

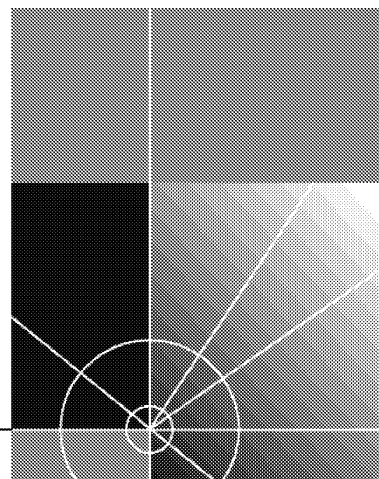


Command Reference Guide

CoreBuilder® 3500
CoreBuilder 9000
CoreBuilder 9400
SuperStack® II Switch 3900
SuperStack II Switch 9300

<http://www.3com.com/>

Part No. 10013505
Published November 1999



3Com Corporation
5400 Bayfront Plaza
Santa Clara, California
95052-8145

Copyright © 1999, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms, or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo, CoreBuilder, DynamicAccess, NETBuilder II, PACE, SmartAgent, SuperStack, and Transcend are registered trademarks of 3Com Corporation. 3Com Facts is a service mark of 3Com Corporation.

PostScript is a registered trademark of Adobe Systems, Inc. AppleTalk is a registered trademark of Apple Computer, Incorporated. Banyan and VINES are registered trademarks of Banyan Worldwide. DEC, DECnet, and PATHWORKS are registered trademarks of Compaq Computer Corporation. OpenView is a registered trademark of Hewlett-Packard Company. AIX, IBM, and NetView are registered trademarks and NetBIOS is a trademark of International Business Machines Corporation. Internet Explorer, Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Netscape, Netscape Navigator, and the Netscape N and Ship's Wheel logos are registered trademarks of Netscape Communications Corporation in the United States and other countries. IPX, Novell, and NetWare are registered trademarks of Novell, Inc. Sun and SunNet Manager are trademarks of Sun Microsystems, Inc. Xerox and XNS are trademarks of Xerox Corporation. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

All other company and product names may be trademarks of the respective companies with which they are associated.

CONTENTS

ABOUT THIS GUIDE

Using This Book	20
Finding Specific Information in This Guide	20
Command Information	22
Recommendations for Entering Commands	23
Conventions	23
Documentation Comments	25
Year 2000 Compliance	25

PART I GETTING STARTED

1 ADMINISTRATION OVERVIEW

Administration Console Overview	29
CoreBuilder 9000 System Management Overview	30
Management and Data Channels	31
CoreBuilder 9000 Management Features	33
EME Overview	33
Configuration Tasks	34
Accessing the Administration Console	35
Password Access Levels	35
Accessing Your System	36
Access Examples	37
Using Menus to Perform Tasks	39
Selecting Menu Options	40
Entering Values	41
Navigating Through the Menus	42

2 COMMAND SUMMARY

PART II SYSTEM-LEVEL FUNCTIONS

3 SYSTEM ENVIRONMENT

Menu Structure	68
system display	69
system fileTransfer	70
system console webHelpConfig	71
system console webAccess	72
system console consoleAccess	73
system console ctlKeys	74
system console password	75
system console screenHeight	76
system console security display	77
system console security define	78
system console security remove	80
system console security access	81
system console security message	82
system console timeout timeOut	83
system console timeout interval	84
system snapshot summary	85
system snapshot detail	86
system snapshot save	87
system softwareUpdate	89
system baseline display	90
system baseline set	91
system baseline requestedState	92
system serialPort terminalSpeed	93
system serialPort modemSpeed	95
system serialPort baudRate	96
system serialPort serialPortMode	98
system serialPort configModem	99
system serialPort enableModem	100
system name	101
system time	102
system time datetime	103
system time timezone	104
system time dst	106
system nvData save	107
system nvData restore	110

- system nvData examine 112
- system nvData reset 113
- system clearDiagBlock 114
- system diagErrLog 115
- system sntp display 116
- system sntp define 117
- system sntp modify 118
- system sntp remove 119
- system sntp state 120
- system sntp pollInterval 121
- system sntp tolerance 122
- system reboot 123
- script 124
- logout 126

4 MODULE ENVIRONMENT

- Menu Structure 128
 - module display 129
 - module snapshot summary 130
 - module snapshot detail 131
 - module baseline display 132
 - module baseline set 133
 - module baseline requestedState 134
 - module redundancy 135
 - module name 136
 - module time 137
 - module screenHeight 138
 - module nvData reset 139
 - module nvData emergencyDownload 140
 - module nvData displayDownload 141
 - module nvData staging 142
 - module clearDiagBlock 143
 - module diagErrLog 144
 - module reboot 145
 - disconnect 146

