 interfaces.	
IPv6: Each VLAN can contain only one IPv6 interface.	
<b>relay disable   enable</b>	
Enables or disables the BOOTP relay on this interface. It is enabled by default.	
<b>ip6host enable   disable</b>	
Enables or disables the IPv6 Host Mode on this interface. The default value is disabled for data interfaces, and enabled for the management interface.	
<b>ena</b>	
Enables this IP interface.	
<b>dis</b>	
Disables this IP interface.	
<b>del</b>	
Removes this IP interface.	
<b>cur</b>	
Displays the current interface settings.	

/cfg/l3/if <interface number>/ip6nd  
IPv6 Neighbor Discovery Configuration Menu

[IP6 Neighbor Discovery Menu]	
rtradv	- Enable/disable router advertisement
managed	- Enable/disable Managed config flag
othercfg	- Enable/disable Other config flag
ralife	- Set Router Advertisement lifetime
dad	- Set number of duplicate address detection attempts
reachtm	- Set advertised reachability time
advint	- Set Router Advertisement maximum interval
advmint	- Set Router Advertisement minimum interval
retimer	- Set Router Advertisement Retrans Timer
hoplmt	- Set Router Advertisement Hop Limit
cur	- Display current Neighbor Discovery configuration

Table 210 describes the IPv6 Neighbor Discovery configuration options.

Table 210 IPv6 Neighbor Discovery Menu Options (/cfg/l3/if/ip6nd)

Command Syntax and Usage

rtradv e|d

Enables or disables IPv6 Router Advertisements on the interface. The default value is disabled.

managed e|d

Enables or disables the *managed address configuration* flag of the interface. When enabled, the host IP address can be set automatically through DHCP. The default value is disabled.

othercfg e|d

Enables or disables the *other stateful configuration* flag, which allows the interface to use DHCP for other stateful configuration. The default value is disabled.

ralife <0-9000>

Configures the IPv6 Router Advertisement lifetime interval. The RA lifetime interval must be greater than or equal to the RA maximum interval (advint), or 0 (zero).  
  
The default value is 1800 seconds.

dad <1-10>

Configures the maximum number of duplicate address detection attempts. The default value is 1.

**Table 210** IPv6 Neighbor Discovery Menu Options (/cfg/l3/if/ip6nd) (continued)

**Command Syntax and Usage**

---

**reachtm** <1-3600>

Configures the advertised reachability time, in seconds. The default value is 30 seconds.

---

**advint** <4-1800>

Configures the Router Advertisement maximum interval. The default value is 600 seconds.

**Note:** Set the maximum RA interval to a value greater than or equal to 4/3 of the minimum RA interval.

---

**advmint** <4-1800>

Configures the Router Advertisement minimum interval. The default value is 198 seconds.

**Note:** Set the minimum RA interval to a value less than or equal to 0.75 of the maximum RA interval.

---

**retimer** <1-3600>

Configures the Router Advertisement re-transmit timer, in seconds. The default value is 1 second.

---

**hoplmt** <1-255>

Configures the Router Advertisement hop limit. The default value is 64.

---

**cur**

Displays the current Neighbor Discovery parameters.

---

`/cfg/l3/gw` *<gateway number>*  
**Default Gateway Configuration Menu**

[Default gateway 1 Menu]	
addr	- Set IP address
intr	- Set interval between ping attempts
retry	- Set number of failed attempts to declare gateway DOWN
arp	- Enable/disable ARP only health checks
ena	- Enable default gateway
dis	- Disable default gateway
del	- Delete default gateway
cur	- Display current default gateway configuration

The switch can be configured with up to 132 IPv4 gateways. Gateway 132 is reserved for switch management.

This option is disabled by default.

**Table 211** Default Gateway Menu Options (`/cfg/l3/gw`)

<b>Command Syntax and Usage</b>	
<b>addr</b> <i>&lt;default gateway address (such as, 192.4.17.44)&gt;</i>	Configures the IP address of the default IP gateway using dotted decimal notation.
<b>intr</b> <i>&lt;0-60 seconds&gt;</i>	The switch pings the default gateway to verify that it's up. The <code>intr</code> option sets the time between health checks. The range is from 0 to 60 seconds. The default is 2 seconds.
<b>retry</b> <i>&lt;number of attempts (1-120)&gt;</i>	Sets the number of failed health check attempts required before declaring this default gateway inoperative. The range is from 1 to 120 attempts. The default is 8 attempts.
<b>arp disable   enable</b>	Enables or disables Address Resolution Protocol (ARP) health checks. The default value is <b>disabled</b> . The <b>arp</b> option does not apply to management gateways.
<b>ena</b>	Enables the gateway for use.
<b>dis</b>	Disables the gateway.

Table 211 Default Gateway Menu Options (/cfg/l3/gw) (continued)

Command Syntax and Usage	
<b>del</b>	Deletes the gateway from the configuration.
<b>cur</b>	Displays the current gateway settings.

/cfg/l3/route  
IPv4 Static Route Configuration Menu

[IP Static Route Menu]	
add	- Add static route
rem	- Remove static route
clear	- Clear static routes
interval	- Change ECMP route health check ping interval
retries	- Change the number of retries for ECMP health check
ecmhash	- Choose ECMP hash mechanism sip/dipsip
cur	- Display current static routes

Up to 128 IPv4 static routes can be configured.

Table 212 IP Static Route Configuration Menu Options (cfg/l3/route)

Command Syntax and Usage	
<b>add</b> <destination> <mask> <gateway> [<interface number>]	Adds a static route. You will be prompted to enter a destination IP address, destination subnet mask, and gateway address. Enter all addresses using dotted decimal notation.  <b>Note:</b> You may add multiple routes with the same IP address, but with different gateways. These routes become Equal Cost Multipath (ECMP) routes. The maximum number of gateways for each destination is five (5).
<b>rem</b> <destination> <mask> [<interface number>]	Removes a static route. The destination address of the route to remove must be specified using dotted decimal notation.  <b>Note:</b> The gateway IP address is optional. Include the gateway when you remove an ECMP route. If you do not include the gateway, then all ECMP paths for the route are deleted.

Table 212 IP Static Route Configuration Menu Options (cfg/l3/route)

Command Syntax and Usage

**clear** *<destination IP address> | <gateway IP address> | all* *<value>*

Clears the selected IPv4 static routes.

**Note:** Use the gateway IP address to clear a single gateway for an ECMP route.

**interval** *<1-60>*

Configures the ping interval for ECMP health checks, in seconds. The default value is one second.

**retries** *<1-60>*

Configures the number of health check retries allowed before the switch declares that the gateway is down. The default value is 3.

**ecmphash** [**sip**] [**dipsip**]

Configures ECMP route hashing parameters. You may choose one of the following parameters:

- ☐ sip: Source IP address
- ☐ dipsip: Destination IP address and source IP address

**cur**

Displays the current IPv4 static routes.

/cfg/13/mroute  
IP Multicast Route Configuration Menu

[IPMC Static Route Menu]

addport

- Add static IP Multicast route for port

remport

- Remove static IP Multicast route for port

addtrnk

- Add static IP Multicast route for trunk

remtrnk

- Remove static IP Multicast route for trunk

addkey

- Add static IP Multicast route for Lacp adminkey

remkey

- Remove static IP Multicast route or Lacp adminkey

cur

- Display current static IPMC route configuration

The following table describes the IP Multicast (IPMC) route menu options. Before you can add an IPMC route, IGMP must be turned on (/cfg/13/igmp on), and IGMP Relay must be enabled (/cfg/13/igmp/relay ena).

Table 213 IPMC Route Configuration Options

Command Syntax and Usage

**addport** <IPMC destination> <VLAN number> <port alias or number>  
**primary|backup|host** <virtual router ID> | **none**

Adds a static multicast route. You will be prompted to enter a destination IP address (in dotted decimal notation), VLAN, and member port. Indicate whether the route is used for a primary, backup, or host multicast router.

**remport** <IPMC destination> <VLAN number> <port alias or number>  
**primary|backup|host** <virtual router ID> | **none**

Removes a static multicast route. The destination address, VLAN, and member port of the route to remove must be specified.

**addtrnk** <IPMC destination> <VLAN number> <trunk group number>  
**primary|backup|host** <virtual router ID> | **none**

Adds a static multicast route. You will be prompted to enter a destination IP address (in dotted decimal notation), VLAN, and member trunk group. Indicate whether the route is used for a primary, backup, or host multicast router.

**remtrnk** <IPMC destination> <VLAN number> <trunk group number>  
**primary|backup|host** <virtual router ID> | **none**

Removes a static multicast route. The destination address, VLAN, and member trunk group of the route to remove must be specified.

Table 213 IPMC Route Configuration Options

Command Syntax and Usage	
<b>addkey</b> <IPMC destination> <VLAN number> <LACP adminkey> <b>primary</b>   <b>backup</b>   <b>host</b> <virtual router ID>   <b>none</b>	Adds a static multicast route. You will be prompted to enter a destination IP address (in dotted decimal notation), VLAN, and LACP adminkey. Indicate whether the route is used for a primary, backup, or host multicast router.
<b>remkey</b> <IPMC destination> <VLAN number> <LACP adminkey> <b>primary</b>   <b>backup</b>   <b>host</b> <virtual router ID>   <b>none</b>	Removes a static multicast route. The destination address, VLAN, and LACP adminkey of the route to remove must be specified.
<b>cur</b>	Displays the current IP multicast routes.



/cfg/l3/arp

## ARP Configuration Menu

Address Resolution Protocol (ARP) is the TCP/IP protocol that resides within the Internet layer. ARP resolves a physical address from an IP address. ARP queries machines on the local network for their physical addresses. ARP also maintains IP to physical address pairs in its cache memory. In any IP communication, the ARP cache is consulted to see if the IP address of the computer or the router is present in the ARP cache. Then the corresponding physical address is used to send a packet.

[ARP Menu]	
static	- Static ARP Menu
rearp	- Set re-ARP period in minutes
cur	- Display current ARP configuration

**Table 214** ARP Configuration Menu Options (/cfg/l3/arp)

---

**Command Syntax and Usage**

---

**static**

Displays Static ARP menu. To view options, see [page 373](#).

---

**rearp** <2-120 minutes>

Defines re-ARP period in minutes. You can set this duration between two and 120 minutes.

---

**cur**

Displays the current ARP configurations.

---

**/cfg/l3/arp/static**  
**ARP Static Configuration Menu**

Static ARP entries are permanent in the ARP cache and do not age out like the ARP entries that are learned dynamically. Static ARP entries enable the switch to reach the hosts without sending an ARP broadcast request to the network. Static ARPs are also useful to communicate with devices that do not respond to ARP requests. Static ARPs can also be configured on some gateways as a protection against malicious ARP Cache corruption and possible DOS attacks.

[Static ARP Menu]	
add	- Add a permanent ARP entry
del	- Delete an ARP entry
clear	- Clear static ARP entries
cur	- Display current static ARP configuration

**Table 215** ARP Static Configuration Menu Options (/cfg/l3/arp/static)

<b>Command Syntax and Usage</b>	
<b>add</b> <IP address> <MAC address> <VLAN number> <port number>	
Adds a permanent ARP entry.	
<b>del</b> <IP address (such as, 192.4.17.101)>	
Deletes a permanent ARP entry.	
<b>clear</b> [all if <interface number> vlan <VLAN number> port <port number>]	
Clears static ARP entries.	
<b>cur</b>	
Displays current static ARP configuration.	

/cfg/l3/frwd

## IP Forwarding Configuration Menu

[IP Forwarding Menu]	
dirbr	- Enable or disable forwarding directed broadcasts
noicmprd	- Enable/disable No ICMP Redirects
on	- Globally turn IP Forwarding ON
off	- Globally turn IP Forwarding OFF
cur	- Display current IP Forwarding configuration

**Table 216** IP Forwarding Configuration Menu Options (/cfg/l3/frwd)

---

**Command Syntax and Usage**

---

**dirbr disable|enable**

Enables or disables forwarding directed broadcasts. The default setting is disabled.

---

**noicmprd disable|enable**

Enables or disables ICMP re-directs. The default setting is disabled.

---

**on**

Enables IP forwarding (routing) on the VFSM. Forwarding is turned on by default.

---

**off**

Disables IP forwarding (routing) on the VFSM.

---

**cur**

Displays the current IP forwarding settings.

---

/cfg/l3/nwf <1-256>  
Network Filter Configuration Menu

[IP Network Filter 1 Menu]	
addr	- IP Address
mask	- IP network filter mask
enable	- Enable Network Filter
disable	- Disable Network Filter
delete	- Delete Network Filter
cur	- Display current Network Filter configuration

Table 217 IP Network Filter Menu Options (/cfg/l3/nwf)

Command Syntax and Usage

**addr** <IP address, such as 192.4.17.44>

Sets the IP address that will be accepted by the peer when the filter is enabled. If used with the mask option, a range of IP addresses is accepted. The default address is 0.0.0.0

For Border Gateway Protocol (BGP), assign the network filter to an access-list in a route map, then assign the route map to the peer.

**mask** <IP network filter mask>

Sets the network filter mask that is used with addr. The default value is 0.0.0.0

For Border Gateway Protocol (BGP), assign the network filter to a route map, then assign the route map to the peer.

**enable**

Enables the Network Filter configuration.

**disable**

Disables the Network Filter configuration.

**delete**

Deletes the Network Filter configuration.

**cur**

Displays the current the Network Filter configuration.

`/cfg/l3/rmap` *<route map number>*  
**Routing Map Configuration Menu**

**Note** – The *map number* (1-32) represents the routing map you wish to configure.

[IP Route Map 1 Menu]	
alist	- Access List number
aspath	- AS Filter Menu
ap	- Set as-path prepend of the matched route
lp	- Set local-preference of the matched route
metric	- Set metric of the matched route
type	- Set OSPF metric-type of the matched route
prec	- Set the precedence of this route map
weight	- Set weight of the matched route
enable	- Enable route map
disable	- Disable route map
delete	- Delete route map
cur	- Display current route map configuration

Routing maps control and modify routing information.

**Table 218** Routing Map Menu Options (`/cfg/l3/rmap`)

**Command Syntax and Usage**

**alist** *<number 1-8>*

Displays the Access List menu. For more information, see [page 378](#).

**aspath** *<number 1-8>*

Displays the Autonomous System (AS) Filter menu. For more information, see [page 379](#).

**ap** *<AS number>* [*<AS number>*] [*<AS number>*] | **none**

Sets the AS path preference of the matched route. You can configure up to three path preferences.

**lp** *<(0-4294967294)>* | **none**

Sets the local preference of the matched route, which affects both inbound and outbound directions. The path with the higher preference is preferred.

**metric** *<(1-4294967294)>* | **none**

Sets the metric of the matched route.

**Table 218** Routing Map Menu Options (/cfg/l3/rmap) (continued)

Command Syntax and Usage	
<b>type</b> <value (1   2)>   none	
Assigns the type of OSPF metric. The default is type 1.	
<ul style="list-style-type: none"><li>□ Type 1—External routes are calculated using both internal and external metrics.</li><li>□ Type 2—External routes are calculated using only the external metrics. Type 1 routes have more cost than Type 2.</li><li>□ none—Removes the OSPF metric.</li></ul>	
<b>prec</b> <value (1-255)>	
Sets the precedence of the route map. The smaller the value, the higher the precedence. Default value is 10.	
<b>weight</b> <value (0-65534)>   none	
Sets the weight of the route map.	
<b>enable</b>	
Enables the route map.	
<b>disable</b>	
Disables the route map.	
<b>delete</b>	
Deletes the route map.	
<b>cur</b>	
Displays the current route configuration.	

**/cfg/l3/rmap** *<route map number>* **/alist** *<access list number>*  
IP Access List Configuration Menu

**Note** – The *route map number* (1-32) and the *access list number* (1-8) represent the IP access list you wish to configure.

```
[IP Access List 1 Menu]
  nwf      - Network Filter number
  metric   - Metric
  action    - Set Network Filter action
  enable   - Enable Access List
  disable  - Disable Access List
  delete   - Delete Access List
  cur      - Display current Access List configuration
```

**Table 219** IP Access List Menu Options (/cfg/l3/rmap/alist)

**Command Syntax and Usage**

**nwf** *<network filter number (1-256)>*

Sets the network filter number. See “/cfg/l3/nwf <1-256>” on page 375 for details.

**metric** *<(1-4294967294)>|none*

Sets the metric value in the AS-External (ASE) LSA.

**action** **permit|deny**

Permits or denies action for the access list.

**enable**

Enables the access list.

**disable**

Disables the access list.

**delete**

Deletes the access list.

**cur**

Displays the current Access List configuration.

**/cfg/l3/rmap** <route map number> **/aspath** <autonomous system path>  
Autonomous System Filter Path Menu

**Note –** The *rmap number* (1-32) and the *path number* (1-8) represent the AS path you wish to configure.

```
[AS Filter 1 Menu]
  as      - AS number
  action  - Set AS Filter action
  enable  - Enable AS Filter
  disable - Disable AS Filter
  delete  - Delete AS Filter
  cur     - Display current AS Filter configuration
```

**Table 220** AS Filter Menu Options (/cfg/l3/rmap/aspath)

**Command Syntax and Usage**

**as** <AS number (1-65535)>  
Sets the Autonomous System filter’s path number.

**action** <permit | deny (p | d)>  
Permits or denies Autonomous System filter action.

**enable**  
Enables the Autonomous System filter.

**disable**  
Disables the Autonomous System filter.

**delete**  
Deletes the Autonomous System filter.

**cur**  
Displays the current Autonomous System filter configuration.



**/cfg/l3/rip**  
**Routing Information Protocol Configuration Menu**

[Routing Information Protocol Menu]

if

- RIP Interface Menu

update

- Set update period in seconds

redist

- RIP Route Redistribute Menu

on

- Globally turn RIP ON

off

- Globally turn RIP OFF

current

- Display current RIP configuration

The RIP Menu is used for configuring Routing Information Protocol (RIP) parameters. This option is turned off by default.

**Table 221** RIP Menu Options (/cfg/l3/rip)

**Command Syntax and Usage**

**if** *<interface number>*

Displays the RIP Interface menu. For more information, see [page 381](#).

**update** *<1-120>*

Configures the time interval for sending for RIP table updates, in seconds. The default value is 30 seconds.

**redist** **fixed|static|ospf|eospf|ebgp|ibgp**

Displays the RIP Route Redistribution menu. For more information, see [page 383](#).

**on**

Globally turns RIP **on**.

**off**

Globally turns RIP **off**.

**cur**

Displays the current RIP configuration.

**/cfg/l3/rip/if** *<interface number>*  
Routing Information Protocol Interface Configuration Menu

[RIP Interface 1 Menu]

version

- Set RIP version

supply

- Enable/disable supplying route updates

listen

- Enable/disable listening to route updates

poison

- Enable/disable poisoned reverse

split

- Enable/disable split horizon

trigg

- Enable/disable triggered updates

mcast

- Enable/disable multicast updates

default

- Set default route action

metric

- Set metric

auth

- Set authentication type

key

- Set authentication key

enable

- Enable interface

disable

- Disable interface

current

- Display current RIP interface configuration

The RIP Interface Menu is used for configuring Routing Information Protocol parameters for the selected interface.

**Note –** Do not configure RIP version 1 parameters if your routing equipment uses RIP version 2.

**Table 222** RIP Interface Menu Options (/cfg/l3/rip/if)

**Command Syntax and Usage**

**version 1|2|both**

Configures the RIP version used by this interface. The default value is version 2.

**supply disable|enable**

When enabled, the switch supplies routes to other routers. The default value is enabled.

**listen disable|enable**

When enabled, the switch learns routes from other routers. The default value is enabled.

**poison disable|enable**

When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon. The default value is disabled.

**split disable|enable**

Enables or disables split horizon. The default value is enabled.

**Table 222** RIP Interface Menu Options (/cfg/l3/rip/if) (continued)

Command Syntax and Usage	
<b>trigg disable   enable</b>	Enables or disables Triggered Updates. Triggered Updates are used to speed convergence. When enabled, Triggered Updates force a router to send update messages immediately, even if it is not yet time for the update message. The default value is <i>enabled</i> .
<b>mcast disable   enable</b>	Enables or disables multicast updates of the routing table (using address 224.0.0.9). The default value is <i>enabled</i> .
<b>default none   listen   supply   both</b>	When enabled, the switch accepts RIP default routes from other routers, but gives them lower priority than configured default gateways. When disabled, the switch rejects RIP default routes. The default value is <i>none</i> .
<b>metric &lt;1-15&gt;</b>	Configures the route metric, which indicates the relative distance to the destination. The default value is 1.
<b>auth none   password</b>	Configures the authentication type. The default is <i>none</i> .
<b>key &lt;password&gt;   none</b>	Configures the authentication key password.
<b>enable</b>	Enables this RIP interface.
<b>disable</b>	Disables this RIP interface.
<b>current</b>	Displays the current RIP configuration.

/cfg/l3/rip/redist fixed|static|ospf|eospf|ebgp|ibgp  
RIP Route Redistribution Configuration Menu

[RIP Redistribute Fixed Menu]	
add	- Add rmap into route redistribution list
rem	- Remove rmap from route redistribution list
export	- Export all routes of this protocol
cur	- Display current route-maps added

The following table describes the RIP Route Redistribute Menu options.

Table 223 RIP Redistribution Menu Options (/cfg/l3/rip/redist)

Command Syntax and Usage

**add** <l-32> <l-32>|all

Adds selected routing maps to the RIP route redistribution list. To add specific route maps, enter routing map numbers, separated by a comma ( , ). To add all 32 route maps, type **all**.

The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.

**rem** <l-32> <l-32>|all

Removes the route map from the RIP route redistribution list.

To remove specific route maps, enter routing map numbers, separated by a comma ( , ). To remove all 32 route maps, type **all**.

**export** <l-15>|none

Exports the routes of this protocol in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter **none**.

**cur**

Displays the current RIP route redistribute configuration.

/cfg/l3/ospf

## Open Shortest Path First Configuration Menu

```
[Open Shortest Path First Menu]
  aindex  - OSPF Area (index) menu
  range   - OSPF Summary Range menu
  if      - OSPF Interface menu
  virt    - OSPF Virtual Links menu
  md5key  - OSPF MD5 Key Menu
  host    - OSPF Host Entry menu
  redistrib - OSPF Route Redistribute menu
  lsdb    - Set the LSDB limit
  default - Originate default route information
  on      - Globally turn OSPF ON
  off     - Globally turn OSPF OFF
  cur     - Display current OSPF configuration
```

**Table 224** OSPF Configuration Menu (/cfg/l3/ospf)

**Command Syntax and Usage**

**aindex** *<area index (0-2)>*

Displays the area index menu. This area index does not represent the actual OSPF area number. See [page 386](#) to view menu options.

**range** *<1-16>*

Displays the summary range menu. See [page 388](#) to view menu options.

**if** *<interface number>*

Displays the OSPF interface configuration menu. See [page 389](#) to view menu options.

**virt** *<virtual link (1-3)>*

Displays the Virtual Links menu used to configure OSPF for a Virtual Link. See [page 391](#) to view menu options.

**md5key** *<key ID (1-255)>*

Assigns a string to MD5 authentication key.

**host** *<1-128>*

Displays the menu for configuring OSPF for the host routes. Up to 128 host routes can be configured. Host routes are used for advertising network device IP addresses to external networks to perform server load balancing within OSPF. It also makes Area Border Route (ABR) load sharing and ABR failover possible. See [page 392](#) to view menu options.

Table 224 OSPF Configuration Menu (/cfg/l3/ospf) (continued)

Command Syntax and Usage	
<b>redist</b> <b>fixed</b>   <b>static</b>   <b>rip</b>   <b>ebgp</b>   <b>ibgp</b>	Displays Route Distribution Menu. See <a href="#">page 393</a> to view menu options.
<b>lsdb</b> <LSDB limit (0-12288, 0 for no limit)>	Sets the link state database limit.
<b>default</b> <metric (1-16777214)> <metric-type 1   2>   <b>none</b>	Sets one default route among multiple choices in an area. Use none for no default.
<b>on</b>	Enables OSPF on the VFSM.
<b>off</b>	Disables OSPF on the VFSM.
<b>cur</b>	Displays the current OSPF configuration settings.

`/cfg/l3/ospf/aindex` *<area index>*  
Area Index Configuration Menu

```
[OSPF Area (index) 1 Menu]
  areaid  - Set area ID
  type    - Set area type
  metric  - Set stub area metric
  auth    - Set authentication type
  spf     - Set time interval between two SPF calculations
  enable  - Enable area
  disable - Disable area
  delete  - Delete area
  cur     - Display current OSPF area configuration
```

**Table 225** Area Index Configuration Menu Options (`/cfg/l3/ospf/aindex`)

---

**Command Syntax and Usage**

---

**areaid** *<IP address (such as, 192.4.17.101)>*

Defines the IP address of the OSPF area number.

---

**type** **transit** | **stub** | **nssa**

Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit.

**Transit area:** allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area.

**Stub area:** is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area.

**NSSA:** Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas.

---

**metric** *<metric value (1-65535)>*

Configures a stub area to send a numeric metric value. All routes received via that stub area carry the configured metric to potentially influencing routing decisions.

Metric value assigns the priority for choosing the switch for default route. Metric type determines the method for influencing routing decisions for external routes.

---

**Table 225** Area Index Configuration Menu Options (/cfg/l3/ospf/aindex)

**Command Syntax and Usage**

**auth** **none** | **password** | **md5**

- ☐ **none**: No authentication required.
- ☐ **password**: Authenticates simple passwords so that only trusted routing devices can participate.
- ☐ **md5**: This parameter is used when MD5 cryptographic authentication is required.

**spf** *<interval (1-255)>*

Configures the minimum time interval, in seconds, between two successive SPF (shortest path first) calculations of the shortest path tree using the Dijkstra’s algorithm. The default value is 10 seconds.

**enable**

Enables the OSPF area.

**disable**

Disables the OSPF area.

**delete**

Deletes the OSPF area.

**cur**

Displays the current OSPF configuration.



*/cfg/13/ospf/range* *<range number>*  
OSPF Summary Range Configuration Menu

[OSPF Summary Range 1 Menu]

addr

- Set IP address

mask

- Set IP mask

aindex

- Set area index

hide

- Enable/disable hide range

enable

- Enable range

disable

- Disable range

delete

- Delete range

cur

- Display current OSPF summary range configuration

**Table 226** OSPF Summary Range Configuration Menu Options  
(/cfg/13/ospf/range)

Command Syntax and Usage

**addr** *<IP Address (such as, 192.4.17.101)>*

Configures the base IP address for the range.

**mask** *<IP mask (such as, 255.255.255.0)>*

Configures the IP address mask for the range.

**aindex** *<area index (0-2)>*

Configures the area index used by the VFSM.

**hide** **disable** | **enable**

Hides the OSPF summary range.

**enable**

Enables the OSPF summary range.

**disable**

Disables the OSPF summary range.

**delete**

Deletes the OSPF summary range.

**current**

Displays the current OSPF summary range.

## `/cfg/l3/ospf/if` *<interface number>* OSPF Interface Configuration Menu

```
[OSPF Interface 1 Menu]
aindex  - Set area index
prio    - Set interface router priority
cost    - Set interface cost
hello   - Set hello interval in seconds or milliseconds
dead    - Set dead interval in seconds or milliseconds
trans   - Set transit delay in seconds
retra   - Set retransmit interval in seconds
key     - Set authentication key
mdkey   - Set MD5 key ID
passive - Enable/disable passive interface
ptop    - Enable/disable point-to-point interface
enable  - Enable interface
disable - Disable interface
delete  - Delete interface
cur     - Display current OSPF interface configuration
```

**Table 227** OSPF Interface Configuration Menu Options (`/cfg/l3/ospf/if`)

---

### Command Syntax and Usage

---

**aindex** *<area index (0-2)>*

Configures the OSPF area index.

---

**prio** *<priority value (0-255)>*

Configures the priority value for the VFSM's OSPF interfaces.

(A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR) or Backup Designated Router (BDR).)

---

**cost** *<1-65535>*

Configures cost set for the selected path—preferred or backup. Usually the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth.

---

**hello** *<1-65535>*

**hello** *<1-65535ms>*

Configures the interval, in seconds or milliseconds, between the `hello` packets for the interfaces.

---

**Table 227** OSPF Interface Configuration Menu Options (/cfg/l3/ospf/if)**Command Syntax and Usage****dead** <1-65535>**dead** <1-65535ms>

Configures the health parameters of a `hello` packet, in seconds or milliseconds, before declaring a silent router to be down.

**trans** <1-3600>

Configures the transit delay in seconds.

**retra** <1-3600>

Configures the retransmit interval in seconds.

**key** <key> | **none**

Sets the authentication key to clear the password.

**mdkey** <key ID (1-255)> | **none**

Assigns an MD5 key to the interface.

**passive enable|disable**

Sets the interface as passive. On a passive interface, you can disable OSPF protocol exchanges, but the router advertises the interface in its LSAs so that IP connectivity to the attached network segment will be established.

**ptop enable|disable**

Sets the interface as point-to-point.

**enable**

Enables OSPF interface.

**disable**

Disables OSPF interface.

**delete**

Deletes OSPF interface.

**cur**

Displays the current settings for OSPF interface.

`/cfg/l3/ospf/virt` *<link number>*  
OSPF Virtual Link Configuration Menu

```
[OSPF Virtual Link 1 Menu]
  aindex - Set area index
  hello  - Set hello interval in seconds or milliseconds
  dead   - Set dead interval in seconds or milliseconds
  trans  - Set transit delay in seconds
  retra  - Set retransmit interval in seconds
  nbr    - Set router ID of virtual neighbor
  key    - Set authentication key
  mdkey  - Set MD5 key ID
  enable - Enable interface
  disable - Disable interface
  delete - Delete interface
  cur    - Display current OSPF interface configuration
```

**Table 228** OSPF Virtual Link Configuration Menu Options (`/cfg/l3/ospf/virt`)

**Command Syntax and Usage**

**aindex** *<area index (0-2)>*

Configures the OSPF area index.

**hello** *<1-65535>*

**hello** *<1-65535ms>*

Configures the authentication parameters of a hello packet, in seconds or milliseconds. The default value is 10 seconds.

**dead** *<1-65535>*

**dead** *<1-65535ms>*

Configures the health parameters of a hello packet, in seconds or milliseconds. The default value is 60 seconds.

**trans** *<1-3600>*

Configures the delay in transit, in seconds. The default value is one second.

**retra** *<1-3600>*

Configures the retransmit interval, in seconds. The default value is five seconds.

**nbr** *<NBR router ID (IP address)>*

Configures the router ID of the virtual neighbor. The default value is 0.0.0.0.

Table 228 OSPF Virtual Link Configuration Menu Options (/cfg/l3/ospf/virt)

Command Syntax and Usage	
<b>key</b> <password>   <b>none</b>	Configures the password (up to eight characters) for each virtual link. The default value is none.
<b>mdkey</b> <key ID (1-255)>   <b>none</b>	Sets MD5 key ID for each virtual link. The default value is none.
<b>enable</b>	Enables OSPF virtual link.
<b>disable</b>	Disables OSPF virtual link.
<b>delete</b>	Deletes OSPF virtual link.
<b>cur</b>	Displays the current OSPF virtual link settings.

**/cfg/l3/ospf/host** <host number>  
OSPF Host Entry Configuration Menu

[OSPF Host Entry 1 Menu]	
addr	- Set host entry IP address
aindex	- Set area index
cost	- Set cost of this host entry
enable	- Enable host entry
disable	- Disable host entry
delete	- Delete host entry
cur	- Display current OSPF host entry configuration

Table 229 OSPF Host Entry Configuration Menu Options (/cfg/l3/ospf/host)

Command Syntax and Usage	
<b>addr</b> <IP address (such as, 192.4.17.101)>	Configures the base IP address for the host entry.
<b>aindex</b> <area index (0-2)>	Configures the area index of the host.

Table 229 OSPF Host Entry Configuration Menu Options (/cfg/l3/ospf/host)

Command Syntax and Usage

**cost** <1-65535>  
Configures the cost value of the host.

**enable**  
Enables OSPF host entry.

**disable**  
Disables OSPF host entry.

**delete**  
Deletes OSPF host entry.

**cur**  
Displays the current OSPF host entries.

/cfg/l3/ospf/redist fixed|static|rip|ebgp|ibgp  
OSPF Route Redistribution Configuration Menu

[OSPF Redistribute Fixed Menu]

add - Add rmap into route redistribution list

rem - Remove rmap from route redistribution list

export - Export all routes of this protocol

cur - Display current route-maps added

Table 230 OSPF Route Redistribution Menu Options (/cfg/l3/ospf/redist)

Command Syntax and Usage

**add** (<route map (1-32)> <route map (1-32)>... | **a11**  
Adds selected routing maps to the rmap list.To add all the 32 route maps, enter **a11**. To add specific route maps, enter routing map numbers one per line, NULL at the end.

This option adds a route map to the route redistribution list. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.

**rem** (<route map (1-32)> <route map (1-32)> ... | **a11**  
Removes the route map from the route redistribution list.

Removes routing maps from the rmap list. To remove all 32 route maps, enter **a11**. To remove specific route maps, enter routing map numbers one per line, NULL at end.

**Table 230** OSPF Route Redistribution Menu Options (/cfg/l3/ospf/redist)

**Command Syntax and Usage**

**export** <metric (1-16777214)> <metric type (1-2)> | **none**

Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter none.

**cur**

Displays the current route map settings.

**/cfg/l3/ospf/md5key <key ID>**  
**OSPF MD5 Key Configuration Menu**

```
[OSPF MD5 Key 1 Menu]
key      - Set authentication key
delete   - Delete key
cur      - Display current MD5 key configuration
```

**Table 231** OSPF MD5 Key Configuration Menu Options (/cfg/ip/ospf/md5key)

**Command Syntax and Usage**

**key** <1-16 characters>

Sets the authentication key for this OSPF packet.

**delete**

Deletes the authentication key for this OSPF packet.

**cur**

Displays the current MD5 key configuration.

/cfg/l3/bgp

## Border Gateway Protocol Configuration Menu

[Border Gateway Protocol Menu]	
peer	- Peer menu
aggr	- Aggregation menu
as	- Set Autonomous System (AS) number
pref	- Set Local Preference
on	- Globally turn BGP ON
off	- Globally turn BGP OFF
cur	- Display current BGP configuration

Border Gateway Protocol (BGP) is an Internet protocol that enables routers on a network to share routing information with each other and advertise information about the segments of the IP address space they can access within their network with routers on external networks. BGP allows you to decide what is the “best” route for a packet to take from your network to a destination on another network, rather than simply setting a default route from your border router(s) to your upstream provider(s). You can configure BGP either within an autonomous system or between different autonomous systems. When run within an autonomous system, it's called internal BGP (iBGP). When run between different autonomous systems, it's called external BGP (eBGP). BGP is defined in RFC 1771.

BGP commands enable you to configure the switch to receive routes and to advertise static routes, fixed routes and virtual server IP addresses with other internal and external routers. In the current BLADEOS implementation, the VFSM does not advertise BGP routes that are learned from one iBGP *speaker* to another iBGP *speaker*.

BGP is turned off by default.

---

**Note –** Fixed routes are subnet routes. There is one fixed route per IP interface.

---

**Table 232** Border Gateway Protocol Menu (/cfg/l3/bgp)

---

**Command Syntax and Usage**

---

**peer** <peer number (1-16)>

Displays the menu used to configure each BGP *peer*. Each border router, within an autonomous system, exchanges routing information with routers on other external networks. To view menu options, see [page 397](#).

---

**aggr** <aggregate number (1-16)>

Displays the Aggregation Menu. To view menu options, see [page 401](#).

---



**Table 232** Border Gateway Protocol Menu (/cfg/l3/bgp) (continued)

Command Syntax and Usage	
<b>as</b> <0-65535>	Set Autonomous System number.
<b>pref</b> <local preference (0-4294967294)>	Sets the local preference. The path with the higher value is preferred.  When multiple peers advertise the same route, use the route with the shortest AS path as the preferred route if you are using eBGP, or use the local preference if you are using iBGP.
<b>on</b>	Globally turns BGP on.
<b>off</b>	Globally turns BGP off.
<b>cur</b>	Displays the current BGP configuration.

## `/cfg/l3/bgp/peer <peer number>` BGP Peer Configuration Menu

```
[BGP Peer 1 Menu]
  redistrib - Redistribution menu
  addr      - Set remote IP address
  ras       - Set remote autonomous system number
  hold      - Set hold time
  alive     - Set keep alive time
  advert    - Set min time between advertisements
  retry     - Set connect retry interval
  orig      - Set min time between route originations
  ttl       - Set time-to-live of IP datagrams
  addi      - Add rmap into in-rmap list
  addo      - Add rmap into out-rmap list
  remi      - Remove rmap from in-rmap list
  remo      - Remove rmap from out-rmap list
  enable    - Enable peer
  disable   - Disable peer
  delete    - Delete peer
  cur       - Display current peer configuration
```

This menu is used to configure BGP peers, which are border routers that exchange routing information with routers on internal and external networks. The peer option is disabled by default.

**Table 233** BGP Peer Configuration Menu Options (`/cfg/l3/bgp/peer`)

---

### Command Syntax and Usage

---

#### **redist**

Displays BGP Redistribution Menu. To view the menu options, see [page 399](#).

---

#### **addr** *<IP address (such as 192.4.17.101)>*

Defines the IP address for the specified peer (border router), using dotted decimal notation. The default address is 0.0.0.0.

---

#### **ras** *<AS number (0-65535)>*

Sets the remote autonomous system number for the specified peer.

---

#### **hold** *<hold time (0, 3-65535)>*

Sets the period of time, in seconds, that will elapse before the peer session is torn down because the switch hasn't received a "keep alive" message from the peer. The default value is 180.

---

#### **alive** *<keepalive time (0, 1-21845)>*

Sets the keep-alive time for the specified peer in seconds. The default value is 60.

---

**Table 233** BGP Peer Configuration Menu Options (/cfg/l3/bgp/peer) (continued)**Command Syntax and Usage**

---

**advert** *<min adv time (1-65535)>*

Sets time, in seconds, between advertisements. The default value is 60 seconds.

---

**retry** *<connect retry interval (1-65535)>*

Sets connection retry interval, in seconds. The default value is 120 seconds.

---

**orig** *<min orig time (1-65535)>*

Sets the minimum time between route originations, in seconds. The default value is 15 seconds.

---

**ttl** *<number of router hops (1-255)>*

Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and should be discarded. TTL specifies a certain time span in seconds that, when exhausted, would cause the packet to be discarded. The TTL is determined by the number of router hops the packet is allowed before it must be discarded.

This command specifies the number of router hops that the IP packet can make. This value is used to restrict the number of “hops” the advertisement makes. It is also used to support multi-hops, which allow BGP peers to talk across a routed network. The default number is set at 1.

**Note:** The TTL value is significant only to eBGP peers, for iBGP peers the TTL value in the IP packets is always 255 (regardless of the configured value).

---

**addi** *<route map ID (1-32)>*

Adds route map into in-route map list.

---

**addo** *<route map ID (1-32)>*

Adds route map into out-route map list.

---

**remi** *<route map ID (1-32)>*

Removes route map from in-route map list.

---

**remo** *<route map ID (1-32)>*

Removes route map from out-route map list.

---

**enable**

Enables this peer configuration.

---

Table 233 BGP Peer Configuration Menu Options (/cfg/l3/bgp/peer) (continued)

Command Syntax and Usage

**disable**

Disables this peer configuration.

**delete**

Deletes this peer configuration.

**cur**

Displays the current BGP peer configuration.

/cfg/l3/bgp/peer/redist  
BGP Redistribution Configuration Menu

```
[Redistribution Menu]
metric - Set default-metric of advertised routes
default - Set default route action
rip - Enable/disable advertising RIP routes
ospf - Enable/disable advertising OSPF routes
fixed - Enable/disable advertising fixed routes
static - Enable/disable advertising static routes
cur - Display current redistribution configuration
```

Table 234 BGP Redistribution Menu Options (/cfg/l3/bgp/peer/redist)

Command Syntax and Usage

**metric** <metric (1-4294967294)> | **none**

Sets default metric of advertised routes.

**default none | import | originate | redistribute**

Sets default route action. Default routes can be configured as follows:

- ☐ none: No routes are configured
- ☐ import: Import these routes.
- ☐ originate: The switch sends a default route to peers if it does not have any default routes in its routing table.
- ☐ redistribute: Default routes are either configured through default gateway or learned through other protocols and redistributed to peer. If the routes are learned from default gateway configuration, you have to enable static routes since the routes from default gateway are static routes. Similarly, if the routes are learned from a certain routing protocol, you have to enable that protocol in this redistribute submenu.

**Table 234** BGP Redistribution Menu Options (/cfg/l3/bgp/peer/redist)

Command Syntax and Usage	
<b>rip disable   enable</b>	
Enables or disables advertising RIP routes	
<b>ospf disable   enable</b>	
Enables or disables advertising OSPF routes.	
<b>fixed disable   enable</b>	
Enables or disables advertising fixed routes.	
<b>static disable   enable</b>	
Enables or disables advertising static routes.	
<b>cur</b>	
Displays current redistribution configuration.	

**/cfg/l3/bgp/aggr** *<aggregation number>*  
BGP Aggregation Configuration Menu

[BGP Aggr 1 Menu]

addr - Set aggregation IP address

mask - Set aggregation network mask

enable - Enable aggregation

disable - Disable aggregation

delete - Delete aggregation

cur - Display current aggregation configuration

This menu enables you to configure BGP aggregation to specify the routes/range of IP destinations a peer router accepts from other peers. All matched routes are aggregated to one route, to reduce the size of the routing table. By default, the first aggregation number is enabled and the rest are disabled.

**Table 235** BGP Aggregation Configuration Menu Options (/cfg/l3/bgp/aggr)

**Command Syntax and Usage**

**addr** *<IP address (such as 192.4.17.101)>*

Defines the starting subnet IP address for this aggregation, using dotted decimal notation. The default address is 0.0.0.0.

**mask** *<IP subnet mask (such as, 255.255.255.0)>*

This IP address mask is used with **addr** to define the range of IP addresses that will be accepted by the peer when the aggregation is enabled. The default address is 0.0.0.0.

**ena**

Enables this BGP aggregation.

**dis**

Disables this BGP aggregation.

**del**

Deletes this BGP aggregation.

**cur**

Displays the current BGP aggregation configuration.

/cfg/l3/igmp  
IGMP Configuration Menu

[IGMP Menu]	
snoop	- IGMP Snoop Menu
relay	- IGMP Relay Menu
mrouter	- Static Multicast Router Menu
igmpflt	- IGMP Filtering Menu
adv	- IGMP Advanced Menu
on	- Globally turn IGMP ON
off	- Globally turn IGMP OFF
cur	- Display current IGMP configuration

Table 236 describes the commands used to configure basic IGMP parameters.

Table 236 IGMP Menu Options (/cfg/l3/igmp)

Command Syntax and Usage

snoop

Displays the IGMP Snoop Menu. To view menu options, see [page 403](#).

relay

Displays the IGMP Relay Menu. To view menu options, see [page 406](#).

mrouter

Displays the Static Multicast Router Menu. To view menu options, see [page 408](#).

igmpflt

Displays the IGMP Filtering Menu. To view menu options, see [page 409](#).

adv

Displays the IGMP Advanced Menu. To view menu options, see [page 412](#).

on

Globally turns IGMP on.

off

Globally turns IGMP off.

cur

Displays the current IGMP configuration parameters.

/cfg/l3/igmp/snoop  
IGMP Snooping Configuration Menu

[IGMP Snoop Menu]

igmpv3

- IGMP Version3 Snoop Menu

mrto

- Set multicast router timeout

aggr

- Aggregate IGMP report

srcip

- Set source ip to use when proxying GSQ

add

- Add VLAN(s) to IGMP Snooping

rem

- Remove VLAN(s) from IGMP Snooping

clear

- Remove all VLAN(s) from IGMP Snooping

ena

- Enable IGMP Snooping

dis

- Disable IGMP Snooping

def

- Set IGMP Snooping settings to factory default

cur

- Display current IGMP Snooping configuration

IGMP Snooping allows the switch to forward multicast traffic only to those ports that request it. IGMP Snooping prevents multicast traffic from being flooded to all ports. The switch learns which server hosts are interested in receiving multicast traffic, and forwards it only to ports connected to those servers.

Table 237 describes the commands used to configure IGMP Snooping.

Table 237 IGMP Snoop Menu Options (/cfg/l3/igmp/snoop)

Command Syntax and Usage

igmpv3

Displays the IGMP version 3 Menu. To view menu options, see [page 404](#).

mrto <1-600 seconds>

Configures the timeout value for IGMP Membership Queries (mrrouter). Once the timeout value is reached, the switch removes the multicast router from its IGMP table, if the proper conditions are met. The range is from 1 to 600 seconds. The default is 255 seconds.

aggr enable | disable

Enables or disables IGMP Membership Report aggregation.

srcip <IP address (such as, 192.4.17.101)>

Configures the source IP address used as a proxy for IGMP Group Specific Queries.

add <VLAN number>

Adds the selected VLAN(s) to IGMP Snooping.



**Table 237** IGMP Snoop Menu Options (/cfg/l3/igmp/snoop) (continued)

**Command Syntax and Usage**

**rem** <VLAN number>

Removes the selected VLAN(s) from IGMP Snooping.

**clear**

Removes all VLANs from IGMP Snooping.

**ena**

Enables IGMP Snooping.

**dis**

Disables IGMP Snooping.

**def**

Resets IGMP Snooping parameters to their default values.

**cur**

Displays the current IGMP Snooping parameters.

**/cfg/l3/igmp/snoop/igmpv3**  
*IGMP Version 3 Configuration Menu*

[IGMP V3 Snoop Menu]	
sources	- Set the number of sources to snoop in group record
v1v2	- Enable/disable snooping IGMPv1/v2 reports
exclude	- Enable/disable snooping EXCLUDE mode reports
ena	- Enable IGMPv3 Snooping
dis	- Disable IGMPv3 Snooping
cur	- Display current IGMP Snooping V3 configuration

Table 238 describes the commands used to configure IGMP version 3.

Table 238 IGMPv3 Menu Options (/cfg/l3/igmp/snoop/igmpv3)

Command Syntax and Usage	
<b>sources</b> <1-64>	Configures the maximum number of IGMP multicast sources to snoop from within the group record. Use this command to limit the number of IGMP sources to provide more refined control. The default value is 8.
<b>v1v2 enable disable</b>	Enables or disables snooping on IGMP version 1 and version 2 reports. When disabled, the switch drops IGMPv1 and IGMPv2 reports. The default value is <i>enabled</i> .
<b>exclude enable disable</b>	Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default value is <i>enabled</i> .
<b>ena</b>	Enables IGMP version 3. The default value is <b>disabled</b> .
<b>dis</b>	Disables IGMP version 3.
<b>cur</b>	Displays the current IGMP version 3 configuration.

/cfg/l3/igmp/relay  
IGMP Relay Configuration Menu

[IGMP Relay Menu]	
mrtr	- Upstream Multicast Router Menu
add	- Add VLAN(s) to downstream
rem	- Remove VLAN(s) from downstream
clear	- Remove all VLAN(s) from downstream
report	- Set unsolicited report interval
ena	- Enable IGMP Relay
dis	- Disable IGMP Relay
cur	- Display current IGMP Relay configuration

Table 240 describes the commands used to configure IGMP Relay.

Table 239 IGMP Relay Menu Options (/cfg/l3/igmp/relay)

Command Syntax and Usage	
mrtr <multicast router number (1-2)>	Displays the Upstream Multicast Router Menu. To view menu options, see <a href="#">page 407</a> .
add <VLAN number>	Adds the VLAN to the list of IGMP Relay VLANs.
rem <VLAN number>	Removes the VLAN from the list of IGMP Relay VLANs.
clear	Removes all VLANs from the list of IGMP Relay VLANs.
report <10-150>	Configures the interval between unsolicited Join reports sent by the switch, in seconds. The default value is 10.
ena	Enables IGMP Relay.
dis	Disables IGMP Relay.
cur	Displays the current IGMP Relay configuration.

`/cfg/l3/igmp/relay/mrtr` *<Mrouter number>*  
IGMP Relay Multicast Router Configuration Menu

[Multicast router 2 Menu]

addr

- Set IP address of multicast router

intr

- Set interval between ping attempts

retry

- Set number of failed attempts to declare router DOWN

restr

- Set number of successful attempts to declare router UP

version

- Set IGMP version

ena

- Enable multicast router

dis

- Disable multicast router

del

- Delete multicast router

cur

- Display current multicast router configuration

Table 242 describes the commands used to configure the IGMP Relay multicast router.

Table 240 IGMP Relay Mrouter Menu Options (/cfg/l3/igmp/relay/mrtr)

Command Syntax and Usage	
<b>addr</b> <i>&lt;IP address (such as, 224.0.1.0)&gt;</i>	Configures the IP address of the IGMP multicast router used for IGMP Relay.
<b>intr</b> <i>&lt;1-60&gt;</i>	Configures the time interval between ping attempts to the upstream Mrouters, in seconds. The default value is 2.
<b>retry</b> <i>&lt;1-120&gt;</i>	Configures the number of failed ping attempts required before the switch declares this Mrouter is down. The default value is 4.
<b>restr</b> <i>&lt;1-128&gt;</i>	Configures the number of successful ping attempts required before the switch declares this Mrouter is up. The default value is 5.
<b>version</b> <i>&lt;1-2&gt;</i>	Configures the IGMP version (1 or 2) of the multicast router.
<b>ena</b>	Enables the multicast router.
<b>dis</b>	Disables the multicast router.

**Table 240** IGMP Relay Mrouter Menu Options (/cfg/l3/igmp/relay/mrtr)

Command Syntax and Usage	
<b>del</b>	Deletes the multicast router from IGMP Relay.
<b>cur</b>	Displays the current IGMP Relay multicast router parameters.

**/cfg/l3/igmp/mrouter**  
IGMP Static Multicast Router Configuration Menu

[Static Multicast Router Menu]	
add	- Add port as Multicast Router Port
rem	- Remove port as Multicast Router Port
clear	- Remove all Static Multicast Router Ports
cur	- Display current Multicast Router configuration

Table 241 describes the commands used to configure a static multicast router.

**Note –** When static Mrouters are used, the switch continues learning dynamic Mrouters via IGMP snooping. However, dynamic Mrouters may not replace static Mrouters. If a dynamic Mrouter has the same port and VLAN combination as a static Mrouter, the dynamic Mrouter is not learned.

**Table 241** IGMP Static Multicast Router Menu Options (/cfg/l3/igmp/mrouter)

Command Syntax and Usage	
<b>add</b> <port number> <VLAN number> <IGMP version number>	Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version (1, 2, or 3) of the multicast router.
<b>rem</b> <port number> <VLAN number> <IGMP version number>	Removes a static multicast router from the selected port/VLAN combination.
<b>clear</b>	Clears all static multicast routers from the switch.
<b>cur</b>	Displays the current IGMP Static Multicast Router parameters.

`/cfg/l3/igmp/igmpflt`  
IGMP Filtering Configuration Menu

[IGMP Filter Menu]	
filter	- IGMP Filter Definition Menu
port	- IGMP Filtering Port Menu
ena	- Enable IGMP Filtering
dis	- Disable IGMP Filtering
cur	- Display current IGMP Filtering configuration

Table 242 describes the commands used to configure an IGMP filter.

**Table 242** IGMP Filtering Menu Options (/cfg/l3/igmp/igmpflt)

Command Syntax and Usage	
<b>filter</b> <filter number (1-16)>	Displays the IGMP Filter Definition Menu. To view menu options, see <a href="#">page 410</a> .
<b>port</b> <port alias or number>	Displays the IGMP Filtering Port Menu. To view menu options, see <a href="#">page 411</a> .
<b>ena</b>	Enables IGMP filtering globally.
<b>dis</b>	Disables IGMP filtering globally.
<b>cur</b>	Displays the current IGMP Filtering parameters.

`/cfg/l3/igmp/igmpflt/filter` *<filter number>*  
IGMP Filter Definition Menu

```
[IGMP Filter 1 Definition Menu]
range    - Set IP Multicast address range
action   - Set filter action
ena      - Enable filter
dis      - Disable filter
del      - Delete filter
cur      - Display current IGMP filter configuration
```

Table 243 describes the commands used to define an IGMP filter.

**Table 243** IGMP Filter Definition Menu Options (`/cfg/l3/igmp/igmpflt/filter`)

Command Syntax and Usage	
<b>range</b> <i>&lt;IP multicast address (such as 225.0.0.10)&gt;</i> <i>&lt;IP multicast address&gt;</i>	Configures the range of IP multicast addresses for this filter.
<b>action allow deny</b>	Allows or denies multicast traffic for the IP multicast addresses specified. The default action is deny.
<b>ena</b>	Enables this IGMP filter.
<b>dis</b>	Disables this IGMP filter.
<b>del</b>	Deletes this filter's parameter definitions.
<b>cur</b>	Displays the current IGMP filter.

`/cfg/l3/igmp/igmpflt/port` *<port number>*  
IGMP Filtering Port Configuration Menu

[IGMP Port EXT1 Menu]

filt

- Enable/disable IGMP filtering on port

add

- Add IGMP filter to port

rem

- Remove IGMP filter from port

cur

- Display current IGMP filtering Port configuration

Table 244 describes the commands used to configure a port for IGMP filtering.

Table 244 IGMP Filter Port Menu Options (/cfg/l3/igmp/igmpflt/port)

Command Syntax and Usage

**filt** **enable** | **disable**

Enables or disables IGMP filtering on this port.

**add** *<filter number (1-16)>*

Adds an IGMP filter to this port.

**rem** *<filter number (1-16)>*

Removes an IGMP filter from this port.

**cur**

Displays the current IGMP filter parameters for this port.



`/cfg/13/igmp/adv`  
IGMP Advanced Configuration Menu

[IGMP Advanced Menu]

qinterval

- Set IGMP query interval

robust

- Set expected packet loss on subnet

timeout

- Set report timeout

fastlv

- Enable/disable Fastleave processing in VLAN

flood

- Flood unregistered IPMC

cpu

- Send unregistered IPMC to CPU

cur

- Display current IGMP Advanced configuration

Table 242 describes the commands used to configure advanced IGMP parameters.

Table 245 IGMP Advanced Menu Options (/cfg/13/igmp/adv)

Command Syntax and Usage

**qinterval** <1-600>

Configures the interval for IGMP Query Reports. The default value is 125 seconds.

**robust** <2-10>

Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), increase the value. The default value is 2.

**timeout** <1-255>

Configures the timeout value for IGMP Membership Reports (host). Once the timeout value is reached, the switch removes the host from its IGMP table, if the conditions are met. The range is from 1 to 255 seconds. The default is 10 seconds.

**fastlv** <VLAN number> **disable** | **enable**

Enables or disables Fastleave processing. Fastleave allows the switch to immediately remove a port from the IGMP port list, if the host sends a Leave message, and the proper conditions are met. This command is disabled by default.

**flood** **enable** | **disable**

Configures the switch to flood unregistered IP multicast traffic to all ports. The default setting is **enabled**.

**Note:** If none of the IGMP hosts reside on the VLAN of the streaming server for a IPMC group, you must disable IGMP flooding to ensure that multicast data is forwarded across the VLANs for that IPMC group.

Table 245 IGMP Advanced Menu Options (/cfg/l3/igmp/adv) (continued)

Command Syntax and Usage

**cpu enable | disable**

Configures the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table, as follows:

- ☐ If no Mrouter is present, drop subsequent packets with same IPMC.
- ☐ If an Mrouter is present, forward subsequent packets to the Mrouter(s) on the ingress VLAN.

The default setting is enabled.

**Note:** If both **flood** and **cpu** are disabled, then the switch drops all unregistered IPMC traffic.

**cur**

Displays the current IGMP Advanced parameters.

/cfg/l3/dns  
Domain Name System Configuration Menu

[Domain Name System Menu]	
prima	- Set IP address of primary DNS server
secon	- Set IP address of secondary DNS server
reqver	- Set the IP version of DNS record to request first
dname	- Set default domain name
cur	- Display current DNS configuration

The Domain Name System (DNS) Menu is used for defining the primary and secondary DNS servers on your local network, and for setting the default domain name served by the switch services. DNS parameters must be configured prior to using hostname parameters with the ping, traceroute, and tftp commands.

**Table 246** Domain Name Service Menu Options (/cfg/l3/dns)

Command Syntax and Usage	
<b>prima</b> <IPv4 address (such as 192.4.17.101)>	
IPv4: You are prompted to set the IP address for your primary DNS server. To set an IPv4 address, use dotted decimal notation.	
<b>prima</b> <IPv6 address (such as 3001:0:0:0:0:abcd:12)>	
IPv6: You are prompted to set the IP address for your primary DNS server. To set an IPv6 address, use hexadecimal format with colons.	
<b>secon</b> <IPv4 address (such as 192.4.17.101)>	
IPv4: You are prompted to set the IP address for your secondary DNS server. To set an IPv4 address, use dotted decimal notation.	
<b>secon</b> <IPv6 address (such as 3001:0:0:0:0:abcd:12)>	
IPv6: You are prompted to set the IP address for your secondary DNS server. To set an IPv6 address, use hexadecimal format with colons.	
If the primary DNS server fails, the configured secondary will be used instead. Enter the IP address using dotted decimal notation.	
<b>reqver v4   v6</b>	
Configures the protocol used for the first request to the DNS server, as follows:	
<input type="checkbox"/> <b>v4</b> : IPv4	
<input type="checkbox"/> <b>v6</b> : IPv6	
<b>dname</b> <dotted DNS notation>   none	
Sets the default domain name used by the switch. For example: mycompany.com	
<b>cur</b>	
Displays the current Domain Name System settings.	

/cfg/l3/bootp

## Bootstrap Protocol Relay Configuration Menu

[Bootstrap Protocol Relay Menu]

addr

- Set IP address of BOOTP server

addr2

- Set IP address of second BOOTP server

on

- Globally turn BOOTP relay ON

off

- Globally turn BOOTP relay OFF

cur

- Display current BOOTP relay configuration

The Bootstrap Protocol (BOOTP) Relay Menu is used to allow hosts to obtain their configurations from a Dynamic Host Configuration Protocol (DHCP) server. The BOOTP configuration enables the switch to forward a client request for an IP address to two DHCP/BOOTP servers with IP addresses that have been configured on the VFSM.

BOOTP relay is turned off by default.

**Table 247** Bootstrap Protocol Relay Configuration Menu Options  
(/cfg/l3/bootp)

---

**Command Syntax and Usage**

---

**addr** <IPv4 address (such as 192.4.17.101)>

Sets the IP address of the BOOTP server. To set an IPv4 address, use dotted decimal notation.

**addr** <IPv6 address (such as 3001:0:0:0:0:abcd:12)>

**IPv6:** Sets the IP address of the BOOTP server. To set an IPv6 address, use hexadecimal format with colons.

---

**addr2** <IPv4 address (such as 192.4.17.101)>

Sets the IP address of the second BOOTP server. To set an IPv4 address, use dotted decimal notation.

**addr2** <IPv6 address (such as 3001:0:0:0:0:abcd:12)>

**IPv6:** Sets the IP address of the second BOOTP server. To set an IPv6 address, use hexadecimal format with colons.

---

**on**

Globally turns on BOOTP relay.

---

**Table 247** Bootstrap Protocol Relay Configuration Menu Options (/cfg/l3/bootp)  
(continued)

Command Syntax and Usage	
<b>off</b>	Globally turns off BOOTP relay.
<b>cur</b>	Displays the current BOOTP relay configuration.

**/cfg/l3/vrrp**  
**VRRP Configuration Menu**

[Virtual Router Redundancy Protocol Menu]	
vr	- VRRP Virtual Router menu
group	- VRRP Virtual Router Group menu
if	- VRRP Interface menu
track	- VRRP Priority Tracking menu
hotstan	- Enable/disable hot-standby processing
on	- Globally turn VRRP ON
off	- Globally turn VRRP OFF
cur	- Display current VRRP configuration

Virtual Router Redundancy Protocol (VRRP) support on VFSMs provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

By default, VRRP is disabled. BLADEOS has extended VRRP to include virtual servers as well, allowing for full active/active redundancy between switches. For more information on VRRP, see the “High Availability” chapter in the *Application Guide*.

**Table 248** VRRP Menu Options (/cfg/l3/vrrp)

---

**Command Syntax and Usage**

---

**vr** *<virtual router number (1-128)>*

Displays the VRRP Virtual Router Menu. This menu is used for configuring virtual routers on this switch. To view menu options, see [page 418](#).

---

**group**

Displays the VRRP virtual router group menu, used to combine all virtual routers together as one logical entity. Group options must be configured when using two or more switches in a hot-standby failover configuration where only one switch is active at any given time. To view menu options, see [page 422](#).

---

**if** *<interface number>*

Displays the VRRP Virtual Router Interface Menu. To view menu options, see [page 425](#).

---

**track**

Displays the VRRP Tracking Menu. This menu is used for weighting the criteria used when modifying priority levels in the master router election process. To view menu options, see [page 426](#).

---

**hotstan disable | enable**

Enables or disables hot standby processing, in which two or more switches provide redundancy for each other. By default, this option is disabled.

---

**on**

Globally enables VRRP on this switch.

---

**off**

Globally disables VRRP on this switch.

---

**cur**

Displays the current VRRP parameters.