PART III ESTABLISHING MANAGEMENT ACCESS

5 OUT-OF-BAND MANAGEMENT

Menu Structure	150
management summary	151
management detail	153
management ip interface summary	156
management ip interface define	157
management ip interface modify	158
management ip interface remove	159
management ip route display	160
management ip route static	162
management ip route remove	163
management ip route flush	164
management ip route default	165
management ip route noDefault	166
management ip route findRoute	167
management ip arp display	168
management ip arp static	169
management ip arp remove	170
management ip arp flushAll	171
management ip arp flushDynamic	172
management ip rip display	173
management ip rip mode	174
management ip rip statistics	176
management ip ping	177
management ip advancedPing	179
management ip traceRoute	182
management ip advancedTraceRoute	184
management ip statistics	186

6 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

Menu Structure	190
snmp display	191
snmp community	192
snmp trap display	193
snmp trap addModify	194
snmp trap remove	196
snmp trap flush	197
snmp trap smtProxyTraps	198
snmp rmonConfiguration	199
snmp writeDisable	200

PART IV PHYSICAL PORT PARAMETERS

7 ETHERNET PORTS

Menu Structure	203
ethernet summary	204
ethernet detail	207
ethernet autoNegotiation	212
ethernet portMode	213
ethernet flowControl	215
ethernet paceAccess	217
ethernet pacerInteractiveAccess	218
ethernet label	219
ethernet portState	220
ethernet monitoring summary	221
ethernet monitoring mode	222

8 FIBER DISTRIBUTED DATA INTERFACE (FDDI)

Menu Structure	223
fddi station display	224
fddi station connectPolicy	225
fddi station tNotify	227
fddi station statusReporting	228
fddi path display	229
fddi path tvxLowerBound	230
fddi path tmaxLowerBound	231
fddi path maxTreq	232
fddi mac summary	233
fddi mac detail	234
fddi mac frameErrorThreshold	237
fddi mac notCopiedThreshold	238
fddi mac llcService	239
fddi mac path	240
fddi port display	241
fddi port lerAlarm	242
fddi port lerCutoff	243
fddi port label	244
fddi port path	245
fddi stationMode display	246
fddi stationMode modify	247

PART V BRIDGING PARAMETERS

9 BRIDGE-WIDE PARAMETERS

Menu Structure	251
bridge display	252
bridge ipFragmentation	255
bridge ipxSnapTranslation	256
bridge addressThreshold	257
bridge agingTime	258
bridge spanningTree stpState	259
bridge spanningTree stpPriority	261
bridge spanningTree stpMaxAge	262
bridge spanningTree stpHelloTime	263
bridge spanningTree stpForwardDelay	264
bridge spanningTree stpGroupAddress	265
bridge gvrpState	266
bridge cos enable	267
bridge cos summary	268
bridge cos modify	269
bridge multicast igmp summary	270
bridge multicast igmp snoopMode	271
bridge multicast igmp queryMode	272
bridge multicast igmp queryIpAddress	273
bridge multicast igmp vlans	274
bridge multicast igmp groups	275
bridge multicast igmp desQuerier	276
bridge multicast igmp rPorts	277
bridge multicast igmp qPort	278

10 BRIDGE PORT PARAMETERS

Menu Structure	279
bridge port summary	280
bridge port detail	283
bridge port multicastLimit	288
bridge port stpState	289
bridge port stpCost	290
bridge port stpPriority	291
bridge port gvrpState	292
bridge port address list	293
bridge port address add	294
bridge port address remove	295

bridge port address find 296
bridge port address flushAll 297
bridge port address flushDynamic 298

11 TRUNKS

Menu Structure 300
bridge trunk autoMap summary 301
bridge trunk autoMap enable/disable 302
bridge trunk autoMap test 303
bridge trunk summary 304
bridge trunk detail 305
bridge trunk define 307
bridge trunk modify 312
bridge trunk remove 318

12 MULTIPPOINT LINK AGGREGATION (MPLA)

Menu Structure 321
bridge mpla summary 322
bridge mpla detail 323
bridge mpla mode 324
bridge mpla peerMacAddress 326

13 RESILIENT LINKS

Menu Structure 327
bridge link summary 328
bridge link detail 329
bridge link define 330
bridge link linkState 332
bridge link activePort 333
bridge link modify 334
bridge link remove 336

14 VIRTUAL LANs (VLANs)

Menu Structure 337
bridge vlan summary 338
bridge vlan detail 341
bridge vlan define (3500/9000 Layer 3) 345
bridge vlan define (3900/9300/9400/ 9000 Layer 2) 352

bridge vlan modify (3500/9000 Layer 3) 355
bridge vlan modify (3900/9300/9400/ 9000 Layer 2) 360
bridge vlan remove 363
bridge vlan mode 364
bridge vlan stpMode 365
bridge vlan vlanAwareMode 366