---

**/cfg/l3/vrrp/vr** <router number>  
Virtual Router Configuration Menu

[VRRP Virtual Router 1 Menu]

track

- Priority Tracking Menu

vrid

- Set virtual router ID

addr

- Set IP address

if

- Set interface number

prio

- Set router priority

adver

- Set advertisement interval

preem

- Enable or disable preemption

ena

- Enable virtual router

dis

- Disable virtual router

del

- Delete virtual router

cur

- Display current VRRP virtual router configuration

This menu is used for configuring virtual routers for this switch. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Virtual routers are disabled by default.

**Table 249** VRRP Virtual Router Menu Options (/cfg/l3/vrrp/vr)

**Command Syntax and Usage**

**track**

Displays the VRRP Priority Tracking Menu for this virtual router. Tracking is a BLADEOS proprietary extension to VRRP, used for modifying the standard priority system used for electing the master router. To view menu options, see [page 420](#).

**vrid** <virtual router ID (1-255)>

Defines the virtual router ID. This is used in conjunction with `addr` (below) to define a virtual router on this switch. To create a pool of VRRP-enabled routing devices which can provide redundancy to each other, each participating VRRP device must be configured with the same virtual router: one that shares the same `vrid` and `addr` combination.

The `vrid` for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. The default value is 1.

All `vrid` values must be unique within the VLAN to which the virtual router's IP interface belongs.

**Table 249** VRRP Virtual Router Menu Options (/cfg/l3/vrrp/vr) (continued)**Command Syntax and Usage****addr** <IP address (such as, 192.4.17.101)>

Defines the IP address for this virtual router using dotted decimal notation. This is used in conjunction with the `vrid` (above) to configure the same virtual router on each participating VRRP device. The default address is 0.0.0.0.

**if** <interface number>

Selects a switch IP interface. If the IP interface has the same IP address as the `addr` option above, this switch is considered the “owner” of the defined virtual router. An owner has a special priority of 255 (highest) and will always assume the role of master router, even if it must pre-empt another virtual router which has assumed master routing authority. This pre-emption occurs even if the `preem` option below is disabled. The default interface is 1.

**prio** <1-254>

Defines the election priority bias for this virtual server. This can be any integer between 1 and 254. The default value is 100.

During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router’s IP address (`addr`) is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest).

When priority tracking is used (/cfg/l3/vrrp/track or /cfg/l3/vrrp/vr #/track), this base priority value can be modified according to a number of performance and operational criteria.

**adver** <1-255>

Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default value is 1.

**preem disable | enable**

Enables or disables master preemption. When enabled, if this virtual router is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when `preem` is disabled, this virtual router will always preempt any other master if this switch is the owner (the IP interface address and virtual router `addr` are the same). By default, this option is enabled.

**ena**

Enables this virtual router.



**Table 249** VRRP Virtual Router Menu Options (/cfg/l3/vrrp/vr) (continued)

**Command Syntax and Usage**

**dis**

Disables this virtual router.

**del**

Deletes this virtual router from the switch configuration.

**cur**

Displays the current configuration information for this virtual router.

**/cfg/l3/vrrp/vr <router number>/track**  
**Virtual Router Priority Tracking Configuration Menu**

[VRRP Virtual Router 1 Priority Tracking Menu]	
vrs	- Enable/disable tracking master virtual routers
ifs	- Enable/disable tracking other interfaces
ports	- Enable/disable tracking VLAN switch ports
cur	- Display current VRRP virtual router configuration

This menu is used for modifying the priority system used when electing the master router from a pool of virtual routers. Various tracking criteria can be used to bias the election results. Each time one of the tracking criteria is met, the priority level for the virtual router is increased by an amount defined through the VRRP Tracking Menu (see [page 426](#)).

Criteria are tracked dynamically, continuously updating virtual router priority levels when enabled. If the virtual router pre-emption option (see `preem` in [Table 249 on page 418](#)) is enabled, this virtual router can assume master routing authority when its priority level rises above that of the current master.

Some tracking criteria (`vrs`, `ifs`, and `ports` below) apply to standard virtual routers, otherwise called “virtual interface routers.” A virtual *server* router is defined as any virtual router whose IP address (`addr`) is the same as any configured virtual server IP address.

**Table 250** Virtual Router Priority Tracking Options (/cfg/l3/vrrp/vr #/track)

Command Syntax and Usage	
<b>vrs</b>	<b>disable   enable</b>
When enabled, the priority for this virtual router will be increased for each virtual router in master mode on this switch. This is useful for making sure that traffic for any particular client/server pairing are handled by the same switch, increasing routing and load balancing efficiency. This command is disabled by default.	
<b>ifs</b>	<b>disable   enable</b>
When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.	
<b>ports</b>	<b>disable   enable</b>
When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered “active” if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.	
<b>cur</b>	
Displays the current configuration for priority tracking for this virtual router.	

**/cfg/l3/vrrp/group**  
Virtual Router Group Configuration Menu

[VRRP Virtual Router Group Menu]

track

- Priority Tracking Menu

vrid

- Set virtual router ID

if

- Set interface number

prio

- Set renter priority

adver

- Set advertisement interval

preem

- Enable or disable preemption

ena

- Enable virtual router

dis

- Disable virtual router

del

- Delete virtual router

cur

- Display current VRRP virtual router configuration

The Virtual Router Group menu is used for associating all virtual routers into a single logical virtual router, which forces all virtual routers on the VFSM to either be master or backup as a group. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Note

– This option is required to be configured only when using at least two VFSMs in a hot-standby failover configuration, where only one switch is active at any time.

**Table 251** Virtual Router Group Menu Options (/cfg/l3/vrrp/group)

**Command Syntax and Usage**

**track**

Displays the VRRP Priority Tracking Menu for the virtual router group. Tracking is a BLADEOS proprietary extension to VRRP, used for modifying the standard priority system used for electing the master router. To view menu options, see [page 424](#).

**vrid** *<virtual router ID (1-255)>*

Defines the virtual router ID.

The `vrid` for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. All `vrid` values must be unique within the VLAN to which the virtual router’s IP interface (see `if` below) belongs. The default virtual router ID is 1.

**if** *<interface number>*

Selects a switch IP interface. The default switch IP interface number is 1.

**Table 251** Virtual Router Group Menu Options (/cfg/l3/vrrp/group) (continued)**Command Syntax and Usage**

---

**prio** <1-254>

Defines the election priority bias for this virtual router group. This can be any integer between 1 and 254. The default value is 100.

During the master router election process, the routing device with the highest virtual router priority number wins.

Each virtual router group is treated as one entity regardless of how many virtual routers are in the group. When the switch tracks the virtual router group, it measures the resources contained in the group (such as interfaces, VLAN ports, real servers). The priority is updated as a group. Every virtual router in the group has the same priority.

The *owner* parameter does not apply to the virtual router group. The group itself cannot be an owner and therefore the priority is 1-254.

---

**adver** <1-255>

Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default is 1.

---

**preem** **disable** | **enable**

Enables or disables master preemption. When enabled, if the virtual router group is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when *preem* is disabled, this virtual router will always preempt any other master if this switch is the owner (the IP interface address and virtual router *addr* are the same). By default, this option is enabled.

---

**ena**

Enables the virtual router group.

---

**dis**

Disables the virtual router group.

---

**del**

Deletes the virtual router group from the switch configuration.

---

**cur**

Displays the current configuration information for the virtual router group.

---

**/cfg/l3/vrrp/group/track**  
Virtual Router Group Priority Tracking Configuration Menu

```
[Virtual Router Group Priority Tracking Menu]
  ifs      - Enable/disable tracking other interfaces
  ports    - Enable/disable tracking VLAN switch ports
  cur      - Display current VRRP Group Tracking configuration
```

**Note** – If *Virtual Router Group Tracking* is enabled, then the tracking option will be available only under *group* option. The tracking setting for the other individual virtual routers will be ignored.

**Table 252** Virtual Router Group Priority Tracking Menu (/cfg/l3/vr/group/track)

**Command Syntax and Usage**

**ifs** **disable** | **enable**

When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.

**ports** **disable** | **enable**

When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered “active” if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.

**cur**

Displays the current configuration for priority tracking for this virtual router.

**/cfg/l3/vrrp/if** *<interface number>*  
VRRP Interface Configuration Menu

**Note –** The *interface-number* represents the IP interface on which authentication parameters must be configured.

[VRRP Interface 1 Menu]	
auth	- Set authentication types
passw	- Set plain-text password
del	- Delete interface
cur	- Display current VRRP interface configuration

This menu is used for configuring VRRP authentication parameters for the IP interfaces used with the virtual routers.

**Table 253** VRRP Interface Menu Options (/cfg/l3/vrrp/if)

**Command Syntax and Usage**

**auth** **none** | **password**

Defines the type of authentication that will be used: **none** (no authentication), or **password** (password authentication).

**passw** *<password>*

Defines a plain text password up to eight characters long. This password will be added to each VRRP packet transmitted by this interface when password authentication is chosen (see **auth** above).

**del**

Clears the authentication configuration parameters for this IP interface. The IP interface itself is not deleted.

**cur**

Displays the current configuration for this IP interface’s authentication parameters.

**/cfg/l3/vrrp/track**  
**VRRP Tracking Configuration Menu**

[VRRP Tracking Menu]	
vrs	- Set priority increment for virtual router tracking
ifs	- Set priority increment for IP interface tracking
ports	- Set priority increment for VLAN switch port tracking
cur	- Display current VRRP Priority Tracking configuration

This menu is used for setting weights for the various criteria used to modify priority levels during the master router election process. Each time one of the tracking criteria is met (see “VRRP Virtual Router Priority Tracking Menu” on [page 420](#)), the priority level for the virtual router is increased by an amount defined through this menu.

**Table 254** VRRP Tracking Menu Options (/cfg/l3/vrrp/track)

---

**Command Syntax and Usage**

---

**vrs** <0-254>

Defines the priority increment value (0 through 254) for virtual routers in master mode detected on this switch. The default value is 2.

---

**ifs** <0-254>

Defines the priority increment value (0 through 254) for active IP interfaces detected on this switch. The default value is 2.

---

**ports** <0-254>

Defines the priority increment value (0 through 254) for active ports on the virtual router’s VLAN. The default value is 2.

---

**cur**

Displays the current configuration of priority tracking increment values.

---

---

**Note –** These priority tracking options only define increment values. These options do not affect the VRRP master router election process until options under the VRRP Virtual Router Priority Tracking Menu (see [page 420](#)) are enabled.

---

*/cfg/13/gw6* *<gateway number>*  
**IPv6 Default Gateway Configuration Menu**

[Default IP6 gateway 1 Menu]

addr

- Set IP address

ena

- Enable default gateway

dis

- Disable default gateway

del

- Delete default gateway

cur

- Display current default gateway configuration

The switch supports IPv6 default gateways:

- Gateway 1 is used for data traffic.
- Gateway 132 is reserved for management.

The following table describes the IPv6 default gateway configuration options.

**Table 255** IPv6 Default Gateway Menu Options (/cfg/13/gw6)

Command Syntax and Usage	
<b>addr</b> <i>&lt;IPv6 address, such as 3001:0:0:0:0:abcd:12&gt;</i>	Configures the IPv6 address of the default gateway, in hexadecimal format with colons.
<b>ena</b>	Enables the default gateway.
<b>dis</b>	Disables the default gateway.
<b>del</b>	Deletes the default gateway.
<b>cur</b>	Displays current IPv6 default gateway settings.



/cfg/l3/route6  
IPv6 Static Route Configuration Menu

[IP6 Static Route Menu]	
add	- Add static route
rem	- Remove static route
clear	- Clear static routes
cur	- Display current IP6 static route configuration

The following table describes the IPv6 static route configuration options.

**Table 256** IP6 Static Route Menu Options (/cfg/l3/route6)

**Command Syntax and Usage**

**add** <IPv6 address, such as 3001:0:0:0:0:abcd:12> <Prefix length> <gateway address>  
[<interface number>]

Adds an IPv6 static route.

**rem** <IPv6 address, such as 3001:0:0:0:0:abcd:12> <Prefix length> [<interface number>]

Removes the IPv6 static route.

**clear**

Clears IPv6 static routes. You are prompted to select the routes to clear, based on the following criteria:

- ☐ **dest**: Destination IPv6 address of the route
- ☐ **gw**: Default gateway address used by the route
- ☐ **if**: Interface used by the route
- ☐ **all**: All IPv6 static routes

**cur**

Displays the current IPv6 static route configuration.

/cfg/l3/nbrcache  
IPv6 Neighbor Discovery Cache Configuration Menu

[Static NBR Cache Menu]	
add	- Add a static NBR Cache entry
del	- Delete a static NBR Cache entry
clear	- Clear static neighbor cache table
cur	- Display current static NBR Cache configuration

The following table describes the IPv6 Neighbor Discovery cache configuration options.

**Table 257** Static NBR Cache Menu Options (/cfg/l3/nbrcache)

Command Syntax and Usage

**add** <IPv6 address, such as 3001:0:0:0:0:abcd:12> <MAC address, such as 00:60:af:00:02:30> <VLAN number> <port number or alias>

Adds a static entry to the Neighbor Discovery cache table. You are prompted for the following information:

- ☐ IP address
- ☐ MAC address
- ☐ VLAN number
- ☐ Port

**del** <IPv6 address, such as 3001:0:0:0:0:abcd:12>

Deletes the selected entry from the Neighbor Discovery cache table.

**clear**

Clears static entries in the Neighbor Discovery cache table. You are prompted to select the entries to clear, based on the following criteria:

- ☐ **IF**: Entries associated with the selected interface
- ☐ **VLAN**: Entries associated with the selected VLAN
- ☐ **Port**: Entries associated with the selected port
- ☐ **All**: All IPv6 Neighbor cache entries.

**cur**

Displays the current configuration of the Neighbor Discovery static cache table.

**/cfg/l3/ospf3**  
**Open Shortest Path First Version 3 Configuration Menu**

[Open Shortest Path First v3 Menu]	
aindex	- OSPFv3 Area (index) Menu
range	- OSPFv3 Summary Range Menu
summpref	- OSPFv3 AS-External Range Menu
if	- OSPFv3 Interface Menu
virt	- OSPFv3 Virtual Links Menu
host	- OSPFv3 Host Entry Menu
rdstcfg	- OSPFv3 Route Redistribute Entry Menu
redist	- OSPFv3 Route Redistribution Menu
abrtype	- Set the alternative ABR type
lsdb	- Set the LSDB limit for external LSA
exoverfl	- Set exit overflow interval in seconds
refbw	- Set reference bandwidth for dflt intf metric calc
spfdelay	- Set delay between topology change and SPF calc
spfhold	- Set hold time between two consecutive SPF calc
rtrid	- Set a fixed router ID
nasbrdfr	- Enable/disable set P-bit by an NSSA internal ASBR
on	- Globally turn OSPFv3 ON
off	- Globally turn OSPFv3 OFF
cur	- Display current OSPFv3 configuration

**Table 258** OSPF Configuration Menu (/cfg/l3/ospf3)

**Command Syntax and Usage**

<b>aindex</b> <area index (0-2)>
Displays the area index menu. This area index does not represent the actual OSPFv3 area number. See <a href="#">page 433</a> to view menu options.
<b>range</b> <1-16>
Displays summary routes menu for up to 16 IP addresses. See <a href="#">page 435</a> to view menu options.
<b>summpref</b> <1-16>
Displays the OSPFv3 summary prefix configuration menu. See <a href="#">page 436</a> to view menu options.
<b>if</b> <interface number>
Displays the OSPFv3 interface configuration menu. See <a href="#">page 438</a> to view menu options.
<b>virt</b> <virtual link (1-3)>
Displays the Virtual Links menu used to configure OSPFv3 for a Virtual Link. See <a href="#">page 440</a> to view menu options.

**Table 258** OSPF Configuration Menu (/cfg/l3/ospf3) (continued)**Command Syntax and Usage****host** <1-128>

Displays the menu for configuring OSPFv3 for the host routes. Up to 128 host routes can be configured. Host routes are used for advertising network device IP addresses to external networks to perform server load balancing within OSPF. It also makes Area Border Route (ABR) load sharing and ABR failover possible. See [page 441](#) to view menu options.

**rdstcfg** <1-128>

Displays the OSPF route redistribution entry menu. See [page 442](#) to view menu options.

**redist** **connected** | **static**

Displays route redistribution menu. See [page 443](#) to view menu options.

**abrtype** {**standard** | **cisco** | **ibm**}

Configures the Area Border Router (ABR) type, as follows:

- ☐ Standard
- ☐ Cisco
- ☐ IBM

The default setting is *standard*.

**lsdb** <LSDB limit (0-2147483647)> | **none**

Sets the link state database limit.

**exoverfl** <0-4294967295>

Configures the number of seconds that a router takes to exit Overflow State. The default value is 0 (zero).

**refbw** <0-4294967295>

Configures the reference bandwidth, in kilobits per second, used to calculate the default interface metric. The default value is 100,000.

**spfdelay** <0-65535>

Configures the number of seconds that SPF calculation is delayed after a topology change message is received. The default value is 5.

**spfhold** <0-65535>

Configures the number of seconds between SPF calculations. The default value is 10.

**Table 258** OSPF Configuration Menu (/cfg/l3/ospf3) (continued)

Command Syntax and Usage	
<b>rtrid</b> <IP address>	Defines the router ID.
<b>nasbrdfr e d</b>	Enables or disables setting of the P-bit in the default Type 7 LSA generated by an NSSA internal ASBR. The default setting is disabled.
<b>on</b>	Enables OSPFv3 on the switch.
<b>off</b>	Disables OSPFv3 on the switch.
<b>cur</b>	Displays the current OSPF configuration settings.

`/cfg/l3/ospf3/aindex` *<area index>*  
Area Index Configuration Menu

[OSPFv3 Area (index) 1 Menu]	
areaid	- Set area ID
type	- Set area type
metric	- Set metric for the default route into stub/NSSA area
mettype	- Set default metric for stub/NSSA area
stb	- Set stability interval for the NSSA area
trnsrole	- Set translation role for the NSSA area
nosumm	- Enable/disable prevent sending summ LSA into stub/NSSA area
enable	- Enable area
disable	- Disable area
delete	- Delete area
cur	- Display current OSPF area configuration

**Table 259** Area Index Configuration Options (`/cfg/l3/ospf3/aindex`)

**Command Syntax and Usage**

**areaid** *<IP address (such as, 192.4.17.101)>*

Defines the IP address of the OSPFv3 area index.

**type** **transit** | **stub** | **nssa**

Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit.

**Transit area:** allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area.

**Stub area:** is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area.

**NSSA:** Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas.

**metric** *<metric value (1-16777215)>*

Configures the cost for the default summary route in a stub area or NSSA.

**mettype** *<1-3>*

Configures the default metric type applied to the route.

This command applies only to area type of Stub/NSSA.

**Table 259** Area Index Configuration Options (/cfg/l3/ospf3/aindex) (continued)

---

**Command Syntax and Usage**

---

**stb** <1-255>

Configures the stability interval for an NSSA, in seconds. When the interval expires, an elected translator determines that its services are no longer required. The default value is 40.

---

**trnsrole** **always**|**candidate**

Configures the translation role for an NSSA area, as follows:

- ☐ **always**: Type 7 LSAs are always translated into Type 5 LSAs.
  - ☐ **candidate**: An NSSA border router participates in the translator election process.
- The default setting is **candidate**.

---

**nosumm** **e**|**d**

Enables or disables the no-summary option. When enabled, the area-border router neither originates nor propagates Inter-Area-Prefix LSAs into stub/NSSA areas. Instead it generates a default Inter-Area-Prefix LSA.

The default setting is **disabled**.

---

**enable**

Enables the OSPFv3 area.

---

**disable**

Disables the OSPFv3 area.

---

**delete**

Deletes the OSPFv3 area.

---

**cur**

Displays the current OSPFv3 area configuration.

---

**/cfg/l3/ospf3/range** *<range number>*  
OSPFv3 Summary Range Configuration Menu

[OSPFv3 Summary Range 1 Menu]	
addr	- Set IPv6 address
preflen	- Set IPv6 prefix length
aindex	- Set area index
lsatype	- Set LSA type for aggregation
tag	- Set route tag
hide	- Enable/disable hide range
enable	- Enable range
disable	- Disable range
delete	- Delete range
cur	- Display current OSPFv3 summary range configuration

**Table 260** OSPFv3 Summary Range Configuration Options  
(/cfg/l3/ospf3/range)

**Command Syntax and Usage**

**addr** *<IPv6 address>*

Configures the base IPv6 address for the range.

**preflen** *<IPv6 prefix length (1-128)>*

Configures the subnet IPv6 prefix length. The default value is 0 (zero).

**aindex** *<area index (0-2)>*

Configures the area index used by the switch.

**lsatype** **summary|Type7**

Configures the LSA type, as follows:

- ☐ Summary LSA
- ☐ Type7 LSA

**tag** *<0-4294967295>*

Configures the route tag.

**hide** **disable|enable**

Hides the OSPFv3 summary range.

**enable**

Enables the OSPFv3 summary range.



**Table 260** OSPFv3 Summary Range Configuration Options  
(/cfg/l3/ospf3/range) (continued)

Command Syntax and Usage	
<b>disable</b>	Disables the OSPFv3 summary range.
<b>delete</b>	Deletes the OSPFv3 summary range.
<b>cur</b>	Displays the current OSPFv3 summary range configuration.

**/cfg/l3/ospf3/summpref** *<range number>*  
OSPFv3 AS-External Range Configuration Menu

[OSPFv3 AS-External Range 1 Menu]	
addr	- Set IPv6 address
preflen	- Set IPv6 prefix length
aindex	- Set area index
aggreff	- Set aggregation effect
transl	- Enable/disable set P-bit in the generated LSA
enable	- Enable range
disable	- Disable range
delete	- Delete range
cur	- Display current OSPFv3 AS-External range configuration

**Table 261** OSPFv3 AS\_External Range Configuration Options  
(/cfg/l3/ospf3/range)

Command Syntax and Usage	
<b>addr</b> <i>&lt;IPv6 address&gt;</i>	Configures the base IPv6 address for the range.
<b>preflen</b> <i>&lt;IPv6 prefix length (1-128)&gt;</i>	Configures the subnet IPv6 prefix length. The default value is 0 (zero).
<b>aindex</b> <i>&lt;area index (0-2)&gt;</i>	Configures the area index used by the switch.

**Table 261** OSPFv3 AS\_External Range Configuration Options  
(/cfg/13/ospf3/range) (continued)

<b>Command Syntax and Usage</b>	
<b>aggreff allowAll denyAll advertise not-advertise</b>	<p>Configures the aggregation effect, as follows:</p> <ul style="list-style-type: none"><li>□ <b>allowAll</b>: If the area ID is 0.0.0.0, aggregated Type-5 LSAs are generated. Aggregated Type-7 LSAs are generated in all the attached NSSAs for the range.</li><li>□ <b>denyAll</b>: Type-5 and Type-7 LSAs are not generated.</li><li>□ <b>advertise</b>: If the area ID is 0.0.0.0, aggregated Type-5 LSAs are generated. For other area IDs, aggregated Type-7 LSAs are generated in the NSSA area.</li><li>□ <b>not-advertise</b>: If the area ID is 0.0.0.0, Type-5 LSAs are not generated, while all NSSA LSAs within the range are cleared and aggregated Type-7 LSAs are generated for all NSSAs. For other area IDs, aggregated Type-7 LSAs are not generated in the NSSA area.</li></ul>
<b>transl e d</b>	<p>When enabled, the P-bit is set in the generated Type-7 LSA. When disabled, the P-bit is cleared. The default setting is disabled.</p>
<b>enable</b>	<p>Enables the OSPFv3 AS-external range.</p>
<b>disable</b>	<p>Disables the OSPFv3 AS-external range.</p>
<b>delete</b>	<p>Deletes the OSPFv3 AS-external range.</p>
<b>cur</b>	<p>Displays the current OSPFv3 AS-external range.</p>

*/cfg/l3/ospf3/if* *<interface number>*  
OSPFv3 Interface Configuration Menu

[OSPFv3 Interface 1 Menu]	
aindex	- Set area index
instance	- Set instance id
prio	- Set interface router priority
cost	- Set interface cost
hello	- Set hello interval in seconds
dead	- Set dead interval in seconds
transm	- Set transmit delay in seconds
retra	- Set retransmit interval in seconds
passive	- Enable/disable passive interface
enable	- Enable interface
disable	- Disable interface
delete	- Delete interface
cur	- Display current OSPFv3 interface configuration

**Table 262** OSPFv3 Interface Configuration Options (*/cfg/l3/ospf3/if*)

**Command Syntax and Usage**

**aindex** *<area index (0-2)>*

Configures the OSPFv3 area index.

**instance** *<0-255>*

Configures the instance ID for the interface.

**prio** *<priority value (0-255)>*

Configures the priority value for the switch's OSPFv3 interface.

A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR).

**cost** *<1-65535>*

Configures the metric value for sending a packet on the interface.

**hello** *<1-65535>*

Configures the indicated interval, in seconds, between the `hello` packets, that the router sends on the interface.

**dead** *<1-65535>*

Configures the time period, in seconds, for which the router waits for `hello` packet from the neighbor before declaring this neighbor down.

**Table 262** OSPFv3 Interface Configuration Options (/cfg/l3/ospf3/if) (continued)

**Command Syntax and Usage**

**transm** <1-1800>

Configures the estimated time, in seconds, taken to transmit LS update packet over this interface.

**retra** <1-1800>

Configures the interval in seconds, between LSA retransmissions for adjacencies belonging to interface.

**passive enable|disable**

Enables or disables the `passive` setting on the interface. On a passive interface, OSPFv3 protocol packets are suppressed.

**enable**

Enables the OSPFv3 interface.

**disable**

Disables the OSPFv3 interface.

**delete**

Deletes the OSPFv3 interface.

**cur**

Displays the current settings for OSPFv3 interface.

`/cfg/l3/ospf3/virt` *<link number>*  
OSPFv3 Virtual Link Configuration Menu

```
[OSPFv3 Virtual Link 1 Menu]
  aindex    - Set area index
  hello     - Set hello interval in seconds
  dead      - Set dead interval in seconds
  trans     - Set transit delay in seconds
  retra     - Set retransmit interval in seconds
  nbr       - Set router ID of virtual neighbor
  enable    - Enable interface
  disable   - Disable interface
  delete    - Delete interface
  cur       - Display current OSPFv3 interface configuration
```

**Table 263** OSPFv3 Virtual Link Configuration Options (`/cfg/l3/ospf3/virt`)

**Command Syntax and Usage**

**aindex** *<area index (0-2)>*

Configures the OSPFv3 area index.

**hello** *<1-65535>*

Configures the indicated interval, in seconds, between the hello packets, that the router sends on the interface.

**dead** *<1-65535>*

Configures the time period, in seconds, for which the router waits for hello packet from the neighbor before declaring this neighbor down.

**trans** *<1-1800>*

Configures the estimated time, in seconds, taken to transmit LS update packet over this interface.

**retra** *<1-1800>*

Configures the interval, in seconds, between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPFv3 virtual link interface. The default value is five seconds.

**nbr** *<NBR router ID (IP address)>*

Configures the router ID of the virtual neighbor. The default setting is 0.0.0.0

**enable**

Enables OSPFv3 virtual link.

**Table 263** OSPFv3 Virtual Link Configuration Options (/cfg/l3/ospf3/virt)

Command Syntax and Usage	
<b>disable</b>	Disables the OSPFv3 virtual link.
<b>delete</b>	Deletes the OSPFv3 virtual link.
<b>cur</b>	Displays the current OSPFv3 virtual link settings.

**/cfg/l3/ospf3/host** *<host number>*  
OSPFv3 Host Entry Configuration Menu

[OSPF Host Entry 1 Menu]	
addr	- Set host entry IP address
aindex	- Set area index
cost	- Set cost of this host entry
enable	- Enable host entry
disable	- Disable host entry
delete	- Delete host entry
cur	- Display current OSPF host entry configuration

**Table 264** OSPFv3 Host Entry Configuration Options (/cfg/l3/ospf3/host)

Command Syntax and Usage	
<b>addr</b> <i>&lt;IPv6 address&gt;</i>	Configures the base IPv6 address for the host entry.
<b>aindex</b> <i>&lt;area index (0-2)&gt;</i>	Configures the area index of the host.
<b>cost</b> <i>&lt;1-65535&gt;</i>	Configures the cost value of the host.
<b>enable</b>	Enables OSPF host entry.
<b>disable</b>	Disables OSPF host entry.

**Table 264** OSPFv3 Host Entry Configuration Options (/cfg/l3/ospf3/host)

**Command Syntax and Usage**

**delete**

Deletes OSPF host entry.

**cur**

Displays the current OSPF host entries.

**/cfg/l3/ospf3/rdstcfg <1-128>**  
**OSPFv3 Redist Entry Configuration Menu**

```
[OSPFv3 Redist Entry 1 Menu]
  addr      - Set redistrib entry IPv6 address
  preflen   - Set IPv6 prefix length
  metric    - Set metric to be applied to the route
  metatype  - Set metric type
  tag       - Set route tag
  enable    - Enable redistrib entry
  disable   - Disable redistrib entry
  delete    - Delete redistrib entry
  cur       - Display current OSPF redistrib entry configuration
```

**Table 265** OSPFv3 Redist Entry Configuration Options (/cfg/l3/ospf3/rdstcfg)

**Command Syntax and Usage**

**addr <IPv6 address>**

Configures the base IPv6 address for the redistribution entry.

**preflen <IPv6 prefix length (1-128)>**

Configures the subnet IPv6 prefix length. The default value is 64.

**metric <1-16777215>**

Configures the route metric value applied to the route before it is advertised into the OSPFv3 domain.

**metatype asExttype1|asExttype2**

Configures the metric type applied to the route before it is advertised into the OSPFv3 domain.

**tag <0-4294967295>|unset**

Configures the route tag. To clear the route tag, enter **unset**.

Table 265 OSPFv3 Redist Entry Configuration Options (/cfg/l3/ospf3/rdstcfg)

Command Syntax and Usage

**enable**

Enables the OSPFv3 redistribution entry.

**disable**

Disables the OSPFv3 redistribution entry.

**delete**

Deletes the OSPFv3 redistribution entry.

**cur**

Displays the current OSPFv3 redistribution configuration entries.

/cfg/l3/ospf3/redist connected|static  
OSPFv3 Redistribute Configuration Menu

```
[OSPF Redistribute Static Menu]
export    - Export all routes of this protocol
cur       - Display current redistribution setting
```

Table 266 OSPFv3 Redistribute Configuration Options (/cfg/l3/ospf3/redist)

Command Syntax and Usage

**export** [*<metric value (1-16777215)>* | **none**] [*<metric type (1-2)>*]  
[*<tag (0-4294967295)>* | **unset**]

Exports the routes of this protocol as external OSPFv3 AS-external LSAs in which the metric, metric type, and route tag are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter **none**.

To clear the route tag, enter **unset**.

**cur**

Displays the current OSPFv3 route redistribution settings.



*/cfg/l3/loopif <interface number (1-5)>*  
**IP Loopback Interface Configuration Menu**

[IP Loopback Interface 2 Menu]	
addr	- Set IP address
mask	- Set subnet mask
ena	- Enable IP interface
dis	- Disable IP interface
del	- Delete IP interface
cur	- Display current interface configuration

An IP loopback interface is not connected to any physical port. A loopback interface is always accessible over the network.

**Table 267** IP Loopback Interface Menu Options (/cfg/l3/loopif)

<b>Command Syntax and Usage</b>	
<b>addr</b> <i>&lt;IP address&gt;</i>	Defines the loopback interface IP address.
<b>mask</b> <i>&lt;subnet mask&gt;</i>	Defines the loopback interface subnet mask.
<b>ena</b>	Enables the loopback interface.
<b>dis</b>	Disables the loopback interface.
<b>del</b>	Deletes the selected loopback interface.
<b>cur</b>	Displays the current IP loopback interface parameters.

/cfg/cee

# Converged Enhanced Ethernet Configuration

[CEE Configuration Menu]

global

- Global CEE Configuration Menu

port

- Port CEE Configuration Menu

on

- Globally turn CEE Features ON

off

- Globally turn CEE Features OFF

cur

- Display current CEE configuration

Table 268 describes the Converged Enhanced Ethernet (CEE) configuration menu options.

Table 268 CEE Configuration Options (/cfg/cee)

Command Syntax and Usage

global

Displays the CEE Global Configuration menu. To view menu options, see [page 446](#).

port

Displays the CEE Port Configuration menu. To view menu options, see [page 450](#).

on

Globally turns CEE on.

off

Globally turns CEE off.

cur

Displays the current CEE parameters.

**/cfg/cee/global**  
**CEE Global Configuration**

[Global CEE Configuration Menu]	
ets	- Enhanced Transmission Selection Menu
pfc	- Priority Flow Control Menu
cur	- Display current CEE configuration

Table 269 describes the global CEE configuration options.

**Table 269** CEE Global Options (/cfg/cee/global)

---

**Command Syntax and Usage**

---

**ets**

Displays the Enhanced Transmission Selection menu. To view menu options, see [page 446](#).

---

**pfc**

Displays the Priority Flow Control menu. To view menu options, see [page 448](#).

---

**cur**

Displays the current global CEE parameters.

---

**/cfg/cee/global/ets**  
**ETS Global Configuration**

[Global Enhanced Transmission Selection Menu]	
pg	- Priority Group Menu
cur	- Displays current ETS configuration

Enhanced Transmission Selection (ETS) allows you to allocate bandwidth to different traffic types, based on 802.1p priority.

Table 270 describes the global ETS configuration options.

---

**Note –** ETS configuration supersedes the QoS 802.1p menu. When ETS is enabled, you cannot configure the 802.1p menu options.

---

Table 270 CEE Global ETS Options (/cfg/cee/global/ets)

Command Syntax and Usage	
<b>pg</b> <0-7, 15>	Displays the Enhanced Transmission Selection menu for the selected Priority Group. To view menu options, see <a href="#">page 447</a> .
<b>cur</b>	Displays the current global CEE parameters.

**/cfg/cee/global/ets/pg** <0-7, 15>  
ETS Global Priority Group Configuration

[PGID 1 Menu]	
create	- Create Priority Group
bw	- Set bandwidth percentage for the Priority Group
prio	- Assign one or more 802.1p priorities to Priority Group
desc	- Set description for the Priority Group
cur	- Display current Priority Group configuration

An ETS Priority Group can be assigned one or more 802.1p priority values. Switch bandwidth is allocated by percentage to each Priority Group.

[Table 271](#) describes the global ETS Priority Group configuration options.

Table 271 Global ETS Priority Group Options (/cfg/cee/global/ets/pg)

Command Syntax and Usage	
<b>create</b> <bandwidth percentage (0-100)> <802.1p value (0-7)>	Allows you to configure Priority Group parameters. You can enter the link bandwidth percentage allocated to the Priority Group, and also assign one or more 802.1p values to the Priority Group.
<b>bw</b> <bandwidth percentage (0-100)>	Configures the link bandwidth allocation for the Priority Group, as a percentage from 1% to 100%.
<b>prio</b> <0-7>	Adds one or more 802.1p priority values to the Priority Group. Enter one value per line, null to end.

**Table 271** Global ETS Priority Group Options (/cfg/cee/global/ets/pg)

Command Syntax and Usage	
<b>desc</b> <1-31 characters>	Enter text that describes this Priority Group.
<b>cur</b>	Displays the current ETS global Priority Group parameters.

**/cfg/cee/global/pfc**  
**Priority Flow Control Global Configuration**

[Global Priority Flow Control Menu]	
pri	- 802.1p Priority PFC Menu
on	- Globally turn PFC ON
off	- Globally turn PFC OFF
cur	- Display current PFC configuration

Priority-based Flow Control (PFC) enhances flow control by allowing the switch to pause traffic based on its 802.1p priority value, while allowing traffic at other priority levels to continue.

[Table 272](#) describes the global Priority Flow Control (PFC) configuration options.

**Table 272** Global Priority Flow Control Options (/cfg/cee/global/pfc)

Command Syntax and Usage	
<b>pri</b> <0-7>	Displays the 802.1p Priority PFC menu. To view menu options, see <a href="#">page 449</a> .
<b>on</b>	Globally turns PFC on.
<b>off</b>	Globally turns PFC off.
<b>cur</b>	Displays the current Priority Flow Control parameters.

`/cfg/cee/global/pfc/pri <0-7>`  
802.1p Priority Flow Control Configuration

[Priority 1 Menu]	
ena	- Enable PFC on this priority queue
dis	- Disable PFC on this priority queue
desc	- Set a description string to identify the priority queue
cur	- Display current PFC configuration

Table 273 describes the global Priority Flow Control (PFC) configuration options.

**Table 273** Global PFC 802.1p Options (/cfg/cee/global/pfc/pri)

---

**Command Syntax and Usage**

---

**ena**

Enables Priority Flow Control on the selected 802.1p priority.

---

**dis**

Disables Priority Flow Control on the selected 802.1p priority.

---

**desc** *<1-31 characters>*

Enter text to describe the 802.1p priority value.

---

**cur**

Displays the current 802.1p Priority Flow Control parameters.

---

*/cfg/cee/port <port alias or number>*  
**CEE Port Configuration**

```
[Port 1 CEE Configuration Menu]
  dcbx      - DCB Capability Exchange Protocol (DCBX) Menu
  pfc       - Priority Flow Control Menu
  cur       - Display current Port CEE configuration
```

Table 274 describes the Converged Enhanced Ethernet (CEE) port configuration options.

**Table 274** CEE Port Options (/cfg/cee/port)

---

**Command Syntax and Usage**

---

**dcbx**

Displays the DCB Capability Exchange Protocol (DCBX) menu for the selected port. To view menu options, see [page 450](#).

**pfc**

Displays the Priority Flow Control (PFC) menu for the selected port. To view menu options, see [page 452](#).

**cur**

Displays the current CEE port parameters.

---

*/cfg/cee/port <port alias or number> /dcbx*  
**DCBX Port Configuration**

```
[Port EXT1 DCBX Config Menu]
  appadv    - Set Advertise flag for Application Protocol
  appwill   - Set Willing flag for Application Protocol
  etsadv    - Set Advertise flag for PG
  etswill   - Set Willing flag for PG
  pfcadv    - Set Advertise flag for PFC
  pfcwill   - Set Willing flag for PFC
  dis       - Disable DCBX
  ena       - Enable DCBX
  cur       - Display current port DCBX configuration
```

Data Center Bridging Capability Exchange (DCBX) protocol is used by Converged Enhanced Ethernet (CEE) networks to exchange advanced detection and configuration data.

Table 275 describes the port DCB Capability Exchange Protocol (DCBX) configuration options.

Table 275 Port DCBX Options (/cfg/cee/port x/dcbx)

Command Syntax and Usage	
<b>appadv enable disable</b>	Enables or disables DCBX Application Protocol advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).
<b>appwill enable disable</b>	Enables or disables Application Protocol willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data).
<b>etsadv enable disable</b>	Enables or disables DCBX ETS advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).
<b>etswill enable disable</b>	Enables or disables ETS willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data).
<b>pfcadv enable disable</b>	Enables or disables DCBX PFC advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).
<b>pfcwill enable disable</b>	Enables or disables PFC willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data).
<b>dis</b>	Disables DCBX on the port.
<b>ena</b>	Enables DCBX on the port.
<b>cur</b>	Displays the current DCBX parameters on the port.



*/cfg/cee/port <port alias or number> /pfc*  
**PFC Port Configuration**

[Port EXT2 PFC Configuration Menu]	
pri	- 802.1p Priority PFC Menu
on	- Turn ON PFC
off	- Turn OFF PFC
cur	- Display current PFC configuration

Table 275 describes the port Priority Flow Control (PFC) configuration options.

**Table 276** Port PFC Options (/cfg/cee/port x/pfc)

---

**Command Syntax and Usage**

---

**pri** <0-7>

Displays the 802.1p Priority PFC menu for the selected port. To view menu options, see [page 453](#).

---

**on**

Turns PFC on for the selected port.

---

**off**

Turns PFC off for the selected port.

---

**cur**

Displays the current PFC parameters for the selected port.

---

**/cfg/cee/port** *<port alias or number>* **/pfc/pri** *<0-7>*  
802.1p PFC Port Configuration

[Priority 1 Menu]	
ena	- Enable PFC on this priority queue
dis	- Disable PFC on this priority queue
desc	- Set a description string to identify the priority queue
cur	- Display current PFC configuration

Table 273 describes the port-level Priority Flow Control (PFC) configuration options.

**Table 277** Port 802.1p PFC Options (/cfg/cee/port x/pfc/pri)

---

**Command Syntax and Usage**

---

**ena**

Enables Priority Flow Control on the selected 802.1p priority.

---

**dis**

Disables Priority Flow Control on the selected 802.1p priority.

---

**desc** *<1-31 characters>*

Enter text to describe the 802.1p priority value.

---

**cur**

Displays the current 802.1p Priority Flow Control parameters.

---

**/cfg/fcoe**

## Fiber Channel over Ethernet Configuration

[Fiber Channel over Ethernet Configuration Menu]	
fips	- FCoE Initialization Protocol (FIP) Snooping Menu
cur	- Display current FCOE configuration

Fiber Channel over Ethernet (FCoE) transports Fiber Channel frames over an Ethernet fabric. The CEE features and FCoE features allow you to create a lossless Ethernet transport mechanism.

[Table 278](#) describes the FCoE configuration options.

**Table 278** FCoE Options (/cfg/fcoe)

### Command Syntax and Usage

#### **fips**

Displays the FCoE Initialization Protocol (FIP) Snooping menu. To view menu options, see [page 454](#).

#### **cur**

Displays the current FCoE parameters.

**/cfg/fcoe/fips**

## FIPS Configuration

[FIP Snooping Configuration Menu]	
port	- Port FIP snooping Menu
on	- Globally turn FIP snooping ON
off	- Globally turn FIP snooping OFF
aclto	- Enable/Disable the removal of expired FCFs and FCOE ACLs
cur	- Display current FIP snooping global configuration

FIP Snooping allows the switch to monitor FCoE Initialization Protocol (FIP) frames to gather discovery, initialization, and maintenance data. This data is used to automatically configure ACLs that provide FCoE connections and data security.

Table 279 describes the FCoE Initialization Protocol (FIP) Snooping configuration options.

Table 279 FIP Snooping Options (/cfg/fcoe/fips)

Command Syntax and Usage	
<b>port</b> <port number>	Displays the FCoE Initialization Protocol (FIP) Snooping menu for the selected port. To view menu options, see <a href="#">page 456</a> .
<b>on</b>	Globally turns FIP Snooping on.
<b>off</b>	Globally turns FIP Snooping off.
<b>aclto e d</b>	Enables or disables ACL time-out removal. When enabled, ACLs associated with expired FCFs and FCoE connections are removed from the system.
<b>cur</b>	Displays the current FIP Snooping parameters.

`/cfg/fcoe/fips/port` *<port alias or number>*  
**FIPS Port Configuration**

[Port 1 FIP Snooping Configuration Menu]

fcfmode

- Set whether FCF is connected to this port

ena

- Enable FIP snooping

dis

- Disable FIP snooping

cur

- Display current FIP snooping configuration

Table 273 describes the port FCoE Initialization Protocol (FIP) Snooping configuration options.

**Table 280** Port FIP Snooping Options (`/cfg/fcoe/fips/port`)

**Command Syntax and Usage**

**fcfmode** `auto|on|off`

Configures FCoE Forwarding (FCF) on the port, as follows:

- ☐ **on**: Configures the port as a Fiber Channel Forwarding (FCF) port.
- ☐ **off**: Configures the port as an FCoE node (ENode).
- ☐ **auto**: Automatically detect the configuration of the connected device, and configure this port to match.

**ena**

Enables FIP Snooping on the port. The default setting is enabled.

**dis**

Disables FIP Snooping on the port.

**cur**

Displays the current FIP Snooping parameters.

/cfg/rmon

# Remote Monitoring Configuration

---

[RMON Menu]	
hist	- RMON History Menu
event	- RMON Event Menu
alarm	- RMON Alarm Menu
cur	- Display current RMON configuration

Remote Monitoring (RMON) allows you to monitor traffic flowing through the switch. The RMON MIB is described in RFC 1757.

[Table 281](#) describes the Remote Monitoring (RMON) configuration menu options.

**Table 281** Remote Monitoring (RMON) Menu Options (/cfg/rmon)

---

## Command Syntax and Usage

---

**hist** <I-65535>

Displays the RMON History Configuration menu. To view menu options, see [page 458](#).

**event** <I-65535>

Displays the RMON Event Configuration menu. To view menu options, see [page 459](#).

**alarm** <I-65535>

Displays the RMON Alarm Configuration menu. To view menu options, see [page 460](#).

**cur**

Displays the current RMON parameters.

---

`/cfg/rmon/hist <1-65535>`  
**RMON History Configuration Menu**

[RMON History 2 Menu]	
ifoid	- Set interface MIB object to monitor
rbnum	- Set the number of requested buckets
intrval	- Set polling interval
owner	- Set owner for the RMON group of statistics
delete	- Delete this history and restore defaults
cur	- Display current history configuration

Table 282 describes the RMON History Menu options.

**Table 282** RMON History Menu Options (/cfg/rmon/hist)

Command Syntax and Usage	
<b>ifoid</b> <i>&lt;1-127 characters&gt;</i>	
Configures the interface MIB Object Identifier. The IFOID must correspond to the standard interface OID, as follows:  1.3.6.1.2.1.2.2.1.1.x  where x is the ifIndex	
<b>rbnum</b> <i>&lt;1-65535&gt;</i>	
Configures the requested number of buckets, which is the number of discrete time intervals over which data is to be saved. The default value is 30.  The maximum number of buckets that can be granted is 50.	
<b>intrval</b> <i>&lt;1-3600&gt;</i>	
Configures the time interval over which the data is sampled for each bucket.  The default value is 1800.	
<b>owner</b> <i>&lt;1-127 characters&gt;</i>	
Enter a text string that identifies the person or entity that uses this History index.	
<b>delete</b>	
Deletes the selected History index.	
<b>cur</b>	
Displays the current RMON History parameters.	

`/cfg/rmon/event <1-65535>`  
**RMON Event Configuration Menu**

[RMON Event 2 Menu]	
descn	- Set description for the event
type	- Set event type
owner	- Set owner for the event
delete	- Delete this event and restore defaults
cur	- Display current event configuration

Table 283 describes the RMON Event Menu options.

**Table 283** RMON Event Menu Options (/cfg/rmon/event)

---

**Command Syntax and Usage**

---

**descn** *<1-127 characters>*

Enter a text string to describe the event.

---

**type** *none|log|trap|both*

Selects the type of notification provided for this event. For log events, an entry is made in the log table and sent to the configured syslog host. For trap events, an SNMP trap is sent to the management station.

---

**owner** *<1-127 characters>*

Enter a text string that identifies the person or entity that uses this event index.

---

**delete**

Deletes the selected RMON Event index.

---

**cur**

Displays the current RMON Event parameters.

---



`/cfg/rmon/alarm </-65535>`  
**RMON Alarm Configuration Menu**

[RMON Alarm 2 Menu]	
oid	- Set MIB oid datasource to monitor
interval	- Set alarm interval
sample	- Set sample type
almtyp	- Set startup alarm type
rlimit	- Set rising threshold
flimit	- Set falling threshold
revtid	- Set event index to fire on rising threshold crossing
fevtid	- Set event index to fire on falling threshold crossing
owner	- Set owner for the alarm
delete	- Delete this alarm and restore defaults
cur	- Display current alarm configuration

The Alarm RMON group can track rising or falling values for a MIB object. The MIB object must be a counter, gauge, integer, or time interval. Each alarm index must correspond to an event index that triggers once the alarm threshold is crossed.

Table 284 describes the RMON Alarm Menu options.

**Table 284** RMON Alarm Menu Options (`/cfg/rmon/alarm`)

**Command Syntax and Usage**

**oid** *</-127 characters>*

Configures an alarm MIB Object Identifier.

**interval** *</-65535>*

Configures the time interval over which data is sampled and compared with the rising and falling thresholds. The default value is 1800.

**sample** *abs|delta*

Configures the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows:

- *abs*—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.
- *delta*—delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.

**almtyp** *rising|falling|either*

Configures the alarm type as rising, falling, or either (rising or falling).

Table 284 RMON Alarm Menu Options (/cfg/rmon/alarm)

Command Syntax and Usage	
<b>rlimit</b> <-2147483647 - 2147483647>	Configures the rising threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated.
<b>flimit</b> <-2147483647 - 2147483647>	Configures the falling threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated.
<b>revtdix</b> <1-65535>	Configures the rising alarm event index that is triggered when a rising threshold is crossed.
<b>fevtdix</b> <1-65535>	Configures the falling alarm event index that is triggered when a falling threshold is crossed.
<b>owner</b> <1-127 characters>	Enter a text string that identifies the person or entity that uses this alarm index.
<b>delete</b>	Deletes the selected RMON Alarm index.
<b>cur</b>	Displays the current RMON Alarm parameters.

/cfg/virt

# Virtualization Configuration

[Virtualization Menu]	
vmpolicy	- Virtual Machines Policy Configuration Menu
vnic	- vNIC Configuration Menu
vmgroup	- Virtual Machines Groups Menu
vmprof	- Virtual Machine Profiles Menu
vmware	- VMware-specific Settings Menu
enavmr	- Enable VMready
disvmr	- Disable VMready
cur	- Display all current virtualization settings

Table 285 describes the general virtualization configuration options. More detailed information is available in the following sections.

**Table 285** Virtualization Configuration Options (/cfg/virt)

**Command Syntax and Usage**

**vmpolicy**

Displays the Virtual Machines Policy menu. To view menu options, see [page 463](#).

**vnic**

Displays the Virtual NIC (vNIC) menu. To view menu options, see [page 464](#).

**vmgroup** <1-32>

Displays the Virtual Machine Groups menu. To view menu options, see [page 469](#).

**vmprof**

Displays the Virtual Machine Profiles menu. To view menu options, see [page 471](#).

**vmware**

Displays the VMware settings menu. To view menu options, see [page 473](#).

**enavmr**

Enables VMready.

**disvmr**

Disables VMready.

**cur**

Displays the current virtualization parameters.

/cfg/virt/vmpolicy

## Virtual Machines Policy Configuration

[VM Policy Configuration Menu]

vmbwidth - VM Bandwidth Configuration Menu

Table 286 describes the Virtual Machines (VM) policy configuration options.

Table 286 VM Policy Options (/cfg/virt/vmpolicy)

Command Syntax and Usage

**vmbwidth** <MAC address> | <UUID> | <name> | <IP address> | <index number>

Displays the bandwidth management menu for the selected Virtual Machine. Enter a unique identifier to select a VM.

/cfg/virt/vmpolicy/vmbwidth <VM identifier>

## VM Policy Bandwidth Management

[VM Bandwidth Management Menu]

txrate - Set VM Transmit Bandwidth (Ingress for switch)

bwctrl - Enable/Disable VM Bandwidth Control

delete - Delete VM bandwidth control Entry

cur - Display current VM bandwidth configuration

Table 287 describes the bandwidth management options for the selected VM. Use these commands to limit the bandwidth used by each VM.

Table 287 VM Bandwidth Management Options (/cfg/virt/vmpolicy/vmbwidth)

Command Syntax and Usage

**txrate** <64-10000000> [32|64|128|256|512|1024|2048|4096] <1-256>

The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the VM to the switch, in kilobits per second. Enter the value in multiples of 64.

The second values configures the maximum burst size, in Kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096.

The third value represents the ACL assigned to the transmission rate. The ACL is automatically, in sequential order, if not specified by the user. If there are no available ACLs, the TXrate cannot be configured. Each TXrate configuration reduces the number of available ACLs by one.

**Table 287** VM Bandwidth Management Options (/cfg/virt/vmpolicy/vmbwidth)

**Command Syntax and Usage**

**rxrate** <64-1000000> [32|64|128|256|512|1024|2048|4096]

The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the switch to the VM, in kilobits per second. Enter the value in multiples of 64.

The second values configures the maximum burst size, in Kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096.

**bwctrl** e|d

Enables or disables bandwidth control on the VM policy.

**delete**

Deletes the bandwidth management settings from this VM policy.

**cur**

Displays the current VM bandwidth management parameters.

**/cfg/virt/vnic**  
**Virtual NIC Configuration**

[VNIC Global Configuration Menu]	
port	- Port vNIC Configuration Menu
vnicgrp	- VNIC Group Configuration Menu
on	- Globally turn vNIC feature ON
off	- Globally turn vNIC feature OFF
cur	- Display current vNIC configuration

Table 288 describes the Virtual NIC (vNIC) configuration options.

**Table 288** Virtual NIC Options (/cfg/virt/vnic)

**Command Syntax and Usage**

**port** <port number>

Displays the port vNIC menu. To view menu options, see [page 465](#).

**vnicgrp** <1-32>

Displays the vNIC group menu. To view menu options, see [page 467](#).

**Table 288** Virtual NIC Options (/cfg/virt/vnic) (continued)

Command Syntax and Usage	
<b>on</b>	Globally turns vNIC on.
<b>off</b>	Globally turns vNIC off.
<b>cur</b>	Displays the current vNIC parameters.

**/cfg/virt/vnic/port** *<port alias or number>*  
**vNIC Port Configuration**

[Port 1 vNICs Menu]	
vnic	- VNIC Configuration Menu
cur	- Display current port vNIC configuration

Table 289 describes the Virtual NIC (vNIC) port configuration options.

**Table 289** Port vNIC Options (/cfg/virt/vnic)

Command Syntax and Usage	
<b>vnic</b> <i>&lt;1-4&gt;</i>	Displays the vNIC menu for the selected vNIC. To view menu options, see <a href="#">page 466</a> .
<b>cur</b>	Displays the current vNIC port parameters.

**/cfg/virt/vnic/port** *<port alias or number>* **/vnic** *<vNIC number>*  
**vNIC Port Configuration**

[vNIC 1.1 Menu]	
bw	- Set maximum bandwidth of the vNIC
ena	- Enable vNIC
dis	- Disable vNIC
cur	- Display current vNIC configuration

Table 290 describes the Virtual NIC (vNIC) port configuration options.

**Table 290** Port vNIC Options (/cfg/virt/vnic/port/vnic)

---

**Command Syntax and Usage**

---

**bw** *<1-100>*

Configures the maximum bandwidth allocated to this vNIC, in increments of 100 Mbps. For example:

- ☐ 1 = 100 Mbps
- ☐ 10 = 1000 Mbps

---

**ena**

Enables the selected vNIC.

---

**dis**

Disables the selected vNIC.

---

**cur**

Displays the current vNIC port parameters.

---

`/cfg/virt/vnic/vnicgrp </-32>`  
**Virtual NIC Group Configuration**

[vNIC Group 1 Menu]

vnicvlan

- Set VLAN number to vNIC group

failover

- Enable/disable uplink failover

addvnic

- Add vNIC to vNIC group

remvnic

- Remove vNIC from vNIC group

addport

- Add port to vNIC group

remport

- Remove port from vNIC group

addtrnk

- Add trunk to vNIC group

remtrnk

- Remove trunk from vNIC group

ena

- Enable vNIC group

dis

- Disable vNIC group

del

- Delete vNIC group

cur

- Display current vNIC group configuration

Table 291 describes the Virtual NIC (vNIC) group configuration options.

**Table 291** Port vNIC Group options (/cfg/virt/vnic/vnicgrp)

**Command Syntax and Usage**

**vnicvlan** *<VLAN number>*

Assigns a VLAN to the vNIC group.

**failover** *e|d*

Enables or disables uplink failover for the vNIC Group. Uplink Failover for the vNIC Group will disable only the affected vNIC links on the port. Other port functions continue to operate normally.

The default setting is disabled.

**addvnic** *<vNIC ID>*

Adds a vNIC to the vNIC Group. The vNIC ID is comprised of the port number and the vNIC number. For example: int1.1

**remvnic** *<vNIC ID>*

Removes the selected vNIC from the vNIC Group.

**addport** *<port number>*

Adds the selected switch port to the vNIC Group.

**remport** *<port number>*

Removes the selected switch port from the vNIC Group.



**Table 291** Port vNIC Group options (/cfg/virt/vnic/vnicgrp)

Command Syntax and Usage	
<b>addtrnk</b> <trunk number>	Adds the selected trunk group to the vNIC Group.
<b>remtrnk</b> <trunk number>	Removes the selected trunk group from the vNIC Group.
<b>ena</b>	Enables the vNIC Group.
<b>dis</b>	Disables the vNIC Group.
<b>del</b>	Deletes the vNIC Group.
<b>cur</b>	Displays the current vNIC Group parameters.

/cfg/virt/vmgroup </-32>  
VM Group Configuration

[VM group 1 Menu]	
vlan	- Set the group's vlan (only for groups with no VM profile)
vmap	- Set VMAP for this group
tag	- Enable vlan tagging on all VM group ports
addvm	- Add a virtual entity to the group
remvm	- Remove a virtual entity from the group
addprof	- Add a VM profile to the group
remprof	- Delete any VM profile associated with the group
addport	- Add ports to the group
remport	- Remove ports from the group
addtrunk	- Add trunk to the group
remtrunk	- Remove trunk from the group
addkey	- Add LACP trunk to the group
remkey	- Remove LACP trunk from the group
stg	- Assign VM group vlan to a Spanning Tree Group
del	- Delete group
cur	- Display current group configuration

Table 292 describes the Virtual Machine (VM) group configuration options. A VM group is a collection of members, such as VMs, ports, or trunk groups. Members of a VM group share certain properties, including VLAN membership, ACLs (VMAP), and VM profiles.

Table 292 VM Group Options (/cfg/virt/vmgroup)

Command Syntax and Usage

**vlan** <VLAN number>

Assigns a VLAN to this VM group. If you do not assign a VLAN to the VM group, the switch automatically assigns an unused VLAN when adding a port or a VM to the VM Group.

**Note:** If you add a VM profile to this group, the group will use the VLAN assigned to the profile.

**vmap add|rem** </-/28> **intports|extports**

Assigns the selected VLAN Map to this VM group. You can choose to limit operation of the VLAN Map to internal ports only or external ports only. If you do not select a port type, the VMAP is applied to the entire VM Group.

For more information about configuring VLAN Maps, see “VMAP Configuration” on page 307.

**tag e|d**

Enables or disables VLAN tagging on ports in this VM group.

**Table 292** VM Group Options (/cfg/virt/vmgroup) (continued)**Command Syntax and Usage**


---

**addvm** <MAC address> | <UUID> | <name> | <IP address> | <index number>

Adds a VM to the VM group. Enter a unique identifier to select a VM.

The UUID and name parameters apply only if Virtual Center information is configured (/cfg/virt/vmware/vcspec).

The VM index number is found in the VM information dump (/info/virt/vm/dump).

**Note:** If the VM is connected to a port that is contained within the VM group, do not add the VM to the VM group.

---

**remvm** <MAC address> | <UUID> | <name> | <IP address> | <index number>

Removes a VM from the VM group. Enter a unique identifier to select a VM.

The UUID and name parameters apply only if Virtual Center information is configured (/cfg/virt/vmware/vcspec).

The VM index number is found in the VM information dump (/info/virt/vm/dump).

---

**addprof** <profile name (1-32 characters)>

Adds the selected VM profile to the VM group.

---

**remprof**

Removes the VM profile assigned to the VM group.

---

**addport** <port number or alias>

Adds the selected port to the VM group.

**Note:** Add a port to a VM group only if no VMs on that port are members of the VM group.

---

**remport** <port number or alias>

Removes the selected port from the VM group.

---

**addtrunk** <trunk number>

Adds the selected trunk group to the VM group.

---

**remtrunk** <trunk number>

Removes the selected trunk group from the VM group.

---

**addkey** <1-65535>

Adds an LACP admin key to the VM group. LACP trunks formed with this admin key will be included in the VM group.

---

Table 292 VM Group Options (/cfg/virt/vmgroup) (continued)

Command Syntax and Usage	
<b>remkey</b> <1-65535>	Removes an LACP admin key from the VM group.
<b>stg</b> <STG number>	Assigns the VM group VLAN to a Spanning Tree Group (STG).
<b>del</b>	Deletes the VM group.
<b>cur</b>	Displays the current VM group parameters.

/cfg/virt/vmprof

VM Profile Configuration

[VM Profiles Menu]	
create	- Create a VM profile
edit	- Edit a VM profile
cur	- Display details of all VM profiles

Configuration of VMs with the VM Agent requires the use of VM profiles, which ease the configuration and management of VM Agent-based VM groups. The VM profile contains a set of properties that will be configured on the Virtual Switch.

After a VM profile has been defined, it can be assigned to a VM group or exported to one or more VMware hosts.

Table 293 describes the VM Profiles configuration options.

Table 293 VM Profile options (/cfg/virt/vmprof)

Command Syntax and Usage	
<b>create</b> <profile name (1-39 characters)>	Defines a name for the VM profile. The switch supports up to 32 VM profiles.

**Table 293** VM Profile options (/cfg/virt/vmprof) (continued)

**Command Syntax and Usage**

**edit** *<profile name>*

Displays the VM Profile Edit menu for the selected profile. To view menu options, see [page 472](#).

**cur**

Displays the current VM Profiles parameters.

**/cfg/virt/vmprof/edit** *<profile name>*  
**VM Profile Edit**

```
[VM profile "myProfile" Menu]
vlan      - Set the VM profile's VLAN ID
shaping   - Set or delete the VM profile's traffic shaping parameters
delete    - Delete this VM profile
cur       - Show details of the current VM profile
```

[Table 294](#) describes the VM Profile Edit options.

**Table 294** Edit VM Profile options (/cfg/virt/vmprof/edit)

**Command Syntax and Usage**

**vlan** *<VLAN number>*

Assigns a VLAN to the VM profile.

**shaping** [*<average (1-1000000000)>* *<burst (1-1000000000)>* *<peak (1-1000000000)>*] **delete**

Configures traffic shaping parameters implemented in the hypervisor, as follows:

- ☐ Average traffic, in Kilobits per second
- ☐ Maximum burst size, in Kilobytes
- ☐ Peak traffic, in Kilobits per second
- ☐ Delete traffic shaping parameters.

**delete**

Deletes the selected VM Profile.

**cur**

Displays the current VM Profiles parameters.

/cfg/virt/vmware  
VM Ware Configuration

[VMware-specific Settings Menu]	
hbport	- Set ESX/ESXi server to vCenter heartbeat UDP port number
vcspec	- Create, update or delete Virtual Center access information
cur	- Display current VMware-specific settings

Table 295 describes the VMware configuration options. When the user configures the VMware Virtual Center, the VM Agent module in the switch can perform advanced functionality by communicating with the VMware management console. The Virtual Center provides VM and Host names, IP addresses, Virtual Switch and port group information. The VM Agent on the switch communicates with the Virtual Center to synchronize VM profiles between the switch and the VMware virtual switch.

Table 295 VMware Options (/cfg/virt/vmware)

Command Syntax and Usage	
hbport	<1-65535>
Configures the UDP port number used for heartbeat communication from the VM host to the Virtual Center. The default value is port 902.	
vcspec	[<IP address>] [<username> noauth]   [delete]
Defines the Virtual Center credentials on the switch. Once you configure the Virtual Center, VM Agent functionality is enabled across the system.	
You are prompted for the following information:	
<div><input type="checkbox"/> IP address of the Virtual Center</div> <div><input type="checkbox"/> User name and password for the Virtual Center</div> <div><input type="checkbox"/> Whether to authenticate the SSL security certificate (yes or no)</div>	
cur	
Displays the current VMware parameters.	

## /cfg/dump Dump

---

The dump program writes the current switch configuration to the terminal screen. To start the dump program, at the Configuration# prompt, enter:

```
Configuration# dump
```

The configuration is displayed with parameters that have been changed from the default values. The screen display can be captured, edited, and placed in a script file, which can be used to configure other switches through a Telnet connection. When using Telnet to configure a new switch, paste the configuration commands from the script file at the command line prompt of the switch. The active configuration can also be saved or loaded via TFTP, as described on [page 475](#).

## /cfg/ptcfg <FTP/TFTP server> <filename> Saving the Active Switch Configuration

---

When the ptcfg command is used, the switch's active configuration commands (as displayed using /cfg/dump) will be uploaded to the specified script configuration file on the FTP/TFTP server. To start the switch configuration upload, at the Configuration# prompt, enter:

```
Configuration# ptcfg <FTP or TFTP server> <filename>
```

Where *server* is the FTP/TFTP server IPv4/IPv6 address or hostname, and *filename* is the name of the target script configuration file.

---

**Note** – The output file is formatted with line-breaks but no carriage returns—the file cannot be viewed with editors that require carriage returns (such as Microsoft Notepad).

---

---

**Note** – If the FTP/TFTP server is running SunOS or the Solaris operating system, the specified ptcfg file must exist prior to executing the ptcfg command and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current configuration data.

---

*/cfg/gtcfg <FTP/TFTP server> <filename>*

## Restoring the Active Switch Configuration

---

When the `gtcfg` command is used, the active configuration will be replaced with the commands found in the specified configuration file. The file can contain a full switch configuration or a partial switch configuration. The configuration loaded using `gtcfg` is not activated until the `apply` command is used. If the `apply` command is found in the configuration script file loaded using this command, the `apply` action will be performed automatically.

To start the switch configuration download, at the `Configuration#` prompt, enter:

```
Configuration# gtcfg <FTP or TFTP server> <filename>
```

Where *server* is the FTP/TFTP server IPv4/IPv6 address or hostname, and *filename* is the name of the target script configuration file.



## CHAPTER 7

# The Operations Menu

---

The Operations Menu is generally used for commands that affect switch performance immediately, but do not alter permanent switch configurations. For example, you can use the Operations Menu to immediately disable a port (without the need to apply or save the change), with the understanding that when the switch is reset, the port returns to its normally configured operation.

### /oper

## Operations Menu

---

```
[Operations Menu]
port      - Operational Port Menu
fcoe      - Operational Fiber Channel Over Ethernet Menu
vrrp      - Operational Virtual Router Redundancy Menu
ip        - Operational IP Menu
prm       - Protected Mode Menu
sys       - Operational System Menu
virt      - Virtualization Operations Menu
passwd    - Change current user password
clrlog    - Clear syslog messages
tnetsshc  - Close all telnet/SSH connections
conlog    - Enable/disable session console logging
cfgtrk    - Track last config change made
ntpreq    - Send NTP request
```

The commands of the Operations Menu enable you to alter switch operational characteristics without affecting switch configuration.

**Table 296** Operations Menu (/oper)

---

**Command Syntax and Usage**

---

**port** *<port alias or number>*

Displays the Operational Port Menu. To view menu options, see [page 480](#).

---

**fcoe**

Displays the Fiber Channel over Ethernet (FCoE) Operations Menu. To view menu options, see [page 482](#).

---

**vrrp**

Displays the Operational Virtual Router Redundancy Menu. To view menu options, see [page 483](#).

---

**ip**

Displays the IP Operations Menu, which has one sub-menu/option, the Operational Border Gateway Protocol Menu. To view menu options, see [page 484](#).

---

**prm**

Displays the Protected Mode menu. To view menu options, see [page 485](#).

---

**sys**

Displays the Operational System menu. To view menu options, see [page 486](#).

---

**virt**

Displays the Virtualization Operations Menu. To view menu options, see [page 487](#).

---

**passwd** *<1-128 characters>*

Allows the user to change the password. You need to enter the current password in use for validation.

---

**clrlog**

Clears all Syslog messages.

---

**tnetsshc**

Closes all open Telnet and SSH connections.

---

**Table 296** Operations Menu (/oper) (continued)

Command Syntax and Usage	
<b>conlog enable disable</b>	
Enables or disables console logging of the current session.	
<b>cfgtrk</b>	
Displays a list of configuration changes made since the last <code>apply</code> command. Each time the <code>apply</code> command is sent, the configuration-tracking log is cleared.	
<b>ntpreq</b>	
Allows the user to send requests to the NTP server.	

*/oper/port <port alias or number>*  
**Operations-Level Port Options Menu**

[Operations Port INT1 Menu]

8021x

- 8021.x Menu

rmon

- Enable/disable RMON for port

ena

- Enable port

dis

- Disable port

cur

- Current port state

Operations-level port options are used for temporarily disabling or enabling a port, and for re-setting the port.

**Table 297** Operations-Level Port Menu Options (/oper/port)

**Command Syntax and Usage**

**8021x**

Displays the 802.1X Port Menu. To view menu options, see [page 481](#).

**rmon e|d**

Enables or disables Remote Monitoring (RMON) for the port. The default setting is disabled.

**ena**

Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset.

**dis**

Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset.

**cur**

Displays the current settings for the port.

*/oper/port <port alias or number>/8021x*  
**Operations-Level Port 802.1X Options Menu**

[802.1X Operation Menu]

reset - Reinitialize 802.1X access control on this port

reauth - Initiate reauthentication on this port now

Operations-level port 802.1X options are used to temporarily set 802.1X parameters for a port.

**Table 298** Operations-Level Port 802.1X Menu Options (/oper/port x/8021x)

**Command Syntax and Usage**

**reset**

Re-initializes the 802.1X access-control parameters for the port. The following actions take place, depending on the 802.1X port configuration:

- ☐ **force unauth** - the port is placed in unauthorized state, and traffic is blocked.
- ☐ **auto** - the port is placed in unauthorized state, then authentication is initiated.
- ☐ **force auth** - the port is placed in authorized state, and authentication is not required.

**reauth**

Re-authenticates the supplicant (client) attached to the port. This command only applies if the port's 802.1X mode is configured as `auto`.

/oper/fcoe

# Operations-Level FCoE Menu

[Operational FCOE Menu]
fips - Operational FIP Snooping Menu

Table 299 Operations-Level FCoE Options (/oper/fcoe)

Command Syntax and Usage

**fips**

Displays the FCoE Initialization Protocol Snooping operations menu.

/oper/fcoe/fips

## FCoE FIP Snooping Operations

[FIP Snooping Operational Menu]
delfcf - Delete an FCF entry and the associated ACLs from the database

Table 300 FIP Snooping Operations (/oper/fcoe/fips)

Command Syntax and Usage

**delfcf** <MAC address>

Deletes the selected FCoE Forwarder (FCF), and any associated ACLs.

/oper/vrrp

# Operations-Level VRRP Options Menu

---

[VRRP Operations Menu]

back - Set virtual router to backup

---

**Table 301** Operations-Level VRRP Menu Options (/oper/vrrp)

---

**Command Syntax and Usage**

---

**back** <virtual router number (1-255)>

Forces the specified master virtual router on this switch into backup mode. This is generally used for passing master control back to a preferred switch once the preferred switch has been returned to service after a failure. When this command is executed, the current master gives up control and initiates a new election by temporarily advertising its own priority level as 0 (lowest). After the new election, the virtual router forced into backup mode by this command will resume master control in the following cases:

- ❑ This switch owns the virtual router (the IP addresses of the virtual router and its IP interface are the same)
  - ❑ This switch’s virtual router has a higher priority and preemption is enabled.
  - ❑ There are no other virtual routers available to take master control.
-

/oper/ip

## Operations-Level IP Options Menu

---

```
[IP Operations Menu]
  bgp      - Operational Border Gateway Protocol Menu
```

---

**Table 302** Operations-Level IP Menu Options (/oper/ip)

**Command Syntax and Usage**

---

**bgp**

Displays the Border Gateway Protocol Operations Menu. To view the menu options see [page 484](#).

---

/oper/ip/bgp

## Operations-Level BGP Options Menu

```
[Border Gateway Protocol Operations Menu]
  start    - Start peer session
  stop     - Stop peer session
  current  - Current BGP operational state
```

---

**Table 303** Operations-Level BGP Menu Options (/oper/ip/bgp)

**Command Syntax and Usage**

---

**start** <peer number (1-16)>

Starts the peer session.

---

**stop** <peer number (1-16)>

Stops the peer session.

---

**cur**

Displays the current BGP operational state.

---



## /oper/prm Protected Mode Options Menu

```
[Protected Mode Menu]
mgt  - Enable/disable local control of external management
ext  - Enable/disable local control of external ports
fact - Enable/disable local control of factory default reset
mif  - Enable/disable local control of Mgmt VLAN interface
on   - Turn on/alter protected mode by applying enabled features
off  - Turn off protected mode by removing all features
cur  - Display current PRM configuration
```

Protected Mode is used to secure certain switch management options, so they cannot be changed by the management module.

**Table 304** Protected Mode Options (/oper/prm)

### Command Syntax and Usage

#### **mgt enable|disable**

Enables exclusive local control of switch management. When Protected Mode is set to **on**, the management module cannot be used to disable external management on the switch. The default value is **enabled**.

**Note:** Due to current management module implementation, this setting cannot be disabled.

#### **ext enable|disable**

Enables exclusive local control of external ports. When Protected Mode is set to **on**, the management module cannot be used to disable external ports on the switch. The default value is **enabled**.

**Note:** Due to current management module implementation, this setting cannot be disabled.

#### **fact enable|disable**

Enables exclusive local control of factory default resets. When Protected Mode is set to **on**, the management module cannot be used to reset the switch software to factory default values. The default value is **enabled**.

**Note:** Due to current management module implementation, this setting cannot be disabled.

#### **mif enable|disable**

Enables exclusive local control of the management interface. When Protected Mode is set to **on**, the management module cannot be used to configure parameters for the management interface. The default value is **enabled**.

**Note:** Due to current management module implementation, this setting cannot be disabled.

Table 304 Protected Mode Options (/oper/prm) (continued)

Command Syntax and Usage	
<b>on</b>	Turns Protected Mode <b>on</b> . When Protected Mode is turned on, the switch takes exclusive local control of all enabled options.
<b>off</b>	Turns Protected Mode <b>off</b> . When Protected Mode is turned off, the switch relinquishes exclusive local control of all enabled options.
<b>cur</b>	Displays the current Protected Mode configuration.

/oper/sys

## System Operations Menu

[Operational System Menu]	
i2c	- System I2C

I2C device commands are to be used only by Technical Support personnel.

/oper/virt

# Virtualization Operations

---

```
[Virtualization Operations Menu]
vmware    - VMware Operations Menu
```

Table 305 describes general virtualization operations options. More details are available in the following sections.

Table 305 Virtualization Options (/oper/virt)

---

## Command Syntax and Usage

---

### vmware

Displays the VMware operations menu.

---

/oper/virt/vmware

# VMware Operations

---

```
[VMware Operations Menu]
addpg      - Add a port group to a Host
addvsw     - Add a Vswitch to a Host
delpg      - Delete a port group from a Host
delvsw     - Delete a Vswitch from a Host
export     - Create or update a VM profile on one or more Hosts
scan       - Perform a VM Agent scan operation now
vmacpg     - Change a vNIC's port group
updp      - Update a port group on a Host
```

Use these commands to perform minor adjustments to the VMware operation. Use these commands to perform Virtual Switch operations directly from the switch. Note that these commands require the configuration of Virtual Center access information (/cfg/virt/vmware/vcspec).

**Table 306** VMware Operations (/oper/virt/vmware)

---

**Command Syntax and Usage**

---

**addpg** [*<Port Group name>* *<host ID>* *<Vswitch name>* *<VLAN number>*  
*<shaping-enabled>* *<average-Kbps>* *<burst-KB>* *<peak-Kbps>*]

Adds a Port Group to a VMware host. You are prompted for the following information:

- ☐ Port Group name
- ☐ VMware host ID (Use host UUID, host IP address, or host name.)
- ☐ Virtual Switch name
- ☐ VLAN ID of the Port Group
- ☐ Whether to enable the traffic-shaping profile (y or n). If you choose y (yes), you are prompted to enter the traffic shaping parameters.

---

**addvsw** *<host ID>* *<Virtual Switch name>*

Adds a Virtual Switch to a VMware host. Use one of the following identifiers to specify the host:

- ☐ UUID
- ☐ IP address
- ☐ Host name

---

**delpg** *<Port Group name>* *<host ID>*

Removes a Port Group from a VMware host. Use one of the following identifiers to specify the host:

- ☐ UUID
- ☐ IP address
- ☐ Host name

---

**delvsw** *<host ID>* *<Virtual Switch name>*

Removes a Virtual Switch from a VMware host. Use one of the following identifiers to specify the host:

- ☐ UUID
  - ☐ IP address
  - ☐ Host name
-

**Table 306** VMware Operations (/oper/virt/vmware) (continued)

---

**Command Syntax and Usage**

---

**export** *<VM profile name>* *<VMware host ID (one per line, 'null' to end)>*  
*<Virtual Switch name>*

Exports a VM Profile to one or more VMware hosts. This command allows you to distribute a VM Profile to VMware hosts.

Use one of the following identifiers to specify each host:

- ☐ UUID
- ☐ IP address
- ☐ Host name

The switch displays a list of available Virtual Switches. You may enter a VSwitch name from the list, or enter a new name to create a new Virtual Switch.

---

**scan**

Performs a scan of the VM Agent, and updates VM information.

---

**vmacpg** *<VNIC MAC address>* *<Port Group name>*

Changes a VNIC's configured Port Group.

---

**updp** *<Port Group name>* *<host ID>* *<VLAN number>* [*<shaping enabled>*  
*<average (1-1000000)>* *<burst (1-1000000)>* *<peak (1-1000000)>*]

Updates a VMware host's Port Group parameters. Use one of the following identifiers for the host ID:

- ☐ UUID
- ☐ IP address
- ☐ Host name

Enter the traffic shaping parameters as follows:

- ☐ Shaping enabled
  - ☐ Average traffic, in Kilobits per second
  - ☐ Maximum burst size, in Kilobytes
  - ☐ Peak traffic, in Kilobits per second
  - ☐ Delete traffic shaping parameters.
-



## CHAPTER 8

# The Boot Options Menu

---

To use the Boot Options Menu, you must be logged in to the switch as the administrator. The Boot Options Menu provides options for:

- Selecting a switch software image to be used when the switch is next reset
- Selecting a configuration block to be used when the switch is next reset
- Downloading or uploading a new software image to the switch via FTP/TFTP

In addition to the Boot Menu, you can use a Web browser or SNMP to work with switch image and configuration files. To use SNMP, refer to [“Switch Images and Configuration Files” on page 556](#).

### /boot

## Boot Menu

---

```
[Boot Options Menu]
bm          - Bridge Module Menu
stack       - Stacking Menu
sched       - Scheduled Switch Reset Menu
image       - Select software image to use on next boot
conf        - Select config block to use on next boot
netboot     - NetBoot and NetConfig menu
mode        - Select CLI mode to use on next boot
prompt      - Prompt for selectable boot mode
gtimg       - Download new software image via TFTP
ptimg       - Upload selected software image via TFTP
reset       - Reset switch [WARNING: Restarts Spanning Tree]
cur         - Display current boot options
```

Each of these options is discussed in greater detail in the following sections.

`/boot/bm <bridge module number>`  
**Bridge Module Menu**

```
[Bridge Module 4 Menu]
    bandw    - Select bandwidth to the bridge module
    ena      - Enable connection to bridge module
    dis      - Disable connection to bridge module
    cur      - Display current bridge module configuration
```

Use these commands to configure connectivity between the VFSM and the BladeCenter’s Fibre Channel Bridge Module. For more information about Bridge Module connections, see the *Application Guide*.

Two Bridge Module connections are available, depending on the switch location, as follows:

■ BCH chassis

HSSM Bay 7	HSSM Bay 8	HSSM Bay 9	HSSM Bay 10
BM Bay 5	BM Bay 4	BM Bay 3	BM Bay 6
BM Bay 3	BM Bay 6	BM Bay 5	BM Bay 4

■ BCHT chassis

HSSM Bay 7	HSSM Bay 8	HSSM Bay 9	HSSM Bay 10
BM Bay 3	BM Bay 1	BM Bay 4	BM Bay 2
BM Bay 4	BM Bay 2	BM Bay 3	BM Bay 1



Table 307 Bridge Module menu options (/boot/bm)

Command Syntax and Usage	
<b>bandw 0   20   40</b>	<p>Configures the bandwidth for the selected Bridge Module, in Gigabits per second.</p> <p><b>Note:</b> Each connection to the Bridge Module requires the use of multiple 10Gb external switch ports (EXTx), as follows:</p> <ul style="list-style-type: none"><li>□ 20Gb = 2 ports</li><li>□ 40Gb = 4 ports</li></ul>
<b>ena</b>	<p>Enables the connection to the selected Bridge Module.</p>
<b>dis</b>	<p>Disables the connection to the selected Bridge Module.</p>
<b>cur</b>	<p>Displays the current Bridge Module configuration.</p>

/boot/stack

## Stacking Boot Menu

```
[Boot Stacking Menu]
mode      - Set the stacking mode for the switch
stktrnk   - Set external 10G ports for Stack Trunks
vlan      - Set VLAN number for control communication
clear     - Set stacking parameters to factory default
pushimg   - Push image to a switch in the stack
ena       - Enable the stacking mode
dis       - Disable the stacking mode
cur       - Display current stacking boot parameters
```

The Stacking Boot menu is used to define the role of the switch in a stack: either as the Master that controls the stack, or as a participating Member switch. Options are available for loading stack software to individual Member switches, and to configure the VLAN that is reserved for inter-switch stacking communications.

You must enable Stacking and reset the switch to enter Stacking mode. When the switch enters Stacking mode, the Stacking configuration menu appears. For more information, see “[Stacking Configuration Menu](#)” on page 291.

Table 308 lists the Boot Stacking command options.

Table 308 Boot Stacking Options (/boot/stack)

Command Syntax and Usage	
<b>mode master member</b>	Configures the Stacking mode for the selected switch.
<b>stktrnk</b> <list of ports>	Configures the ports used to connect the switch to the stack. Enter only 10Gb external ports .
<b>vlan</b> <VLAN number>	Configures the VLAN used for Stacking control communication.
<b>clear</b>	Resets the Stacking boot parameters to their default values.
<b>pushimg image1 image2 boot</b>	Pushes the selected software file from the master to the selected switch.
<b>ena</b>	Enables the switch stack.
<b>dis</b>	Disables the switch stack.
<b>cur</b>	Displays current Stacking boot parameters.

When in stacking mode, the following stand-alone features are not supported:

- Active Multi-Path Protocol (AMP)
- SFD
- sFlow port monitoring
- Uni-Directional Link Detection (UDLD)
- Port flood blocking
- BCM rate control
- Link Layer Detection Protocol (LLDP)

- Private VLANs
- RIP
- OSPF and OSPFv3
- IPv6
- Virtual Router Redundancy Protocol (VRRP)
- Loopback Interfaces
- Router IDs
- Route maps
- Border Gateway Protocol (BGP)
- MAC address notification
- Static MAC address adding
- Static multicast
- Static routes
- Converged Enhanced Ethernet (CEE) and Fibre Channel over Ethernet (FCOE)
- MSTP and RSTP settings for CIST, Name, Rev, and Maxhop
- IGMP Relay and IGMPv3
- Virtual NICs

Switch menus and commands for unsupported features may be unavailable, or may have no effect on switch operation.

/boot/sched

## Scheduled Reboot Menu

```
[Boot Schedule Menu]
set          - Set switch reset time
cancel      - Cancel pending switch reset
cur         - Display current switch reset schedule
```

This feature allows you to schedule a reboot to occur at a particular time in the future. This feature is particularly helpful if the user needs to perform switch upgrades during off-peak hours. You can set the reboot time, cancel a previously scheduled reboot, and check the time of the currently set reboot schedule.

**Table 309** Boot Scheduling Options (/boot/sched)

Command Syntax and Usage	
<b>set</b>	Defines the reboot schedule. Follow the prompts to configure schedule options.
<b>cancel</b>	Cancels the next pending scheduled reboot.
<b>cur</b>	Displays the current reboot scheduling parameters.

/boot/netboot

## Netboot Configuration Menu

```
[Netboot configuration Menu]
  ena      - Enable netconfig
  dis      - Disable netconfig
  tftpaddr - TFTP Server IP address
  cfgfile  - Location of config file on tftp server
  cur      - Display current configuration
```

Netboot allows the switch to automatically download its configuration file over the network during switch reboot, and apply the new configuration. Upon reboot, the switch includes the following options in its DHCP requests:

- Option 66 (TFTP server address)
- Option 67 (file path)

If the DHCP server returns the information, the switch initiates a TFTP file transfer, and loads the configuration file into the active configuration block. As the switch boots up, it applies the new configuration file. Note that the option 66 TFTP server address must be specified in IP-address format (host name is not supported).

If DHCP is not enabled, or the DHCP server does not return the required information, the switch uses the manually-configured TFTP server address and file path.

**Table 310** Netboot Options (/boot/netboot)

---

**Command Syntax and Usage**

---

**ena**

Enables Netboot. When enabled, the switch boots into factory-default configuration, and attempts to download a new configuration file.

**dis**

Disables Netboot.

**tftpaddr** <IP address>

Configures the IP address of the TFTP server used for manual configuration. This server is used if DHCP is not enabled, or if the DHCP server does not return the required information.

---

Table 310 Netboot Options (/boot/netboot)

Command Syntax and Usage	
<b>cfgfile</b> <1-31 characters>	Defines the file path for the configuration file on the TFTP server. For example:  /directory/sub/config.cfg
<b>cur</b>	Displays the current Netboot parameters.

## Updating the Switch Software Image

---

The switch software image is the executable code running on the Virtual Fabric 10Gb Switch Module (VFSM). A version of the image ships with the switch, and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your switch. To get the latest version of software available for your VFSM, go to:

<http://www-304.ibm.com/jct01004c/systems/support>

On the support site, click on **software updates**. On the switch, use the `/boot/cur` command to determine the current software version.

The typical upgrade process for the software image consists of the following steps:

- Place the new image onto a FTP or TFTP server on your network, or on a local computer.
- Transfer the new image to your switch.
- Select the new software image to be loaded into switch memory the next time the switch is reset.

## Loading New Software to Your Switch

The switch can store up to two different software images, called `image1` and `image2`, as well as boot software, called `boot`. When you load new software, you must specify where it should be placed: either into `image1`, `image2`, or `boot`.

For example, if your active image is currently loaded into `image1`, you would probably load the new image software into `image2`. This lets you test the new software and reload the original active image (stored in `image1`), if needed.

## Using the BBI

You can use the Browser-Based Interface to load software onto the VFSM. The software image to load can reside in one of the following locations:

- FTP server
- TFTP server
- Local computer

After you log onto the BBI, perform the following steps to load a software image:

1. Click the **Configure** context button in the toolbar.
2. In the Navigation Window, select **System > Config/Image Control**.

The Switch Image and Configuration Management page appears.

Switch Image and Configuration Management									
Image 1 Version	version 6.3.0, downloaded 0:45:39 Thu Mar 2, 2010 NormalConnect								
Image 2 Version	version 6.1.1, downloaded 0:41:27 Thu Mar 2, 2010 NormalConnect								
Boot Version	version 6.3.0								
Active Image Version	6.3.0								
Next Boot Image Selection	image 1 ▾								
<table border="1"> <tr> <td>Active Configuration Block</td> <td>factory config</td> </tr> <tr> <td>Next Boot Configuration Block Selection</td> <td>factory config ▾</td> </tr> <tr> <td>Next CLI Boot Mode Selection</td> <td>BLADEOS CLI ▾</td> </tr> <tr> <td>Prompt for selectable boot mode</td> <td>ENABLE ▾</td> </tr> </table>		Active Configuration Block	factory config	Next Boot Configuration Block Selection	factory config ▾	Next CLI Boot Mode Selection	BLADEOS CLI ▾	Prompt for selectable boot mode	ENABLE ▾
Active Configuration Block	factory config								
Next Boot Configuration Block Selection	factory config ▾								
Next CLI Boot Mode Selection	BLADEOS CLI ▾								
Prompt for selectable boot mode	ENABLE ▾								
<table border="1"> <tr> <td>NetBoot</td> <td></td> </tr> <tr> <td>NetConfig for next boot</td> <td>DISABLE ▾</td> </tr> <tr> <td>TFTP IP Address</td> <td>10.10.20.1</td> </tr> <tr> <td>Config file</td> <td></td> </tr> </table>		NetBoot		NetConfig for next boot	DISABLE ▾	TFTP IP Address	10.10.20.1	Config file	
NetBoot									
NetConfig for next boot	DISABLE ▾								
TFTP IP Address	10.10.20.1								
Config file									
<table border="1"> <tr> <td colspan="2"><b>FTP/TFTP Settings</b></td> </tr> <tr> <td>Hostname or IP Address of FTP/TFTP server</td> <td></td> </tr> <tr> <td>Username for FTP Server or Blank for TFTP Server</td> <td></td> </tr> <tr> <td>Password for FTP Server</td> <td></td> </tr> </table>		<b>FTP/TFTP Settings</b>		Hostname or IP Address of FTP/TFTP server		Username for FTP Server or Blank for TFTP Server		Password for FTP Server	
<b>FTP/TFTP Settings</b>									
Hostname or IP Address of FTP/TFTP server									
Username for FTP Server or Blank for TFTP Server									
Password for FTP Server									
<table border="1"> <tr> <td colspan="2"><b>Image Settings</b></td> </tr> <tr> <td>Image for Transfer</td> <td>image 1 ▾</td> </tr> <tr> <td>Image Filename (on server)</td> <td>6.3.0_os.img</td> </tr> <tr> <td>Image Filename (on HTTP Client)</td> <td></td> </tr> </table>		<b>Image Settings</b>		Image for Transfer	image 1 ▾	Image Filename (on server)	6.3.0_os.img	Image Filename (on HTTP Client)	
<b>Image Settings</b>									
Image for Transfer	image 1 ▾								
Image Filename (on server)	6.3.0_os.img								
Image Filename (on HTTP Client)									
<div> <div>Get Image</div> <div>Put Image</div> </div> <div> <div>Browse...</div> <div>Download via Browser</div> </div>									

- If you are loading software from your computer (HTTP client), go to [Step 4](#).

If you are loading software from a FTP/TFTP server, enter the server's information in the FTP/TFTP Settings section.



4. In the Image Settings section, select the image version you want to replace (Image for Transfer).
  - If you are loading software from a FTP/TFTP server, enter the file name and click **Get Image**.
  - If you are loading software from your computer, click **Browse**.  
In the File Upload Dialog, select the file and click **OK**.  
Click **Download via Browser**.

Once the image has loaded, the page refreshes to show the new software.

## Using the CLI

To load a new software image to your switch, you need the following:

- The image or boot software loaded on a FTP/TFTP server on your network
- The hostname or IPv4/IPv6 address of the FTP/TFTP server
- The name of the new software image or boot file

---

**Note** – The DNS parameters must be configured if specifying hostnames. See [“Domain Name System Configuration Menu” on page 413](#).

---

When the above requirements are met, use the following procedure to download the new software to your switch.

1. At the `Boot Options#` prompt, enter:

```
Boot Options# gting
```

2. Enter the name of the switch software to be replaced:

```
Enter name of switch software image to be replaced  
["image1"/"image2"/"boot"]: <image>
```

3. Enter the hostname or IPv4/IPv6 address of the FTP or TFTP server.

```
Enter hostname or IP address of FTP/TFTP server: <name or IP address>
```

4. Enter the name of the new software file on the server.

```
Enter name of file on FTP/TFTP server: <filename>
```

The exact form of the name will vary by server. However, the file location is normally relative to the FTP or TFTP directory (usually `/tftpboot`).

5. Enter your username for the server, if applicable.

```
Enter username for FTP server or hit return for TFTP server: <username>  
or <Enter>
```

6. The system prompts you to confirm your request.

You should next select a software image to run, as described below.

## Selecting a Software Image to Run

You can select which software image (image1 or image2) you want to run in switch memory for the next reboot.

1. At the `Boot Options#` prompt, enter:

```
Boot Options# image
```

2. Enter the name of the image you want the switch to use upon the next boot.

The system informs you of which image is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use switch software "image1" on next reset.  
Specify new image to use on next reset ["image1"/"image2"]:
```

## Uploading a Software Image from Your Switch

You can upload a software image from the switch to a FTP or TFTP server.

1. At the `Boot Options#` prompt, enter:

```
Boot Options# ptimg
```

2. The system prompts you for information. Enter the desired image:

```
Enter name of switch software image to be uploaded  
["image1"|"image2"|"boot"]: <image>
```

3. Enter the name or the IPv4/IPv6 address of the FTP or TFTP server:

```
Enter hostname or IP address of FTP/TFTP server: <name or IP address>
```

4. Enter the name of the file into which the image will be uploaded on the FTP or TFTP server:

```
Enter name of file on FTP/TFTP server: <filename>
```

5. The system then requests confirmation of what you have entered. To have the file uploaded, enter **y**.

```
image2 currently contains Software Version 6.3
that was downloaded at 0:23:39 Thu Jan  4, 2010.
Upload will transfer image2 (2788535 bytes) to file "image1"
on FTP/TFTP server 192.1.1.1.
Confirm upload operation (y/n) ? y
```

## Selecting a Configuration Block

When you make configuration changes to the VFSM, you must save the changes so that they are retained beyond the next time the switch is reset. When you perform the `save` command, your new configuration changes are placed in the *active* configuration block. The previous configuration is copied into the *backup* configuration block.

There is also a *factory* configuration block. This holds the default configuration set by the factory when your VFSM was manufactured. Under certain circumstances, it may be desirable to reset the switch configuration to the default. This can be useful when a custom-configured VFSM is moved to a network environment where it will be re-configured for a different purpose.

---

**Note** – You also can use Netboot to automatically download a configuration file when the switch reboots. For more details, see [“Netboot Configuration Menu” on page 497](#).

---

Use the following procedure to set which configuration block you want the switch to load the next time it is reset:

1. At the `Boot Options#` prompt, enter:

```
Boot Options# conf
```

2. Enter the name of the configuration block you want the switch to use:

The system informs you of which configuration block is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use active configuration block on next reset.  
Specify new block to use ["active"/"backup"/"factory"]:
```

## Resetting the Switch

---

You can reset the switch to make your software image file and configuration block changes occur.

**Note** – Resetting the switch causes the Spanning Tree Group to restart. This process can be lengthy, depending on the topology of your network.

---

To reset the switch, at the `Boot Options#` prompt, enter:

```
>> Boot Options# reset
```

You are prompted to confirm your request.

## Accessing the ISCLI

---

The default command-line interface for the VFSM is the BLADEOS CLI. To access the ISCLI, enter the following command and reset the VFSM:

```
Main# boot/mode iscli
```

To access the BLADEOS CLI, enter the following command from the ISCLI and reload the VFSM:

```
Switch (config)# boot cli-mode bladeos-cli
```

Users can select the CLI mode upon login, if the `/boot/prompt` command is enabled. Only an administrator can view and enable `/boot/prompt`. When `/boot/prompt` is enabled, the first user to log in can select the CLI mode. Subsequent users must use the selected CLI mode, until all users have logged out.

## Using the Boot Management Menu

The Boot Management menu allows you to switch the software image, reset the switch to factory defaults, or to recover from a failed software download.

You can interrupt the boot process and enter the Boot Management menu from the serial console port. When the system displays Memory Test, press **<Shift B>**. The Boot Management menu appears.

```
Resetting the System ...
Memory Test .....

Boot Management Menu
1 - Change booting image
2 - Change configuration block
3 - Xmodem download
4 - Exit

Please choose your menu option: 1
Current boot image is 1. Enter image to boot: 1 or 2: 2
Booting from image 2
```

The Boot Management menu allows you to perform the following actions:

- To change the booting image, press 1 and follow the screen prompts.
- To change the configuration block, press 2, and follow the screen prompts.
- To perform an Xmodem download, press 3 and follow the screen prompts.
- To exit the Boot Management menu, press 4. The booting process continues.

## Recovering from a Failed Upgrade

Use the following procedure to recover from a failed software upgrade.

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports XModem Download (for example, HyperTerminal, CRT, PuTTY) and select the following serial port characteristics:
  - Speed: 9600 bps
  - Data Bits: 8
  - Stop Bits: 1
  - Parity: None
  - Flow Control: None

3. Boot the switch and access the Boot Management menu by pressing <Shift B> while the Memory Test is in progress and the dots are being displayed.
4. Select 3 for Xmodem download. When you see the following message, change the Serial Port characteristics to 115200 bps:

```
## Switch baudrate to 115200 bps and press ENTER ...
```

5. Press <Enter> to set the system into download accept mode. When the readiness meter displays (a series of “C” characters), start XModem on your terminal emulator.
6. Select the Boot Image to download. The XModem initiates the file transfer. When the download is complete, a message similar to the following is displayed:

```
yzModem - CRC mode, 62494(SOH)/0(STX)/0(CAN) packets, 6 retries

Extracting images ... Do *NOT* power cycle the switch.

**** VMLINUX ****

Un-Protected 10 sectors

Erasing Flash..... done

Writing to Flash.....done

Protected 10 sectors

**** RAMDISK ****

Un-Protected 44 sectors

Erasing Flash..... done

Writing to Flash.....done

Protected 44 sectors

**** BOOT CODE ****

Un-Protected 8 sectors

Erasing Flash..... done

Writing to Flash.....done

Protected 8 sectors
```

7. When you see the following message, change the Serial Port characteristics to 9600 bps:

```
## Switch baudrate to 9600 bps and press ESC ...
```

8. Press the Escape key (<Esc>) to re-display the Boot Management menu.
9. Select 3 to start a new XModem Download. When you see the following message, change the Serial Port characteristics to 115200 bps:

```
## Switch baudrate to 115200 bps and press ENTER ...
```

10. Press <Enter> to continue the download.
11. Select the OS Image to download. The XModem initiates the file transfer. When the download is complete, a message similar to the following is displayed:

```
yzModem - CRC mode, 27186(SOH)/0(STX)/0(CAN) packets, 6 retries
Extracting images ... Do *NOT* power cycle the switch.

**** Switch OS ****

Please choose the Switch OS Image to upgrade [1|2|n] :
```

12. Select the image number to load the new image (1 or 2). It is recommended that you select 1. A message similar to the following is displayed:

```
Switch OS Image 1 ...

Un-Protected 27 sectors

Erasing Flash..... done

Writing to Flash.....done

Protected 27 sectors
```

13. When you see the following message, change the Serial Port characteristics to 9600 bps:

```
## Switch baudrate to 9600 bps and press ESC ...
```

14. Press the Escape key (<Esc>) to re-display the Boot Management menu.

Select 4 to exit and boot the new image.





## CHAPTER 9

# The Maintenance Menu

---

The Maintenance Menu is used to manage dump information and forward database information. It also includes a debugging menu to help with troubleshooting.

`/maint`

## Maintenance Menu

---

**Note** – To use the Maintenance Menu, you must be logged in to the switch as the administrator.

---

```
[Maintenance Menu]
  sys      - System Maintenance Menu
  fdb      - Forwarding Database Manipulation Menu
  debug    - Debugging Menu
  lldp     - LLDP Cache Manipulation Menu
  arp      - ARP Cache Manipulation Menu
  route    - IP Route Manipulation Menu
  igmp     - IGMP Multicast Group Menu
  nbrcache - IP6 NBR Cache Manipulation Menu
  route6   - IP6 Route Manipulation Menu
  uudmp    - Uuencode FLASH dump
  ptdmp    - Upload FLASH dump via FTP/TFTP
  ptlog    - Upload file via TFTP
  cldmp    - Clear FLASH dump
  tsdmp    - Tech support dump
  pttsdmp  - Upload tech support dump via FTP/TFTP
```

Dump information contains internal switch state data that is written to flash memory on the Virtual Fabric 10Gb Switch Module (VFSM) after any one of the following occurs:

- The watchdog timer forces a switch reset. The purpose of the watchdog timer is to reboot the switch if the switch software freezes.
- The switch detects a hardware or software problem that requires a reboot.

**Table 311** Maintenance Menu (/maint)**Command Syntax and Usage****sys**

Displays the System Maintenance Menu. To view menu options, see [page 511](#).

**fdb**

Displays the Forwarding Database Manipulation Menu. To view menu options, see [page 512](#).

**debug**

Displays the Debugging Menu. To view menu options, see [page 513](#).

**lldp**

Displays the LLDP Cache Manipulation Menu. To view menu options, see [page 514](#).

**arp**

Displays the ARP Cache Manipulation Menu. To view menu options, see [page 515](#).

**route**

Displays the IP Route Manipulation Menu. To view menu options, see [page 516](#).

**igmp**

Displays the IGMP Maintenance Menu. To view menu options, see [page 517](#).

**nbrcache**

Displays the IPv6 Neighbor Cache Manipulation Menu. To view menu options, see [page 520](#).

**route6**

Displays the IPv6 Route Manipulation Menu. To view menu options, see [page 521](#).

**uudmp**

Displays dump information in uuencoded format. For details, see [page 522](#).

**ptdmp** <host name> <file name>

Saves the system dump information via TFTP. For details, see [page 522](#).

**ptlog**

Saves the system log file (SYSLOG) via TFTP.

Table 311 Maintenance Menu (/maint)

Command Syntax and Usage
<b>cltmp</b> Clears dump information from flash memory. For details, see <a href="#">page 523</a> .
<b>tsdump</b> Dumps all VFSM information, statistics, and configuration. You can log the tsdump output into a file.
<b>pttsdump</b> Redirects the technical support dump (tsdump) to an external TFTP server.

/maint/sys

## System Maintenance Menu

This menu is reserved for use by IBM Service Support. The options are used to perform system debugging.

[System Maintenance Menu]
flags     - Set NVRAM flag word
tmask    - Set MP trace mask word

Table 312 System Maintenance Menu Options (/maint/sys)

Command Syntax and Usage
<b>flags</b> <new NVRAM flags word as 0xFFFFFFFF> This command sets the flags that are used for debugging purposes by Technical Support personnel.
<b>tmask</b> <new trace mask word as 0xFFFFFFFF> [p] This command sets the trace mask that is used for debugging purposes by Technical Support personnel.

/maint/fdb

# Forwarding Database Maintenance Menu

[FDB Manipulation Menu]

find

- Show a single FDB entry by MAC address

port

- Show FDB entries for a single port

vlan

- Show FDB entries for a single VLAN

dump

- Show all FDB entries

del

- Delete an FDB entry

clear

- Clear entire FDB

mcdump

- Display all Multicast MAC entries added

mcreload

- Reload all Multicast MAC entries

The Forwarding Database Manipulation Menu can be used to view information and to delete a MAC address from the forwarding database or clear the entire forwarding database. This is helpful in identifying problems associated with MAC address learning and packet forwarding decisions.

**Table 313** FDB Manipulation Menu Options (/maint/fdb)

Command Syntax and Usage

**find** <MAC address> [*<VLAN number>*]

Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using one of the following formats:

- ☐ xx:xx:xx:xx:xx:xx (such as 08:00:20:12:34:56)
- ☐ xxxxxxxxxxxx (such as 080020123456)

**port** *<port alias or number>*

Displays all FDB entries for a particular port.

**vlan** *<VLAN number>*

Displays all FDB entries on a single VLAN.

**dump**

Displays all entries in the Forwarding Database. For details, see [page 77](#).

**del** <MAC address> [*<VLAN number>*]

Removes a single FDB entry.

**clear**

Clears the entire Forwarding Database from switch memory.

Table 313 FDB Manipulation Menu Options (/maint/fdb)

Command Syntax and Usage

**mcdump**

Displays all Multicast MAC entries in the FDB.

**mcreload**

Reloads static Multicast MAC entries.

/maint/debug  
**Debugging Menu**

```
[Miscellaneous Debug Menu]
tbuf      - Show MP trace buffer
snap      - Show MP snap (or post-mortem) trace buffer
clrcfg    - Clear all flash configs
```

The Miscellaneous Debug Menu displays trace buffer information about events that can be helpful in understanding switch operation. You can view the following information using the debug menu:

- Events traced by the Management Processor (MP)
- Events traced to a buffer area when a reset occurs

If the switch resets for any reason, the MP trace buffer is saved into the snap trace buffer area. The output from these commands can be interpreted by Service Support personnel.

Table 314 Miscellaneous Debug Menu Options (/maint/debug)

Command Syntax and Usage

**tbuf**

Displays the Management Processor trace buffer. Header information similar to the following is shown:

MP trace buffer at 13:28:15 Fri May 30, 2008; mask: 0x2ffdf748

The buffer information is displayed after the header.

**snap**

Displays the Management Processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reset occurred.

**clrcfg**

Deletes all flash configuration blocks.

/maint/lldp

# LLDP Cache Manipulation Menu

[LLDP Menu]	
port	- Show LLDP port information
rx	- Show LLDP receive state machine information
tx	- Show LLDP transmit state machine information
remodev	- Show LLDP remote devices information
dump	- Show all LLDP information
clear	- Clear LLDP remote devices information

Table 320 describes the LLDP cache manipulation commands.

Table 315 LLDP Cache Manipulation Options (/maint/lldp)

Command Syntax and Usage

**port** <port alias or number>

Displays Link Layer Discovery Protocol (LLDP) port information.

**rx**

Displays information about the LLDP receive state machine.

**tx**

Displays information about the LLDP transmit state machine.

**remodev** <1-256>

Displays information received from LLDP -capable devices.

**dump**

Displays all LLDP information.

**clear**

Clears the LLDP cache.

/maint/arp

# ARP Cache Maintenance Menu

[Address Resolution Protocol Menu]

find	- Show a single ARP entry by IP address
port	- Show ARP entries on a single port
vlan	- Show ARP entries on a single VLAN
addr	- Show ARP entries for switch's interfaces
dump	- Show all ARP entries
clear	- Clear ARP cache

**Table 316** ARP Maintenance Menu Options (/maint/arp)

**Command Syntax and Usage**

**find** <IP address (such as, 192.4.17.101)>

Shows a single ARP entry by IP address.

**port** <port alias or number>

Shows ARP entries on a single port.

**vlan** <VLAN number>

Shows ARP entries on a single VLAN.

**addr**

Shows the list of IP addresses which the switch will respond to for ARP requests.

**dump**

Shows all ARP entries.

**clear**

Clears the entire ARP list from switch memory.

**Note** – To display all ARP entries currently held in the switch, or a portion according to one of the options listed on the menu above (find, port, vlan, dump), you can also refer to “ARP Information” on [page 104](#).

/maint/route

# IP Route Manipulation Menu

[IP Routing Menu]	
find	- Show a single route by destination IP address
gw	- Show routes to a single gateway
type	- Show routes of a single type
tag	- Show routes of a single tag
if	- Show routes on a single interface
dump	- Show all routes
clear	- Clear route table

**Table 317** IP Route Manipulation Menu Options (/maint/route)

**Command Syntax and Usage**

**find** *<IP address (such as, 192.4.17.101)>*

Shows a single route by destination IP address.

**gw** *<default gateway address (such as, 192.4.17.44)>*

Shows routes to a default gateway.

**type** **indirect** | **direct** | **local** | **broadcast** | **martian** | **multicast**

Shows routes of a single type. For a description of IP routing types, see [Table 34 on page 102](#)

**tag** **fixed** | **static** | **addr** | **rip** | **ospf** | **bgp** | **broadcast** | **martian** | **multicast**

Shows routes of a single tag. For a description of IP routing tags, see [Table 35 on page 103](#)

**if** *<interface number>*

Shows routes on a single interface.

**dump**

Shows all routes.

**clear**

Clears the route table from switch memory.

**Note** – To display all routes, you can also refer to “IP Routing Information” on [page 101](#).



/maint/igmp

# IGMP Maintenance Menu

---

[IGMP Multicast Group Menu]

group - Multicast Group Menu

mrouter - IGMP Multicast Router Port Menu

clear - Clear group and mrouter tables

Table 318 describes the IGMP Maintenance commands.

Table 318 IGMP Maintenance Menu Options (/maint/igmp)

---

Command Syntax and Usage

---

**group**

Displays the Multicast Group menu. To view menu options, see [page 518](#).

---

**mrouter**

Displays the Multicast Router Port menu. To view menu options, see [page 517](#).

---

**clear**

Clears the IGMP group table and Mrouter tables.

---

/maint/igmp/group  
IGMP Group Maintenance Menu

[IGMP Multicast Group Menu]	
find	- Show a single group by IP group address
vlan	- Show groups on a single vlan
port	- Show groups on a single port
trunk	- Show groups on a single trunk
detail	- Show detail of a single group by IP address
dump	- Show all groups
clear	- Clear group tables

Table 318 describes the IGMP Maintenance commands.

Table 319 IGMP Multicast Group Maintenance Menu Options  
(/maint/igmp/group)

Command Syntax and Usage

**find** <IP address>

Displays a single IGMP multicast group by its IP address.

**vlan** <VLAN number>

Displays all IGMP multicast groups on a single VLAN.

**port** <port number or alias>

Displays all IGMP multicast groups on a single port.

**trunk** <trunk number>

Displays all IGMP multicast groups on a single trunk group.

**detail** <IP address>

Displays detailed information about a single IGMP multicast group.

**dump**

Displays information for all multicast groups.

**clear**

Clears the IGMP group tables.

/maint/igmp/mrouter  
IGMP Multicast Routers Maintenance Menu

[IGMP Multicast Routers Menu]

vlan

- Show all multicast router ports on a single vlan

dump

- Show all multicast router ports

clear

- Clear multicast router port table

Table 320 describes the IGMP multicast router (Mrouter) maintenance commands.

Table 320 IGMP Mrouter Maintenance Menu Options (/maint/igmp/mrouter)

Command Syntax and Usage

**vlan** <VLAN number>

Shows all IGMP multicast router ports on a single VLAN.

**dump**

Shows all multicast router ports.

**clear**

Clears the IGMP Multicast Router port table.

/maint/nbrcache

# IPv6 Neighbor Discovery Cache Manipulation

[Neighbor Cache Manipulation Menu]  
find - Show a single NBR Cache entry by IP address  
port - Show NBR Cache entries on a single port  
vlan - Show NBR Cache entries on a single VLAN  
dump - Show all NBR Cache entries  
clear - Clear neighbor cache

Table 321 describes the IPv6 Neighbor Discovery cache manipulation options.

Table 321 IPv6 Neighbor Discovery Cache Manipulation (/maint/nbrcache)

Command Syntax and Usage

**find** <IPv6 address>

Shows a single IPv6 Neighbor Discovery cache entry by IP address.

**port** <port alias or number>

Shows IPv6 Neighbor Discovery cache entries on a single port.

**vlan** <VLAN number>

Shows IPv6 Neighbor Discovery cache entries on a single VLAN.

**dump**

Shows all IPv6 Neighbor Discovery cache entries.

**clear**

Clears all IPv6 Neighbor Discovery cache entries from switch memory.

/maint/route6

# IPv6 Route Manipulation Menu

---

```
[IP6 Routing Menu]
dump      - Show all routes
clear     - Clear route table
```

Table 322 describes the IPv6 Route maintenance options.

Table 322 IPv6 Route Manipulation (/maint/route6)

---

Command Syntax and Usage

---

**dump**

Shows all IPv6 routes.

---

**clear**

Clears all IPv6 routes from switch memory.

---

## /maint/uudmp

# Uuencode Flash Dump

---

Using this command, dump information is presented in uuencoded format. This format makes it easy to capture the dump information as a file or a string of characters.

If you want to capture dump information to a file, set your communication software on your workstation to capture session data prior to issuing the `uudmp` command. This will ensure that you do not lose any information. Once entered, the `uudmp` command will cause approximately 23,300 lines of data to be displayed on your screen and copied into the file.

Using the `uudmp` command, dump information can be read multiple times. The command does not cause the information to be updated or cleared from flash memory.

---

**Note** – Dump information is not cleared automatically. In order for any subsequent dump information to be written to flash memory, you must manually clear the dump region. For more information on clearing the dump region, see [page 523](#).

---

To access dump information, at the `Maintenance#` prompt, enter:

```
Maintenance# uudmp
```

The dump information is displayed on your screen and, if you have configured your communication software to do so, captured to a file. If the dump region is empty, the following appears:

```
No FLASH dump available.
```

## /maint/ptdmp <FTP/TFTP server> <filename>

# FTP/TFTP System Dump Put

---

Use this command to `put` (save) the system dump to a FTP/TFTP server.

---

**Note** – If the FTP/TFTP server is running SunOS or the Solaris operating system, the specified `ptdmp` file must exist *prior* to executing the `ptdmp` command, and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current dump data.

---

To save dump information via FTP/TFTP, at the `Maintenance#` prompt, enter:

```
Maintenance# ptdmp <FTP/TFTP server> <filename>
```

Where *server* is the FTP/TFTP server IPv4/IPv6 address or hostname, and *filename* is the target dump file.

`/maint/cldmp`

## Clearing Dump Information

---

To clear dump information from flash memory, at the Maintenance# prompt, enter:

```
Maintenance# cldmp
```

The switch clears the dump region of flash memory and displays the following message:

```
FLASH dump region cleared.
```

If the flash dump region is already clear, the switch displays the following message:

```
FLASH dump region is already clear.
```

## Unscheduled System Dumps

---

If there is an unscheduled system dump to flash memory, the following message is displayed when you log on to the switch:

```
Note: A system dump exists in FLASH. The dump was saved
      at 13:43:22 Wednesday January 30, 2010. Use /maint/uudmp to
      extract the dump for analysis and /maint/cldmp to
      clear the FLASH region. The region must be cleared
      before another dump can be saved.
```





## APPENDIX A

# BLADEOS Syslog Messages

---

The following syntax is used when outputting syslog messages:

*<Time stamp><Log Label>BLADEOS<Thread ID> : <Message>*

The following parameters are used:

■ *<Timestamp>*

The time of the message event is displayed in the following format:

month day hour:minute:second

For example: Aug 19 14:20:30

■ *<Log Label>*

The following types of log messages are recorded: LOG\_CRIT, LOG\_WARNING, LOG\_ALERT, LOG\_ERR, LOG\_NOTICE, and LOG\_INFO

■ *<Thread ID>*

This is the software thread that reports the log message. For example:

stg, ip, console, telnet, vrrp, system, web server, ssh, bgp

■ *<Message>*: The log message

Following is a list of potential syslog messages. To keep this list as short as possible, only the *<Thread ID>* and *<Message>* are shown. The messages are sorted by *<Log Label>*.

Where the *<Thread ID>* is listed as mgmt, one of the following may be shown: console, telnet, web server, or ssh.

## LOG\_CRIT

Thread	LOG_CRIT Message
SSH	can't allocate memory in load_MP_INT()
SSH	currently not enough resource for loading RSA {private   public key}
SYSTEM	Failed to Read <SFP type> {ID   Voltage} for port {<port>   ???}
SYSTEM	Poll SFP/XFP Failed to get Status
SYSTEM	System memory is at <n> percent
SYSTEM	Temp back to normal
SYSTEM	TEMP CAUTION DETECTED
SYSTEM	Voltage (<voltage>) is OVER Range on port <port>

## LOG\_WARNING

Thread	LOG_WARNING Message
	Changing numcos sets up the default COSq configuration. Please see diff.
8021X	Authentication session terminated with {Failure   Success} on port <port>
8021X	Could not create failover checkpoint record for port <port>
8021X	Logoff request on port <port>
8021X	Port <port> {assigned to removed from} vlan <VLAN>
8021X	RADIUS server <IP address> auth response for port <port> has an invalid Tunnel-Type value (<tunnel type>); should be 13 for VLAN assignment
8021X	RADIUS server <IP address> auth response for port <port> has an invalid Tunnel-Medium-Type value (<tunnel type>); should be 6 for VLAN assignment
8021X	RADIUS server <IP address> auth response for port <port> is missing one or more tunneling attributes for VLAN assignment
8021X	RADIUS server <IP address> auth response has a VLAN id (<VLAN>) of a reserved VLAN and cannot be assigned to port <port>
8021X	RADIUS server <IP address> auth response has a VLAN id (<VLAN>) of a non-existent or disabled VLAN, and cannot be assigned to port <port>

Thread	LOG_WARNING Message (continued)
8021X	RADIUS server <IP address> auth response has an invalid VLAN id (<VLAN>) and cannot be assigned to port <port>
AMP	Access port <port> is receiving AMP packets from access switch <MAC address>
CFG	Authentication should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <interface>.
CFG	Multicast should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <interface>.
CFG	Switch cannot support more than 16 protocols simultaneously!
CFG	Unfit config exists when protocol-vlan apply.
DCBX	Feature "{DCBX   ETS   PFC   App Proto   VNIC   ETS}" not supported by peer on port <port>
HOTLINKS	"Error" is set to "Standby   Active"
HOTLINKS	"Learning" is set to "Standby   Active"
HOTLINKS	"None" is set to "Standby   Active"
HOTLINKS	"Side Max" is set to "Standby   Active"
HOTLINKS	has no "{Side Max   None   Learning   Error}" interface
IP	<IP address> configured as V<version> and received IGMP V{1   2} query
LLDP	ERROR!!! The request port item <item> is invalid
MGMT	Management Ports 1 and 2 DISABLED because Management Module 1 and 2 are BOTH IN-ACTIVE
NTP	cannot contact any NTP server
NTP	cannot contact [primary   secondary] NTP server <IP address>
STACK	no master present in the stack so far
STACK	The specified backup (<csnum>) is the current master - a specified master; no backup will be selected in this case
SYSTEM	<SFP type> removed at port <csnum>:<port>
SYSTEM	Failed to read status register
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]

Thread	LOG_WARNING Message (continued)
SYSTEM	Interface <interface> failed to renew DHCP Lease.
SYSTEM	Port EXT<n> is disabled due to Bridge configuration. Please remove device from this port.
SYSTEM	transceiver missing at port <port>
TEAMING	error, action is undefined
TEAMING	is down, but teardown is blocked
TEAMING	is down, control ports are auto disabled
TEAMING	is up, control ports are auto controlled
VNIC	Peer does not support VNIC on port <port>

## LOG\_ALERT

Thread	LOG_ALERT Message
	Possible buffer overrun attack detected!
AMP	Access port <port> is receiving AMP packets from aggregator switch <MAC address>
AMP	Access trunk <trunk ID> is receiving AMP packets from {access   aggregator} switch <MAC address>
AMP	Aggregator {port <port>   trunk <trunk ID>} is receiving AMP packets from access switch <MAC address>
AMP	AMP group <group> topology is DOWN
AMP	AMP keep-alive timeout on {port <port>   trunk <trunk ID>}
AMP	AMP packets looped back on {port <port>   trunk <trunk ID>}
AMP	Discarding BPDUs received on port <port> while AMP is enabled
AMP	Dropping AMP v<group> packets received on {port <port>   trunk <trunk ID>}, expecting v<AMP version>
AMP	Port <port> is disabled by AMP BPDU guard
AMP	Putting port <port> in blocking state
BGP	Invalid notification (Code:<code>, Subcode:<subcode>) received from <IP address>

Thread	LOG_ALERT Message (continued)
BGP	session with <IP address> failed (bad event:<event>)
BGP	<p>session with &lt;IP address&gt; failed &lt;reason&gt;</p> <p>Reasons:</p> <ul style="list-style-type: none"> <li>■ Connect Retry Expire</li> <li>■ Holdtime Expire</li> <li>■ Invalid</li> <li>■ Keepalive Expire</li> <li>■ Receive KEEPALIVE</li> <li>■ Receive NOTIFICATION</li> <li>■ Receive OPEN</li> <li>■ Receive UPDATE</li> <li>■ Start</li> <li>■ Stop</li> <li>■ Transport Conn Closed</li> <li>■ Transport Conn Failed</li> <li>■ Transport Conn Open</li> <li>■ Transport Fatal Error</li> </ul>
BGP	<p>session with &lt;IP address&gt; failed &lt;reason type&gt; : &lt;reason&gt;</p> <p>Reason Types:</p> <ul style="list-style-type: none"> <li>■ FSM Error</li> <li>■ Hold Timer Expired</li> <li>■ Message Header Error</li> <li>■ OPEN Message Error</li> <li>■ UPDATE Message Error</li> </ul> <p>Reasons:</p> <ul style="list-style-type: none"> <li>■ AS Routing Loop</li> <li>■ Attr Flags Error</li> <li>■ Attr Length Error</li> <li>■ Auth Failure</li> <li>■ Bad BGP Identifier</li> <li>■ Bad HoldTime</li> <li>■ Bad Length</li> <li>■ Bad Peer AS</li> <li>■ Bad Type</li> <li>■ Conn Not Synced</li> <li>■ Invalid Network Field</li> <li>■ Invalid NEXTHOP Attr</li> <li>■ Invalid ORIGIN Attr</li> <li>■ Malformed AS_PATH</li> <li>■ Malformed Attr List</li> <li>■ Missing Well Known Attr</li> <li>■ None</li> <li>■ Optional Attr Error</li> <li>■ Unrecognized Well Known Attr</li> <li>■ Unsupported Opt Param</li> <li>■ Unsupported Version</li> </ul>
HOTLINKS	LACP trunk <trunk ID> and <trunk ID> formed with admin key <key>
IP	cannot contact default gateway <IP address>
IP	Dynamic Routing table is full
IP	Route table full

Thread	LOG_ALERT Message (continued)
MGMT	Maximum number of login failures (<threshold>) has been exceeded.
OSPF	Interface IP <IP address>, Interface State {Down   Loopback   Waiting   P To P   DR   BackupDR   DR Other}: Interface down detached
OSPF	LS Database full: likely incorrect/missing routes or failed neighbors
OSPF	Neighbor Router ID <router ID>, Neighbor State {Down   Attempt   Init   2 Way   ExStart   Exchange   Loading   Full   Loopback   Waiting   P To P   DR   BackupDR   DR Other}
OSPF	OSPF Route table full: likely incorrect/missing routes
RMON	Event.<description>
STP	CIST new root bridge
STP	CIST topology change detected
STP	Fast Forward port <port> active, putting port into forwarding state
STP	New preferred Fast Uplink port <port> active for STG <STG>, {restarting   canceling} timer
STP	own BPDU received from port <port>
STP	Port <port>, putting port into blocking state
STP	Preferred STG <STG> Fast Uplink port has gone down. Putting secondary Fast Uplink port <port> into forwarding
STP	Setting STG <STG> Fast Uplink primary port <port> forwarding and backup port <port> blocking
STP	STG <STG> preferred Fast Uplink port <port> active. Waiting <seconds> seconds before switching from port <port>
STP	STG <STG>, new root bridge
STP	STG <STG>, topology change detected
STP	STG <STG> root port <port> has gone down. Putting backup Fast Uplink port <port> into forwarding
SYSTEM	<SFP type> incorrect device in port <port>. Device is DISABLED.
SYSTEM	<SFP type> inserted at port <port> is UNAPPROVED !

Thread	LOG_ALERT Message (continued)
SYSTEM	<SFP type> inserted at port <port> is UNAPPROVED ! {DAC   SFP   SFP+   XFP   ???} is DISABLED.
SYSTEM	Ingress PVST+ BPDU's spotted from port <port>
SYSTEM	LACP trunk <trunk ID> and <trunk ID> formed with admin key <key>
SYSTEM	Port <port> is configured for {1Gb   10Gb}. Installed {10Gb   1Gb} Device not supported with current config.
VRRP	Received <x> virtual routers instead of <y>
VRRP	received errored advertisement from <IP address>
VRRP	received incorrect addresses from <IP address>
VRRP	received incorrect advertisement interval <interval> from <IP address>
VRRP	received incorrect VRRP authentication type from <IP address>
VRRP	received incorrect VRRP password from <IP address>
VRRP	VRRP : received incorrect IP addresses list from <IP address>

## LOG\_ERR

Thread	LOG_ERR Message
CFG	Can't assign a port with same protocol to different VLANs.
CFG	Configuration file is EMPTY
CFG	Configuration is too large
CFG	Default VLAN cannot be a private-VLAN.
CFG	Error writing active config to FLASH! Another save is in progress
CFG	Error writing active config to FLASH! Configuration is too large
CFG	Error writing active config to FLASH! Unknown error
CFG	ERROR: Cannot enable/disable RMON for Mgmt Port <port>
CFG	Have not defined protocol type!
CFG	Management VLAN cannot be a private-VLAN.
CFG	Management VLAN cannot support protocols.

Thread	LOG_ERR Message (continued)
CFG	Maximum allowed number (30) of Alarm groups have already been created.
CFG	Maximum allowed number (30) of Event groups have already been created.
CFG	Maximum allowed number (5) of History groups have already been created.
CFG	Need to enable port's tag for tagging pvlan.
CFG	Overflow! Port has more than 16 protocols.
CFG	Port is not for this protocol.
CFG	Switch rem port fails when disable {protocol   vlan}.
CFG	TFTP {Copy cfgRcv} attempting to redirect a previously redirected output
DCBX	Duplicate DCBX Application Protocol Sub-TLV detected on port <port>
DCBX	Duplicate DCBX Control Sub-TLV detected on port <port>
DCBX	Duplicate DCBX PFC Sub-TLV detected on port <port>
DCBX	Duplicate DCBX PG Sub-TLV detected on port <port>
DCBX	Duplicate DCBX VNIC Sub-TLV detected on port <port>
DCBX	Multiple peers detected on port <port>
IP6	EXCEPTIONAL CASE Trying to create IP6 Interface after the Ip6Shutdown
IP6	Ip6SetAddr(failed):if=<interface>, addr <IPv6 address>, rc=<reason code>
IP6	IPv6 route table full
IP6	ipv6_add_interface_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_add_nbrcache_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_rem_route_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_vlan_change_immediate: Buffer Non Linear for ip6_cfa_params
LLDP	Port <port>: Cannot add new entry. MSAP database is full!
MGMT	Apply is issued by another user. Try later
MGMT	Attempting to add the Mgt Default Route with the Mgt IP Interface (<interface>) DISABLED.
MGMT	Critical Error failed to add Interface <interface>
MGMT	Critical Error failed to {add   attach} Loopback Interface <interface>



Thread	LOG_ERR Message (continued)
MGMT	Critical Error failed to detach Loopback Interface <i>&lt;interface&gt;</i> rc= <i>&lt;reason code&gt;</i>
MGMT	Diff is issued by another user. Try later
MGMT	Dump is issued by another user. Try later
MGMT	Error: Apply not done
MGMT	ERROR: Cannot enable {OSPF   OSPFv3} on Management interface.
MGMT	Error: Pushed {image1   image2} size <i>&lt;bytes&gt;</i> bigger than the capacity <i>&lt;maximum bytes&gt;</i> .
MGMT	Error: Invalid {image1   image2}
MGMT	Error: Pushed {image1   image2} size <i>&lt;bytes&gt;</i> bigger than the capacity <i>&lt;maximum bytes&gt;</i> .
MGMT	Error: Save not done.
MGMT	Firmware download failed (insufficient memory
MGMT	Invalid CRC value. Boot image rejected
MGMT	Revert Apply is issued by another user. Try later
MGMT	Revert is issued by another user. Try later.
MGMT	Save is issued by another user. Try later
MGMT	unapplied changes reverted
MGMT	VPD_IP_STATIC - add_address <i>&lt;IP address&gt;</i> failed
MGT	You are attempting to load an image that has been corrupted or belongs to another switch type. Please verify you have the correct file for this switch and try again. [Error: Invalid header magic value <i>&lt;value&gt;</i> .] Boot image rejected
NTP	unable to listen to NTP port
RMON	Maximum {Alarm   Event   History} groups exceeded when trying to add group <i>&lt;group&gt;</i> via SNMP
STACK	Boot Image could not be successfully received by <i>&lt;MAC adress&gt;</i> [. Resending it.]
STACK	Config File could not be successfully received by <i>&lt;MAC adress&gt;</i> [. Resending it.]
STACK	File <i>&lt;File ID&gt;</i> could not be successfully received by <i>&lt;MAC adress&gt;</i> [. Resending it.]
STACK	Image1   2 could not be successfully received by <i>&lt;MAC adress&gt;</i> [. Resending it.]

Thread	LOG_ERR Message (continued)
STACK	Incorrect xfer status: from <MAC address> for {Boot Image   Image1   Image2   Config File   File <File ID>} status <status>
STACK	Switch with duplicate UUID/bay (<UUID>, <bay>) trying to join.
STACK	The joining of switch (<MAC address>) in BCS chassis bay <bay number> with different port mapping is denied
STACK	The joining of switch (<MAC address>) with different chassis type <chassis type> is denied
STACK	The joining of switch (<MAC address>) with different type <switch type> is denied
STACK	The master is in BCS chassis bay <bay number> with different port mapping
STP	Cannot set "{Hello Time   Max Age   Forward Delay   Aging}" (Switch is in MSTP mode)
SYSTEM	Error: BOOTP Offer was found incompatible with the other IP interfaces
SYSTEM	Error: DHCP Offer was found invalid by ip configuration checking; please see system log for details.
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]
SYSTEM	Not enough memory!
SYSTEM	Port <port> disabled. Link params(speed/mode) mismatch with <trunk name> <trunk ID>
SYSTEM	Port <port> disabled. Same LACP admin_key with port "PORT_INT_<port>" link params(speed/mode)"
SYSTEM	{PortChannel   Trunk group} creation failed for {IntPortChannel   PortChannel   Internal Trunk group   Trunk group} <trunk ID>. Only <maximum trunks> {PortChannels   Trunk groups} supported by hardware.
TFTP	Error: Receive file from the master failed for <file ID>.
TFTP	Error: Receive transfer of config file from the master failed
TFTP	Error: Receive transfer of image1   2 from the master failed
TFTP	Error: Sending of {boot image   config file   image1   image2} to switch <MAC address> failed

## LOG\_NOTICE

Thread	LOG_NOTICE Message
	<minutes> {minute   minutes} until scheduled reboot
	ARP table is full.
	Could not create check point entry for VNIC
	Current config successfully tftp'd <filename> from <hostname>
	Current config successfully tftp'd to <hostname>: <filename>
	Number of COSqs has been changed since boot. Save and reset the switch to activate the new configuration.
	Port <port> mode is changed to full duplex for 1000 Mbps operation.
	scheduled switch reboot
	switch reset at <time> has been canceled
	switch reset scheduled at <time>
8021X	Authentication session terminated with {Failure   Success} on port <port>
8021X	Could not create failover checkpoint record for port <port>
8021X	Logoff request on port <port>
8021X	Port <port> {assigned to   removed from} vlan <VLAN>
8021X	RADIUS server <IP address> auth response for port <port> has an invalid Tunnel-Type value (<tunnel type>); should be 13 for VLAN assignment
8021X	RADIUS server <IP address> auth response for port <port> has an invalid Tunnel-Medium-Type value (<tunnel type>); should be 6 for VLAN assignment
8021X	RADIUS server <IP address> auth response for port <port> is missing one or more tunneling attributes for VLAN assignment
8021X	RADIUS server <IP address> auth response has a VLAN id (<VLAN>) of a reserved VLAN and cannot be assigned to port <port>
8021X	RADIUS server <IP address> auth response has a VLAN id (<VLAN>) of a non-existent or disabled VLAN, and cannot be assigned to port <port>
8021X	RADIUS server <IP address> auth response has an invalid VLAN id (<VLAN>) and cannot be assigned to port <port>
AMP	AMP group <group> topology is UP

Thread	LOG_NOTICE Message (continued)
AMP	Multiple LACP trunks using admin key <group> are currently active
AMP	Putting port <port> in forwarding state
BGP	session established with <IP address>
CFG	Note: The configured AMP interval and timeout-count values result in a very short keep-alive timeout that may lead to unstable topologies in some configurations. The suggested keep-alive timeout is at least <value> centisecond[s]
CFG	Note: AMP switch type is {aggregator   access}; aggregator-{port   portchannel   trunk} configuration is ignored
CONSOLE	RADIUS: authentication timeout. Retrying...
CONSOLE	RADIUS: failed to contact primary   secondary server
CONSOLE	RADIUS: No configured RADIUS server
CONSOLE	RADIUS: trying alternate server...
DCBX	Detected DCBX peer on port <port>
DCBX	Feature "{DCBX   ETS   PFC   App Proto   VNIC   ETS}" not supported by peer on port <port>
DCBX	LLDP [TX &] RX are disabled on port <port>
DCBX	LLDP TX is disabled on port <port>
DCBX	Not able to detect DCBX peer on port <port>
DCBX	Peer on port port stopped responding to DCBX message
FCOE	Failed to create FCOE vlan <VLAN>
FCOE	FCF <MAC address> has been removed.
FCOE	FCF <MAC address> is now operational.
FCOE	FCOE connection between VN_PORT <MAC address> and FCF <MAC address> {has been established   is down}.
FCOE	FCOE vlan <VLAN> created.
FCOE	Port <port> has been added to the FCOE vlan <VLAN>.
FCOE	VN_PORT <MAC address> has been reassigned, the old connection will be deleted.
HOTLINKS	"Error" is set to "Standby   Active"

Thread	LOG_NOTICE Message (continued)
HOTLINKS	"Learning" is set to "Standby   Active"
HOTLINKS	"None" is set to "Standby   Active"
HOTLINKS	"Side Max" is set to "Standby   Active"
HOTLINKS	has no "{Side Max   None   Learning   Error}" interface
IP	cannot contact multicast router <IP address>
IP	default gateway <IP address> {disabled   enabled   operational}
IP	Either Route or Arp table is full. Please check GEA L3 statistics (/stat/l3/gea) to verify.
IP	IGMP - {L3 IPMC   L3 IPv4 Multicas   Backup UP groups   Backup DOWN groups   IGMP groups   IPMC} table is full!
IP	IGMP - V1 timer is running for group <IP address>, vlan <VLAN>[, port <port>] Ignored leave!
IP	L3 table is full. Please check GEA L3 statistics (/stat/l3/gea) to verify.
IP	multicast router <IP address> operational
IP	New Multicast router learned on <IP address>, Vlan <VLAN>, Version V<version>
IP	Received {IGMPv1   IGMPv2} query from <IP address>
IP	VLAN <VLAN> is not in the igmp relay list. Mrouter <IP address> will be down
IP	Warning: Enabling dhcp will delete master switch IP interface and default gateway configurations.
LACP	LACP is {up   down} on port <port>
LINK	link {down   up} on port <port>
LINK	Port <port> disabled by PVST Protection
MGMT	<username> automatically logged out from BBI because changing of authentication type
MGMT	<username>(<user type>) {logout   ejected   idle timeout   connection closed} from {BBI   Console   Telnet/SSH}
MGMT	<username>(<user type>) login {on Console   from host <IP address>   from BBI}

Thread	LOG_NOTICE Message (continued)
MGMT	Authentication failed for backdoor.
MGMT	Authentication failed for backdoor. Password incorrect!
MGMT	Authentication failed for backdoor. Telnet disabled!
MGMT	boot config block changed
MGMT	boot image changed
MGMT	boot mode changed
MGMT	Chassis Control of External Ports can not be changed thru I2C Control Register
MGMT	Chassis Control of Management via all ports can not be changed thru I2C Control Register
MGMT	Chassis Control of Mgmt VLAN Interface from VPD can not be changed thru I2C Control Register
MGMT	Chassis Control of Reset Factory Defaults can not be changed thru I2C Control Register
MGMT	DAD found duplicate IP address on management interface <i>&lt;interface&gt;</i>
MGMT	enable password changed
MGMT	Error in setting the new config
MGMT	External Ports can not be ENABLED thru I2C Control Register
MGMT	External Ports can not be DISABLED thru I2C Control Register
MGMT	External Ports DISABLED ENABLED thru I2C Control Register
MGMT	Failed login attempt via {BBI   TELNET} from host <i>&lt;IP address&gt;</i> .
MGMT	Failed login attempt via the CONSOLE
MGMT	FLASH Dump cleared from BBI
MGMT	Invalid Chassis SubType ( <i>&lt;subtype&gt;</i> ) detected, assuming {bct   bc}
MGMT	Invalid IOBay ( <i>&lt;IOBay ID&gt;</i> ) detected, assuming ex@top-ex in@bot.
MGMT	Invalid SlotID ( <i>&lt;slot ID&gt;</i> ) detected, assuming Slot 1.
MGMT	Local Control of External Ports ENABLED thru Protected Mode
MGMT	Local Control of Management via all ports ENABLED thru Protected Mode

Thread	LOG_NOTICE Message (continued)
MGMT	Local Control of Mgmt VLAN Interface from VPD ENABLED thru Protected Mode
MGMT	Local Control of Reset Factory Defaults is ENABLED thru Protected Mode
MGMT	Management Port 1   2 RESET thru I2C Control Register
MGMT	Management STG 16 configurations from old config file moved to STG 32
MGMT	Management via all ports cannot be DISABLED thru I2C Control Register
MGMT	Management via all ports {ENABLED   is DISABLED} thru I2C Control Register
MGMT	Membership for Port <port> in vlan <VLAN> is not effective while the port is assigned with PVID <PVID> by 802.1x
MGMT	Method {STATIC   DHCP   DISABLED} IP Address <IP address>, Mask <netmask>[, Gateway <IP address>]
MGMT	Method {STATIC   DHCPv6   DISABLED   STATELESS} IP Address <IPv6 address>/<prefix length>[, Gateway <IPv6 address>]
MGMT	Gateway <IP address> not in the same subnet as the Mgt IP <IP address>/<netmask>
MGMT	New config set
MGMT	New Management Gateway <IP address> configured
MGMT	New Management Gateway <IPv6 address> configured default
MGMT	New Management IP Address <IP address> configured
MGMT	packet-buffer statistics cleared
MGMT	PANIC command from CLI
MGMT	PASSWORD FIX-UP MODE IN USE
MGMT	Password for {oper   operator} changed by {SNMP user   <username>}, notifying admin to save.
MGMT	Port <port> remains untagged while it is assigned PVID <PVID> by 802.1x
MGMT	Port <port> was not enabled because it is disabled thru configuration.
MGMT	Port MGT1 DISABLED and MGT2 ENABLED because Management Module 2 is active

Thread	LOG_NOTICE Message (continued)
MGMT	Port MGT1 ENABLED and MGT2 DISABLED because Management Module 1 is active
MGMT	Protected Mode Mismatch : MM capabilities is not a subset of MM permissions.
MGMT	Protected Mode Mismatch : MM Config inconsistent with SM Config.
MGMT	Protected Mode Mismatch : MM does not support PRM.
MGMT	Protected Mode Mismatch : SM retains PRM local control of previously selected features.
MGMT	RADIUS server timeouts
MGMT	RADIUS: authentication timeout. Retrying...
MGMT	RADIUS: failed to contact {primary secondary} server
MGMT	RADIUS: No configured RADIUS server
MGMT	RADIUS: trying alternate server...
MGMT	scp<username>(<user type>) {logout   ejected   idle timeout   connection closed} from {Console   Telnet/SSH}
MGMT	scp<username>(<user type>) login {on Console   from host <IP address>}
MGMT	second syslog host changed to {this host   <IP address>}
MGMT	selectable [boot] mode changed
MGMT	STP BPDU statistics cleared
MGMT	STM Mismatch : SM does not have enough capabilities for STM.
MGMT	STM Warning : Chassis does NOT support stacking mode.
MGMT	switch reset from CLI
MGMT	syslog host changed to {this host   <IP address>}
MGMT	System clock set to <time>.
MGMT	System date set to <date>.
MGMT	Terminating BBI connection from host <IP address>
MGMT	Updated switch image to match master's image version. Reset needed
MGMT	User <username> deleted by {SNMP user   <username>}.



Thread	LOG_NOTICE Message (continued)
MGMT	User <username> is {deleted   disabled} and will be ejected by {SNMP user   <username>}
MGMT	User {oper   operator} is disabled and will be ejected by {SNMP user   <username>}.
MGMT	Wrong config file type
NTP	System clock updated
OSPF	Neighbor Router ID <router ID>, Neighbor State {Down   Loopback   Waiting   P To P   DR   BackupDR   DR Other   Attempt   Init   2 Way   ExStart   Exchange   Loading   Full}
OSPFV3	Link state database is FULL.Ignoring LSA.
OSPFV3	nbr <router ID> changes state from {DOWN   ATTEMPT   INIT   2WAY   EXSTART   EXCHANGE   LOADING   FULL} to {DOWN   ATTEMPT   INIT   2WAY   EXSTART   EXCHANGE   LOADING   FULL}[, Neighbor Down: {Interface down or detached   Dead timer expired}]
OSPFV3	virtual link nbr <router ID> changes state from {DOWN   ATTEMPT   INIT   2WAY   EXSTART   EXCHANGE   LOADING   FULL} to {DOWN   ATTEMPT   INIT   2WAY   EXSTART   EXCHANGE   LOADING   FULL}[, Neighbor Down: {Interface down or detached   Dead timer expired}]
SERVER	link {down   up} on port <port>
SSH	(remote disconnect msg)
SSH	<username>(<user type>) {logout   ejected   idle timeout   connection closed} from {Console   Telnet/SSH}
SSH	<username>(<user type>) login {on Console   from host <IP address>}
SSH	Error in setting the new config
SSH	Failed login attempt via SSH
SSH	New config set
SSH	scp<username>(<user type>) {logout   ejected   idle timeout   connection closed} from {Console   Telnet/SSH}
SSH	scp<username>(<user type>) login {on Console   from host <IP address>}

Thread	LOG_NOTICE Message (continued)
SSH	Wrong config file type
STACK	<MAC address> become master {after init   from backup}
STACK	a specified master switch just joined the stack
STACK	A switch (<MAC address>) with no csnum assigned just joined.
STACK	attached switch <MAC address> cleared
STACK	BACKUP_GONE   BACKUP_PRESENT received from the master <MAC address>
STACK	BE_BACKUP   BE_MEMBER received from the master <MAC address>
STACK	BE_BACKUP   BE_MEMBER sent to <MAC address>
STACK	Boot Image successfully received by <MAC address>
STACK	CFG_REQ {received from   sent to} <MAC address>
STACK	CFG_SCRIPT received from the master <MAC address>
STACK	CFG_SCRIPT sent to <MAC address>
STACK	Config File successfully received by <MAC address>>
STACK	Current switch state changed, {all current sessions   current console session} will be terminated.
STACK	DCS from csnum 0 received
STACK	DCS from non-master received
STACK	DCS sync from csnum 0 received
STACK	DCS sync from non-master received
STACK	DELAYED_REBOOT timer expired
STACK	File <File ID> successfully received by <MAC address>
STACK	FORCED_DETACH received from the master <MAC address>
STACK	FORCED_DETACH sent to <MAC address>
STACK	I_AM_BACKUP {received from   sent to} <MAC address>
STACK	I_AM_MASTER received from the master <MAC address>
STACK	Image1   2 successfully received by <MAC address>

Thread	LOG_NOTICE Message (continued)
STACK	ingress application traffic {are blocked   is resumed}
STACK	JOIN_STACK received from <MAC address>
STACK	LEAVE_STACK received from <MAC address>
STACK	Link down on stack port <csnum>:<port> (UUID <UUID>, Bay <bay>)
STACK	Link up on stack port <csnum>:<port>
STACK	local csnum changed to <csnum>
STACK	local ports disabled by local {master   switch}
STACK	local ports disabled by the master
STACK	local ports enabled by {local master   the master}
STACK	Member could not send the status of the tftp transfer to the master
STACK	Member switch booted with <A> cosQ. Master switch has <B> cosQ. Resetting to update.
STACK	merger of two stacks detected [on remote switch <MAC address>]
STACK	more than one specified master switches joined the stack
STACK	Newly {attached   configured} switch's boot config is {active   backup   factory}, updating to {active   backup   factory}
STACK	Newly attached switch's boot image is <image>. Not matching Master's boot image <image>, updating.
STACK	Newly attached switch's cosQ configuration is <A>. Not matching Master's cosQ configuration <B>, updating.
STACK	Newly attached switch's flash version is <version>. Not matching Master's version, updating image <image>.
STACK	Newly attached switch's NetConfig is {enabled   disabled}, updating to {enabled   disabled}
STACK	Newly attached switch's version matches Master's flash, but not current version. Please reset Master to allow new members to join.
STACK	Newly attached switch's version matches Master's version. Rebooting attached switch.
STACK	no master present now while one existed before

Thread	LOG_NOTICE Message (continued)
STACK	old master disappeared
STACK	PARAM_REQ_ATTACH received from the master <MAC address>
STACK	REQ_ATTACH received from <MAC address>
STACK	requested to reboot by the master
STACK	STACK: <SFP type> {inserted   removed} at port <csnum>:<port>
STACK	switch {revert   revert apply} from DC
STACK	Switch <csnum>, <MAC address> just joined.
STACK	switch apply from DC
STACK	switch save requested by the master
STACK	The specified backup (<csnum>) is the current master - a specified master; no backup will be selected in this case
STACK	TO_JOIN_STACK {received from   sent to} <MAC address>
SYSTEM	<SFP type> inserted at port <port>
SYSTEM	Address for interface <interface> ignored because of mismatch.
SYSTEM	Change fiber GIG port <port> mode to full duplex
SYSTEM	Change fiber GIG port <port> speed to 1000
SYSTEM	Changed ARP entry for IP <IP address> to: MAC <MAC address>, Port <port>, VLAN <VLAN>
SYSTEM	Could NOT read Active Cable Compliance
SYSTEM	ECMP route gateway <IP address> [via if <interface>] is {down   up}
SYSTEM	Enable auto negotiation for copper GIG port: <port>
SYSTEM	Failed to read 10Gb Compliance (SR/LR) for <SFP type> <port>.
SYSTEM	Failed to read cable length for DAC.
SYSTEM	Failed to read Connector Type (OPT/CX4) for <SFP type> <port>.
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]
SYSTEM	Mask for interface <interface> ignored because of mismatch.
SYSTEM	Not enough memory!

Thread	LOG_NOTICE Message (continued)																										
SYSTEM	Port <i>&lt;port&gt;</i> disabled																										
SYSTEM	Port <i>&lt;port&gt;</i> disabled by BPDU Guard																										
SYSTEM	Port <i>&lt;port&gt;</i> disabled by OAM (unidirectional   TX-RX Loop)																										
SYSTEM	Port <i>&lt;port&gt;</i> disabled by UDLD (unknown   unidirectional   bidirectional   TX-RX loop   neighbor mismatch)																										
SYSTEM	Port <i>&lt;port&gt;</i> disabled due to reason code <i>&lt;reason code&gt;</i>																										
SYSTEM	rebooted ( <i>&lt;reason&gt;</i> )[, administrator logged in]  Reason: <table> <tr> <td>■ Boot watchdog reset</td><td>■ reset from console</td></tr> <tr> <td>■ console PANIC command</td><td>■ reset from EM</td></tr> <tr> <td>■ console RESET KEY</td><td>■ reset from Telnet/SSH</td></tr> <tr> <td>■ hard reset by SNMP</td><td>■ scheduled reboot</td></tr> <tr> <td>■ hard reset by WEB-UI</td><td>■ SMS-64 found an over-voltage</td></tr> <tr> <td>■ hard reset from console</td><td>■ SMS-64 found an under-voltage</td></tr> <tr> <td>■ hard reset from Telnet</td><td>■ software ASSERT</td></tr> <tr> <td>■ low memory</td><td>■ software PANIC</td></tr> <tr> <td>■ MM Cycled Power Domain</td><td>■ software VERIFY</td></tr> <tr> <td>■ power cycle</td><td>■ Telnet PANIC command</td></tr> <tr> <td>■ Reset Button was pushed</td><td>■ unknown reason</td></tr> <tr> <td>■ reset by SNMP</td><td>■ watchdog timer</td></tr> <tr> <td>■ reset by WEB-UI</td><td></td></tr> </table>	■ Boot watchdog reset	■ reset from console	■ console PANIC command	■ reset from EM	■ console RESET KEY	■ reset from Telnet/SSH	■ hard reset by SNMP	■ scheduled reboot	■ hard reset by WEB-UI	■ SMS-64 found an over-voltage	■ hard reset from console	■ SMS-64 found an under-voltage	■ hard reset from Telnet	■ software ASSERT	■ low memory	■ software PANIC	■ MM Cycled Power Domain	■ software VERIFY	■ power cycle	■ Telnet PANIC command	■ Reset Button was pushed	■ unknown reason	■ reset by SNMP	■ watchdog timer	■ reset by WEB-UI	
■ Boot watchdog reset	■ reset from console																										
■ console PANIC command	■ reset from EM																										
■ console RESET KEY	■ reset from Telnet/SSH																										
■ hard reset by SNMP	■ scheduled reboot																										
■ hard reset by WEB-UI	■ SMS-64 found an over-voltage																										
■ hard reset from console	■ SMS-64 found an under-voltage																										
■ hard reset from Telnet	■ software ASSERT																										
■ low memory	■ software PANIC																										
■ MM Cycled Power Domain	■ software VERIFY																										
■ power cycle	■ Telnet PANIC command																										
■ Reset Button was pushed	■ unknown reason																										
■ reset by SNMP	■ watchdog timer																										
■ reset by WEB-UI																											
SYSTEM	Received BOOTP Offer: IP: <i>&lt;IP address&gt;</i> , Mask: <i>&lt;netmask&gt;</i> , Broadcast <i>&lt;IP address&gt;</i> , GW: <i>&lt;IP address&gt;</i>																										
SYSTEM	Received DHCP Offer: IP: <i>&lt;IP address&gt;</i> , Mask: <i>&lt;netmask&gt;</i> Broadcast <i>&lt;IP address&gt;</i> , GW: <i>&lt;IP address&gt;</i>																										
SYSTEM	Received DHCPv6 Reply for IF <i>&lt;interface&gt;</i> IPv6: <i>&lt;IPv6 address&gt;</i> Prefix: <i>&lt;prefix length&gt;</i>																										
SYSTEM	server with MAC address <i>&lt;MAC address&gt;</i> was {added to   removed from} network																										
SYSTEM	SM_PRM_Control change FAILED.																										
SYSTEM	SM_PRM_Control changed.																										

Thread	LOG_NOTICE Message (continued)
SYSTEM	Watchdog threshold changed from <old value> to <new value> seconds
SYSTEM	Watchdog timer has been {enabled
TEAMING	error, action is undefined
TEAMING	is down, but teardown is blocked
TEAMING	is down, control ports are auto disabled
TEAMING	is up, control ports are auto controlled
VLAN	Default VLAN can not be deleted
VM	<IP address> moved from {port <port>   trunk IT <trunk ID>} to {port <port>   trunk IT <trunk ID>}
VM	Could not create check point entry for VM MAC [HOST]
VM	MAC address <MAC address> moved from {port <port>   trunk IT <trunk ID>} to {port <port>   trunk IT <trunk ID>}
VM	[(Refresh)] VI server unreachable or certificate invalid.
VM	Virtual Machine with {IP address <IP address>   MAC address <MAC address>} came online
VM	Virtual Machine with {IP address <IP address>   MAC address <MAC address>} changed its VLAN to <new VLAN>. It was previously in VLAN <old VLAN>
VM	Virtual Machine with {IP address <IP address>   MAC address <MAC address>} is a member of VLAN <VLAN>
VM	Virtual Machine with {IP address <IP address>   MAC address <MAC address>} is not in VLAN <VLAN> anymore
VM	[(Refresh)] VM agent command not implemented.
VM	[(Refresh)] VM agent could not be started.
VM	[(Refresh)] VM agent could not login to server.
VM	[(Refresh)] VM agent could not retrieve {host   VM} properties.
VM	[(Refresh)] VM agent encountered a file error.
VM	[(Refresh)] VM agent encountered an IPC error.
VM	[(Refresh)] VM agent file error.
VM	[(Refresh)] VM Agent not active.

Thread	LOG_NOTICE Message (continued)
VM	[(Refresh)] VM agent operation failed due to a conflict.
VM	[(Refresh)] VM agent operation failed.
VM	[(Refresh)] VM agent operation needs no change.
VM	[(Refresh)] VM agent operation timed out.
VM	[(Refresh)] VM agent protocol error.
VM	VM agent resumed (Refresh).
VM	VM agent resumed (Scan).
VM	[(Refresh)] VM agent timed out and could not be stopped.
VM	[(Refresh)] VM agent timed out.
VM	[(Refresh)] VM agent unable to logout from server.
VM	[(Refresh)] VM agent unknown error.
VM	[(Refresh)] VM agent VE limit reached.
VM	[(Refresh)] VM agent: Invalid ID.
VM	VM agent: local table full.
VM	VM MAC <MAC address> NOT added to hash table
VM	VM move detected but failed to move network conf
VRRP	virtual router <IP address> is now {BACKUP   MASTER}
WEB	<username> ejected from BBI
WEB	<username> ejected from BBI because username password was changed
WEB	RSA host key is being saved to Flash ROM, please don't reboot the box immediately.

## LOG\_INFO

Thread	LOG_INFO Message
	System log cleared by user <username>.
	System log cleared via SNMP.
DIFFTRAK	/* Config changes at <time> by <username> */ <config diff> /* Done */

Thread	LOG_INFO Message (continued)
HOTLINKS	"Error" is set to "{Active   Standby}"
HOTLINKS	"Learning" is set to "{Active   Standby}"
HOTLINKS	"None" is set to "{Active   Standby}"
HOTLINKS	"Side Max" is set to "{Active   Standby}"
HOTLINKS	has no "{Side Max   None   Learning   Error}" interface
MGMT	/* Config changes at <time> by <username> */ <config diff> /* Done */
MGMT	<username> ejected from BBI
MGMT	<username>(<user type>) {logout   ejected   idle timeout   connection closed} from {Console   Telnet/SSH}
MGMT	<username>(<user type>) login {on Console   from host <IP address>}
MGMT	All local control functions are enabled when PRM mode is activated
MGMT	Boot image ({Boot   Kernel   FS}, <size> bytes) download complete.
MGMT	boot image changed
MGMT	boot kernel download completed. Now writing to flash.
MGMT	boot kernel downloaded {from host <hostname>   via browser}, filename too long to be displayed, software version <version>
MGMT	boot kernel downloaded from host <hostname>, file'<filename>', software version <version>
MGMT	Boot Sector now contains Software Version <version>
MGMT	Can't downgrade to image with only single flash support
MGMT	Could not revert unsaved changes
MGMT	Download already currently in progress. Try again later via {Browser   BBI}
MGMT	Error in setting the new config
MGMT	Failed to allocate buffer for diff track.
MGMT	Failover just occurred, please try later
MGMT	Firmware download failed to {invalid image   image1   image2   boot kernel   undefined   SP boot kernel}



Thread	LOG_INFO Message (continued)
MGMT	Firmware downloaded to {invalid image   image1   image2   boot kernel   undefined   SP boot kernel}.
MGMT	Flash dump successfully tftp'd to <hostname>:<filename>
MGMT	FLASH ERROR - invalid address used
MGMT	Flash Read Error. Failed to read flash into holding structure. Quitting
MGMT	Flash Write Error
MGMT	Flash Write Error. Failed to allocate buffer. Quitting
MGMT	Flash Write Error. Trying again
MGMT	Forced unit detach detected, please try later
MGMT	FS Sector now contains Software Version <version>
MGMT	image1   2 download completed. Now writing to flash.
MGMT	image1   2 downloaded {from host <hostname>   via browser}, filename too long to be displayed, software version <version>
MGMT	image1   2 downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	image1   2 downloaded from the master, softer version <version>
MGMT	image1   2 now contains Software Version <version>
MGMT	Incorrect image being loaded
MGMT	Invalid diff track address. Continuing with apply()
MGMT	Invalid image being loaded for this switch type
MGMT	invalid image download completed. Now writing to flash.
MGMT	invalid image downloaded {from host <hostname>   via browser}, filename too long to be displayed, software version <version>
MGMT	invalid image downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	Kernel Sector now contains Software Version <version>
MGMT	NETBOOT: Config successfully downloaded and applied from <hostname>:<filename>
MGMT	New config set

Thread	LOG_INFO Message (continued)
MGMT	new configuration applied [from BBI   EM   NETBOOT   SCP   SNMP   Stacking Master]
MGMT	new configuration saved from {BBI   BladeOS   ISCLI   SNMP}
MGMT	Please save your current configuration and restart the stack.
MGMT	Protected Mode is already OFF.
MGMT	scp<username>(<user type>) {logout   ejected   idle timeout   connection closed} from {Console   Telnet/SSH}
MGMT	scp<username>(<user type>) login {on Console   from host <IP address>}
MGMT	Setting of Mgmt VLAN Interface cannot be changed to Disabled
MGMT	SP boot kernel download completed. Now writing to flash.
MGMT	SP boot kernel downloaded {from host <hostname>   via browser}, filename too long to be displayed, software version <version>
MGMT	SP boot kernel downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	Starting Firmware download for {invalid image   image1   image2   boot kernel   undefined   SP boot kernel}.
MGMT	Static FDB entry on disabled VLAN
MGMT	Static FDB entry on invalid VLAN
MGMT	Tech support dump failed
MGMT	Tech support dump successfully tftp'd to <hostname>:<filename>
MGMT	Two Phase Apply Failed in Creating Backup Config Block.
MGMT	undefined download completed. Now writing to flash.
MGMT	undefined downloaded {from host <hostname>   via browser}, filename too long to be displayed, software version <version>
MGMT	undefined downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	unsaved changes reverted [from BBI   from SNMP]
MGMT	Unsupported GBIC {accepted   refused}
MGMT	user {SNMP user   <username>} ejected from BBI

Thread	LOG_INFO Message (continued)
MGMT	Verification of new {invalid image   image1   image2   boot kernel   undefined   SP boot kernel} in FLASH successful.
MGMT	WARNING WARNING WARNING WARNING!!!!!!! CRC Error detected in BOOT region ( {Boot   Kernel   FS} ) - download another image and DO NOT reset your switch
MGMT	WARNING: A Reboot is required for the new downloaded image to take effect.
MGMT	Watchdog has been {enabled   disabled}
MGMT	Watchdog timeout interval is now <seconds> seconds)
MGMT	Writing to flash...This can take up to {90   150} seconds. Please wait
MGMT	Wrong config file type
MGMT	You must enable permission for control of {External Management   External Ports   Factory Default Reset   Mgmt VLAN Interface} from the MM or you must Disable this feature.
MGMT	You must select at least one PRM Feature to turn on
RMON	RMON {alarm   event   history} index <ID> was deleted via SNMP
RMON	SNMP configuration for RMON {alarm   event   history} index <ID> applied
SSH	<username>(<user type>) {logout   ejected   idle timeout   connection closed} from {Console   Telnet/SSH}
SSH	<username>(<user type>) login {on Console   from host <IP address>}
SSH	Error in setting the new config
SSH	New config set
SSH	scp<username>(<user type>) {logout   ejected   idle timeout   connection closed} from {Console   Telnet/SSH}
SSH	scp<username>(<user type>) login {on Console   from host <IP address>}
SSH	server key autogen {starts   completes}
SSH	Wrong config file type
SYSTEM	booted version <version> from Flash image <image>, {active   backup   factory} config block
SYSTEM	FDB Learning {DISABLED   ENABLED} for port <port>

Thread	LOG_INFO Message (continued)
SYSTEM	Insert another transceiver or change configuration and manually enable port <port>
TFTP	Successfully sent {boot image   image1   mage2} to switch <MAC adress>

## Appendix B

# BLADEOS SNMP Agent

---

### SNMP Overview

---

The BLADEOS SNMP agent supports SNMP version 3. Security is provided through SNMP community strings. The default community strings are “public” for SNMP GET operation and “private” for SNMP SET operation. The community string can be modified only through the Command Line Interface (CLI). Detailed SNMP MIBs and trap definitions of the BLADEOS SNMP agent are contained in the following BLADEOS enterprise MIB document:

GbESM-24-10G-L2L3.mib

The BLADEOS SNMP agent supports the following standard MIBs:

- rfc1213.mib
- rfc1215.mib
- rfc1493.mib
- rfc1573.mib
- rfc1643.mib
- rfc1757.mib
- rfc1907.mib
- rfc2037.mib
- rfc2571.mib
- rfc2572.mib
- rfc2573.mib
- rfc2574.mib
- rfc2575.mib
- rfc2576.mib
- ieee8021ab.mib
- dot1x.mib
- rfc1657.mib
- rfc1850.mib

The BLADEOS SNMP agent supports the following generic traps as defined in RFC 1215:

- ColdStart
- WarmStart
- LinkDown
- LinkUp
- AuthenticationFailure

The SNMP agent also supports two Spanning Tree traps as defined in RFC 1493:

- NewRoot
- TopologyChange

The following are the enterprise SNMP traps supported in BLADEOS:

**Table 323** BLADEOS-Supported Enterprise SNMP Traps

Trap Name	Description
altSwDefGwUp	Signifies that the default gateway is alive.
altSwDefGwDown	Signifies that the default gateway is down.
altSwDefGwInService	Signifies that the default gateway is up and in service
altSwDefGwNotInService	Signifies that the default gateway is alive but not in service
altSwVrrpNewMaster	Indicates that the sending agent has transitioned to 'Master' state.
altSwVrrpNewBackup	Indicates that the sending agent has transitioned to 'Backup' state.
altSwVrrpAuthFailure	Signifies that a packet has been received from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type. Implementation of this trap is optional.
altSwLoginFailure	Signifies that someone failed to enter a valid username/password combination.
altSwTempExceedThreshold	Signifies that the switch temperature has exceeded maximum safety limits.
altSwTempReturnThreshold	Signifies that the switch temperature has returned below maximum safety limits.
altSwStgNewRoot	Signifies that the bridge has become the new root of the STG.
altSwStgTopologyChanged	Signifies that there was a STG topology change.
altSwStgBlockingState	An altSwStgBlockingState trap is sent when port state is changed in blocking state.
altSwCistNewRoot	Signifies that the bridge has become the new root of the CIST.
altSwCistTopologyChanged	Signifies that there was a CIST topology change.
altSwHotlinksMasterUp	Signifies that the Master interface is active.
altSwHotlinksMasterDn	Signifies that the Master interface is not active.
altSwHotlinksBackupUp	Signifies that the Backup interface is active.

**Table 323** BLADEOS-Supported Enterprise SNMP Traps

Trap Name	Description
altSwHotlinksBackupDn	Signifies that the Backup interface is not active.
altSwHotlinksNone	Signifies that there are no active interfaces.
altSwValidLogin	Signifies that a user login has occurred.
altSwValidLogout	Signifies that a user logout has occurred.
altVMGroupVMotion	Signifies that a virtual machine has moved from a port to another.
altVMGroupVMOonline	Signifies that a advance provisioned virtual machine has came online.
altVMGroupVMvlanChange	Signifies that a virtual machine has entered into a VLAN, or changed the VLAN.

## Switch Images and Configuration Files

This section describes how to use MIB calls to work with switch images and configuration files. You can use a standard SNMP tool to perform the actions, using the MIBs listed in [Table 324](#).

[Table 324](#) lists the MIBS used to perform operations associated with the Switch Image and Configuration files.

**Table 324** MIBs for Switch Image and Configuration Files

MIB Name	MIB OID
agTransferServer	1.3.6.1.4.1872.2.5.1.1.7.1.0
agTransferImage	1.3.6.1.4.1872.2.5.1.1.7.2.0
agTransferImageFileName	1.3.6.1.4.1872.2.5.1.1.7.3.0
agTransferCfgFileName	1.3.6.1.4.1872.2.5.1.1.7.4.0
agTransferDumpFileName	1.3.6.1.4.1872.2.5.1.1.7.5.0
agTransferAction	1.3.6.1.4.1872.2.5.1.1.7.6.0
agTransferLastActionStatus	1.3.6.1.4.1872.2.5.1.1.7.7.0
agTransferUserName	1.3.6.1.4.1872.2.5.1.1.7.9.0



**Table 324** MIBs for Switch Image and Configuration Files

MIB Name	MIB OID
agTransferPassword	1.3.6.1.4.1.1872.2.5.1.1.7.10.0
agTransferTSDumpFileName	1.3.6.1.4.1.1872.2.5.1.1.7.11.0

The following SNMP actions can be performed using the MIBs listed in [Table 324](#).

- Load a new Switch image (boot or running) from a FTP/TFTP server
- Load a previously saved switch configuration from a FTP/TFTP server
- Save the switch configuration to a FTP/TFTP server
- Save a switch dump to a FTP/TFTP server

## Loading a New Switch Image

To load a new switch image with the name “MyNewImage-1.img” into image2, follow the steps below. This example assumes you have a FTP/TFTP server at 192.168.10.10.

1. Set the FTP/TFTP server address where the switch image resides:

```
Set agTransferServer.0 "192.168.10.10"
```

2. Set the area where the new image will be loaded:

```
Set agTransferImage.0 "image2"
```

3. Set the name of the image:

```
Set agTransferImageFileName.0 "MyNewImage-1.img"
```

4. If you are using an FTP server, enter a username:

```
Set agTransferUserName.0 "MyName"
```

5. If you are using an FTP server, enter a password:

```
Set agTransferPassword.0 "MyPassword"
```

6. Initiate the transfer. To transfer a switch image, enter 2 (gting):

```
Set agTransferAction.0 "2"
```

## Loading a Saved Switch Configuration

To load a saved switch configuration with the name “MyRunningConfig.cfg” into the switch, follow the steps below. This example assumes you have a TFTP server at 192.168.10.10.

1. Set the FTP/TFTP server address where the switch Configuration File resides:

```
Set agTransferServer.0 "192.168.10.10"
```

2. Set the name of the configuration file:

```
Set agTransferCfgFileName.0 "MyRunningConfig.cfg"
```

3. If you are using an FTP server, enter a username:

```
Set agTransferUserName.0 "MyName"
```

4. If you are using an FTP server, enter a password:

```
Set agTransferPassword.0 "MyPassword"
```

5. Initiate the transfer. To restore a running configuration, enter 3:

```
Set agTransferAction.0 "3"
```

## Saving the Switch Configuration

To save the switch configuration to a FTP/TFTP server follow the steps below. This example assumes you have a FTP/TFTP server at 192.168.10.10.

1. Set the FTP/TFTP server address where the configuration file is saved:

```
Set agTransferServer.0 "192.168.10.10"
```

2. Set the name of the configuration file:

```
Set agTransferCfgFileName.0 "MyRunningConfig.cfg"
```

3. If you are using an FTP server, enter a username:

```
Set agTransferUserName.0 "MyName"
```

4. If you are using an FTP server, enter a password:

```
Set agTransferPassword.0 "MyPassword"
```

5. Initiate the transfer. To save a running configuration file, enter 4:

```
Set agTransferAction.0 "4"
```

## Saving a Switch Dump

To save a switch dump to a FTP/TFTP server, follow the steps below. This example assumes you have a FTP/TFTP server at 192.168.10.10.

1. Set the FTP/TFTP server address where the configuration will be saved:

```
Set agTransferServer.0 "192.168.10.10"
```

2. Set the name of dump file:

```
Set agTransferDumpFileName.0 "MyDumpFile.dmp"
```

3. If you are using an FTP server, enter a username:

```
Set agTransferUserName.0 "MyName"
```

4. If you are using an FTP server, enter a password:

```
Set agTransferPassword.0 "MyPassword"
```

5. Initiate the transfer. To save a dump file, enter 5:

```
Set agTransferAction.0 "5"
```



# Index

---

## Symbols

/ command ..... 41

## Numerics

802.1p ..... 294

802.1x ..... 313

## A

abbreviating commands (CLI) ..... 46

access control

    user ..... 274

ACL Port menu ..... 289, 290

ACL re-marking ..... 303

ACL statistics ..... 227

active configuration block ..... 240, 503

active IP interface ..... 424

active port

    VLAN ..... 424

active switch configuration

    gtcfg ..... 475

    ptcfg ..... 474

    restoring ..... 475

active switch, saving and loading configuration .... 475

addr

    IP route tag ..... 103

administrator account ..... 29, 31

admpw (system option) ..... 274

aggregator

    AMP ..... 74

aging

    STP information ..... 89, 92

AMP aggregator ..... 74

AMP configuration ..... 319

AMP group information ..... 75

apply (global command) ..... 240

applying configuration changes ..... 240

autonomous system filter action ..... 379

autonomous system filter path

    action ..... 379

    as ..... 379

    aspath ..... 379

## B

backup configuration block ..... 240, 503

bandwidth allocation

    Priority Groups ..... 447

banner (system option) ..... 243

BBI ..... 23

BGP

    aggregation configuration ..... 401

    configuration ..... 395

    eBGP ..... 395

    iBGP ..... 395

    in route ..... 398

    IP address, border router ..... 397

    IP route tag ..... 103

    keep-alive time ..... 397

    peer ..... 395

    peer configuration ..... 397

    redistribution configuration ..... 399

    remote autonomous system ..... 397

    router hops ..... 398

BLOCKING (port state) ..... 90

Boot Management menu ..... 505

boot options menu ..... 491

bootstrap protocol ..... 415

Border Gateway Protocol ..... 103

    configuration ..... 395

Border Gateway Protocol (BGP)

    operations-level options ..... 484

BPDU. *See Bridge Protocol Data Unit.*

bridge priority ..... 89, 95

Bridge Protocol Data Unit (BPDU) ..... 89, 95

    STP transmission frequency ..... 330

Bridge Spanning-Tree parameters ..... 330

broadcast	
IP route tag .....	103
IP route type.....	102
Browser-Based Interface .....	23

## C

capture dump information to a file .....	522
CEE configuration .....	445
Cisco Ether Channel .....	339
CIST .....	325
CIST information .....	94
clear	
ARP entries.....	515
dump information .....	523
FDB entry.....	512
routing table.....	516
command (help) .....	41
Command-Line Interface (CLI) .....	23 to 30, 31, 39
commands	
abbreviations.....	46
conventions used in this manual.....	19
global commands.....	41
shortcuts .....	45
stacking .....	45
tab completion.....	46
Common Internal Spanning Tree .....	325
configuration	
802.1x .....	313
administrator password.....	274
apply changes.....	240
CIST .....	325
default gateway interval, for health checks .....	367
default gateway IP address .....	367
dump command.....	474
failover.....	345
flow control .....	286
Gigabit Ethernet .....	282
IGMP.....	402
IP static route .....	370
IP subnet address .....	364
IPv4 static route.....	368
LDAP .....	254
port mirroring.....	309
port trunking .....	339
save changes .....	240
SNMP .....	257
switch IP address .....	363
TACACS+ .....	250
user password .....	274
view changes .....	239
VLAN default (PVID).....	283
VLAN IP interface .....	364
VLAN tagging .....	283
VRRP .....	416
configuration block	
active .....	503
backup .....	503
factory .....	503
selection .....	503
configuration menu .....	237
configuration, RIP.....	380
configuring routing information protocol.....	381
connecting	
via console.....	24
console port	
connecting .....	24
Converged Enhanced Ethernet.....	445
COS queue information .....	132
cost	
STP information .....	89, 92, 95
STP port option .....	331
CPU statistics .....	226
CPU utilization .....	226
cur (system option).....	249, 256, 272

## D

date	
system option.....	242
daylight savings time .....	242
DCB Capability Exchange Protocol .....	450
DCBX configuration .....	450
DCBX information.....	148
debugging .....	509
default gateway	
information.....	99, 100
interval, for health checks .....	367
default gateway, IPv6 .....	427
default password .....	29
delete	
FDB entry .....	512
diff (global) command, viewing changes .....	239
direct (IP route type).....	102
directed broadcasts .....	374
DISABLED (port state) .....	90
disconnect idle timeout.....	30
DNS statistics .....	203
downloading software.....	499

dump	
configuration command .....	474
maintenance .....	509
duplex mode	
link status .....	49, 140
dynamic routes .....	516

## E

ECMP route hashing .....	369
Enhanced Transmission Selection .....	446
ENode .....	456
error disable and recovery	
port .....	285
system .....	244
EtherChannel (port trunking) .....	339
ETS configuration .....	446
ETS Priority Group .....	447

## F

factory configuration block .....	503
factory default configuration .....	30, 31, 32
failover	
configuration .....	345
FCF port .....	456
FCoE configuration .....	454
FCoE Initialization Protocol .....	454
FCoE statistics .....	229
FDB statistics .....	184
Fiber Channel Forwarding .....	456
Fiber Channel over Ethernet .....	454
FIP Snooping configuration .....	454
first-time configuration .....	30, 31 to 37
fixed	
IP route tag .....	103
flag field .....	105
flow control .....	49, 140
configuring .....	286
forwarding configuration	
IP forwarding configuration .....	374
forwarding database (FDB) .....	509
delete entry .....	512
Forwarding Database Information Menu .....	76
Forwarding Database Menu .....	512
forwarding state (FWD) .....	77, 89, 95, 96
fwd (STP bridge option) .....	330
FwdDel (forward delay), bridge port .....	89, 92, 95

## G

gateway, IPv4 .....	367
gig (Port Menu option) .....	282
Gigabit Ethernet	
configuration .....	282
Gigabit Ethernet Physical Link .....	282
global commands .....	41
gtcfg (TFTP load command) .....	475

## H

health checks	
default gateway interval, retries .....	367
retry, number of failed health checks .....	367
hello	
STP information .....	89, 92, 95
help .....	41
Hot Links configuration .....	351
hot-standby failover .....	422
hprompt	
system option .....	243
HTTPS .....	277

## I

ICMP statistics .....	204
idle timeout .....	30
IEEE standards	
802.1d .....	89, 328
802.1p .....	294
802.1s .....	323
802.1w .....	323
802.1x .....	86
IGMP .....	402
IGMP Snooping .....	403
IGMP statistics .....	209
image	
downloading .....	499
software, selecting .....	502
indirect (IP route type) .....	102
Information Menu .....	47
Interface change stats .....	214, 220
IP address	
ARP information .....	104
configuring default gateway .....	367
IP forwarding	
directed broadcasts .....	374
IP forwarding information .....	99, 100
IP Information .....	124, 126
IP Information Menu .....	99, 100

IP interface .....	364
active .....	424
configuring address .....	363
configuring VLANs .....	364
IP interfaces .....	102
information .....	99, 100
IP route tag .....	103
priority increment value (ifs) for VRRP .....	426
IP network filter configuration .....	375
IP Route Manipulation Menu .....	516
IP routing .....	
tag parameters .....	103
IP Static Route Menu .....	370
IP statistics .....	193, 196
IP switch processor statistics .....	190
IPv4 Static Route Menu .....	368
IPv6 default gateway configuration .....	427
IPv6 Neighbor Discovery .....	365
IPv6 static routes .....	428

## L

LACP .....	343
Layer 2 Menu .....	70
Layer 3 Menu .....	98
LDAP .....	254
LEARNING (port state) .....	89, 90, 95
Link Aggregation Control Protocol configuration .....	
LACP .....	343
link status .....	49
command .....	140
duplex mode .....	49, 140
port speed .....	49, 140
Link Status Information .....	140
linkt (SNMP option) .....	258
LISTENING (port state) .....	90
LLDP .....	
configuration .....	335
statistics .....	187
TLV .....	337
local (IP route type) .....	102
log (syslog messages) .....	246
Loopback Interface configuration .....	444

## M

MAC (media access control) address 52, 64, 76, 104, 512 .....	
Main Menu .....	39
Command-Line Interface (CLI) .....	30
summary .....	40

Maintenance .....	
IGMP .....	517
IGMP Groups .....	518
IGMP Multicast Routers .....	519
Maintenance Menu .....	509
management module .....	24
Management Processor (MP) .....	513
display MAC address .....	52, 64
manual style conventions .....	19
martian .....	
IP route tag (filtered) .....	103
IP route type (filtered out) .....	102
mask (IP interface subnet address) .....	364
MaxAge (STP information) .....	89, 92, 95
MD5 cryptographic authentication .....	387
MD5 key .....	390
media access control. <i>See</i> MAC address.	
metering (ACL) ACL metering .....	302
Miscellaneous Debug Menu .....	513
monitor port .....	309
mp packet .....	224
MP. <i>See</i> Management Processor.	
multicast IP route type .....	102
multiple management VLANs .....	356
Multiple Spanning Tree configuration .....	323
mxage (STP bridge option) .....	330

## N

nbr change statistics .....	212, 218
Neighbor Discovery cache configuration .....	429
Neighbor Discovery configuration .....	365
network management .....	23
notice .....	243
NTP server menu .....	256
NTP synchronization .....	256

## O

OAM Discovery .....	
configuration .....	288
information .....	85
online help .....	41
Operation, Administration, and Maintenance protocol .....	288
operations menu .....	477
operations-level BGP options .....	484
operations-level IP options .....	484
Operations-Level Port Options .....	480, 481, 485
operations-level VRRP options .....	483



ospf	
area index .....	384, 386, 430
authentication key .....	390
configuration .....	384
cost of the selected path .....	389
cost value of the host .....	393, 441
dead, declaring a silent router to be down .....	390, 438
dead, health parameter of a hello packet .....	391, 440
export .....	394
fixed routes .....	395
general .....	211
global .....	211
hello, authentication parameter of a hello packet .....	391, 440
host entry configuration .....	392, 441
host routes .....	384, 431
interface .....	384, 430
interface configuration .....	389
link state database .....	385, 431
Not-So-Stubby Area .....	386, 433
priority value of the switch interface .....	389
range number .....	384, 430
redistribution menu .....	385, 431
route redistribution configuration .....	393
spf, shortest path first .....	387
stub area .....	386, 433
summary range configuration .....	388
transit area .....	386, 433
transit delay .....	390
type .....	386, 433
virtual link .....	384, 430
virtual link configuration .....	391, 440
virtual neighbor, router ID .....	391, 440
OSPF Database Information .....	111
OSPF general .....	108
OSPF General Information .....	110, 117
OSPF Information .....	108, 114
OSPF Information Route Codes .....	113
OSPF statistics .....	210, 215, 216
OSPFv3	
configuration .....	430
<b>P</b>	
parameters	
tag .....	103
type .....	102
Password	
user access control .....	274
password	
administrator account .....	29
default .....	29
user account .....	29
VRRP authentication .....	425
passwords .....	29
PFC configuration .....	448
ping .....	42
poisoned reverse, as used with split horizon .....	381
port configuration .....	282
Port Error Disable and Recovery .....	285
Port Menu	
configuration options .....	282
configuring Gigabit Ethernet (gig) .....	282
port mirroring	
configuration .....	309
Port number .....	140
port speed .....	49, 140
port states	
UNK (unknown) .....	77
port trunking	
description .....	339
port trunking configuration .....	339
ports	
disabling (temporarily) .....	285
information .....	142
membership of the VLAN .....	72, 97
priority .....	89, 95
STP port priority .....	331
VLAN ID .....	49, 142
preemption	
assuming VRRP master routing authority .....	420
virtual router .....	419, 423
priority	
virtual router .....	423
priority (STP port option) .....	331
Priority Flow Control .....	448
Priority Group	
ETS .....	447
prisrv	
primary radius server .....	248
Private VLAN .....	359
Protected Mode .....	485
Protocol-based VLAN .....	357
ptcfg (TFTP save command) .....	474
PVID (port VLAN ID) .....	49, 142
PVLAN .....	357
pwd .....	43

**Q**

quiet (screen display option) ..... 43

**R**

RADIUS server menu ..... 248

read community string (SNMP option) ..... 258

receive flow control ..... 286

reference ports ..... 77

re-mark ACL ..... 303

Remote Monitoring (RMON) ..... 457

restarting switch setup ..... 33

retries

    radius server ..... 248

retry

    health checks for default gateway ..... 367

rip

    IP route tag ..... 103

RIP Information ..... 121

RIP information ..... 121, 122, 123

RIP. *See Routing Information Protocol.*

RMON

    configuration ..... 457

    information ..... 135

    port configuration ..... 283

    statistics ..... 178

route statistics ..... 201, 202

router hops ..... 398

routing information protocol

    configuration ..... 381

Routing Information Protocol (RIP) ..... 103, 380

    options ..... 381

    poisoned reverse ..... 381

    split horizon ..... 381

    version 1 parameters ..... 381

RSTP information ..... 91

Rx/Tx statistics ..... 212, 217

**S**

save (global command) ..... 240

    noback option ..... 240

save command ..... 503

secret

    radius server ..... 248

secsrv

    secondary radius server ..... 248

Secure Shell ..... 246

setup facility ..... 30, 31

    restarting ..... 33

    starting ..... 32

    stopping ..... 33

sFlow configuration ..... 280

shortcuts (CLI) ..... 45

snap traces

    buffer ..... 513

SNMP ..... 23, 162, 257

    menu options ..... 258

    set and get access ..... 258

SNMP Agent ..... 553

SNMP statistics ..... 230

SNMPv3 ..... 259

software

    image ..... 499

    image file and version ..... 52, 64

software upgrade

    recovery ..... 505

spanning tree

    configuration ..... 328

Spanning-Tree Protocol ..... 96

    bridge parameters ..... 330

    bridge priority ..... 89, 95

    port cost option ..... 331

    port priority option ..... 331

    root bridge ..... 89, 95, 330

    switch reset effect ..... 504

split horizon ..... 381

Stacking

    boot options ..... 493

    configuration ..... 291

stacking commands (CLI) ..... 45

starting switch setup ..... 32

state (STP information) ..... 90, 92, 95

static

    IP route tag ..... 103

static route

    rem ..... 368

static route, IPv6 ..... 428

statis route

    add ..... 368

statistics

    management processor ..... 223

Statistics Menu ..... 161

stopping switch setup ..... 33

subnet address mask ..... 364

subnets

    IP interface ..... 363

switch	
name and location .....	52, 64
resetting .....	504
syslog	
system host log configuration .....	245
system	
contact (SNMP option) .....	258
date and time .....	52, 64
information .....	64
location (SNMP option) .....	258
System Error Disable and Recovery .....	244
System Information .....	51
System Maintenance Menu .....	511
system options	
admpw (administrator password) .....	274
cur (current system parameters) ....	249, 256, 272
date .....	242
hprompt .....	243
login banner .....	243
time .....	242
tnport .....	271
usrpw (user password) .....	274
wport .....	271
system parameters, current .....	249, 256, 272

## T

tab completion (CLI) .....	46
tacacs .....	250
TACACS+ .....	250
TCP .....	191
TCP statistics .....	206, 225
Telnet	
configuring switches using .....	474
telnet	
radius server .....	249
Telnet support	
optional setup for Telnet support .....	33
text conventions .....	19
TFTP .....	501
PUT and GET commands .....	474
TFTP server .....	474
thash	
layer 2 .....	341, 342
time	
system option .....	242
timeout	
radius server .....	248
timeouts	
idle connection .....	30
timers kickoff .....	214, 220

TLV .....	337
tnport	
system option .....	271
trace buffer .....	513
traceroute .....	43
Tracking	
VRRP .....	418
transmit flow control .....	286
trunk hash algorithm .....	340
trunk troupe information .....	96
type of area	
ospf .....	386, 433
type parameters .....	102
typographic conventions, manual .....	19

## U

UCB statistics .....	226
UDLD	
configuration .....	287
information .....	84
UDP .....	191
UDP statistics .....	208
UniDirectional Link Detection .....	287
unknown (UNK) port state .....	77
Unscheduled System Dump .....	523
upgrade	
recover from failure .....	505
upgrade, switch software .....	499
user access control configuration .....	274
user account .....	29
usrpw (system option) .....	274
Uencode Flash Dump .....	522

## V

verbose .....	43
Virtual NIC	
group configuration .....	467
Virtual NIC configuration .....	464
virtual router	
description .....	418
priority .....	423
tracking criteria .....	420
virtual router group	
VRRP priority tracking .....	422
virtual router group configuration .....	422
virtual router group priority tracking .....	424

Virtual Router Redundancy Protocol (VRRP)	
authentication parameters for IP interfaces .....	425
group options (prio) .....	423
operations-level options .....	483
password, authentication .....	425
priority election for the virtual router .....	419
priority tracking options .....	397, 421
Virtual Router Redundancy Protocol configuration	416
virtual routers	
increasing priority level of .....	420
master preemption (preem) .....	423
master preemption (prio) .....	419
priority increment values (vrs) for VRRP .....	426
virtualization	
configuration .....	462
information .....	144
operations .....	487
VLAN	
active port .....	424
configuration .....	355
VLAN tagging	
port configuration .....	283
port restrictions .....	356
VLANs	
ARP entry information .....	104
information .....	97
name .....	72, 97
port membership .....	72, 97
setting default number (PVID) .....	283
tagging .....	49, 142, 356
VLAN Number .....	97
VM	
bandwidth management .....	463
group configuration .....	469
information .....	145
policy .....	463
profile configuration .....	471
VMware configuration .....	473
VMware information .....	145
VMware operations .....	487
VNIC configuration .....	464
VNIC group configuration .....	467
VRID (virtual router ID) .....	418, 422
VRRP	
interface configuration .....	425
master advertisements .....	419
tracking .....	418
tracking configuration .....	426
VRRP Information .....	130
VRRP master advertisements	
time interval .....	423
VRRP statistics .....	221
<b>W</b>	
watchdog timer .....	509
weights	
setting virtual router priority values .....	426
wport .....	271
write community string (SNMP option) .....	258