15 PACKET FILTERS

Menu Structure 370
bridge packetFilter list 371
bridge packetFilter display 372
bridge packetFilter create portGroup 373
bridge packetFilter create custom 374
bridge packetFilter delete 376
bridge packetFilter edit 377
bridge packetFilter load 379
bridge packetFilter assign 382
bridge packetFilter unassign 384
bridge packetFilter portGroup list 386
bridge packetFilter portGroup display 387
bridge packetFilter portGroup create 388
bridge packetFilter portGroup delete 390
bridge packetFilter portGroup addPort 391
bridge packetFilter portGroup removePort 392

PART VI ROUTING PROTOCOLS

16 INTERNET PROTOCOL (IP)

Menu Structure 396
ip interface summary 398
ip interface detail 400
ip interface define (3500/9000 Layer 3) 403
ip interface define (3900/9300/9400/ 9000 Layer 2) 406
ip interface modify 407
ip interface remove 408
ip interface arpProxy 409
ip interface broadcastAddress 411
ip interface directedBroadcast 412
ip interface icmpRedirect 413
ip interface icmpRouterDiscovery 415

ip interface statistics 418
ip route display 420
ip route static 422
ip route remove 423
ip route flush 424
ip route default 425
ip route noDefault 426
ip route findRoute 427
ip arp display 428
ip arp static 429
ip arp remove 430
ip arp flushAll 431
ip arp flushDynamic 432
ip arp age 433
ip arp statistics 434
ip dns display 436
ip dns domainName 437
ip dns define 438
ip dns modify 439
ip dns remove 440
ip dns nslookup 441
ip udpHelper display 442
ip udpHelper define 443
ip udpHelper remove 444
ip udpHelper hopCountLimit 445
ip udpHelper threshold 446
ip udpHelper interface first 447
ip udpHelper interface even 448
ip udpHelper interface sequential 449
ip routing 450
ip rip display 451
ip rip mode 453
ip rip compatibilityMode 455
ip rip cost 456
ip rip poisonReverse 457
ip rip routeAggregation Mode 458
ip rip password 459
ip rip addAdvertisement 460
ip rip remove Advertisement 462
ip rip policy summary 463
ip rip policy detail 464
ip rip policy define 465
ip rip policy modify 469
ip rip policy remove 471

- ip rip statistics 472
- ip ping 473
- ip advancedPing 475
- ip traceRoute 478
- ip advancedTraceRoute 480
- ip statistics 482

17 VIRTUAL ROUTER REDUNDANCY (VRRP)

- Menu Structure 485
 - ip vrrp summary 486
 - ip vrrp detail 488
 - ip vrrp define 492
 - ip vrrp modify 495
 - ip vrrp remove 498
 - ip vrrp mode 499
 - ip vrrp neighbor 500
 - ip vrrp statistics 501

18 IP MULTICAST

- Menu Structure 504
 - ip multicast dvmrp interface summary 505
 - ip multicast dvmrp interface detail 506
 - ip multicast dvmrp interface mode 507
 - ip multicast dvmrp interface metric 508
 - ip multicast dvmrp tunnels summary 509
 - ip multicast dvmrp tunnels define 511
 - ip multicast dvmrp tunnels remove 513
 - ip multicast dvmrp tunnels address 514
 - ip multicast dvmrp tunnels threshold 515
 - ip multicast dvmrp tunnels metric 516
 - ip multicast dvmrp routeDisplay 517
 - ip multicast dvmrp cacheDisplay 518
 - ip multicast dvmrp default 520
 - ip multicast igmp interface summary 521
 - ip multicast igmp interface detail 522
 - ip multicast igmp interface TTL 523
 - ip multicast igmp snooping 524
 - ip multicast igmp querying 525
 - ip multicast cache 526
 - ip multicast traceRoute 528

19 OPEN SHORTEST PATH FIRST (OSPF)

Menu Structure	530
ip ospf areas display	531
ip ospf areas defineArea	532
ip ospf areas modifyArea	533
ip ospf areas removeArea	534
ip ospf areas addRange	535
ip ospf areas modifyRange	536
ip ospf areas removeRange	537
ip ospf defaultRouteMetric display	538
ip ospf defaultRouteMetric define	539
ip ospf defaultRouteMetric remove	540
ip ospf interface summary	541
ip ospf interface detail	542
ip ospf interface statistics	544
ip ospf interface mode	548
ip ospf interface priority	549
ip ospf interface areaID	550
ip ospf interface cost	551
ip ospf interface delay	552
ip ospf interface hello	553
ip ospf interface retransmit	554
ip ospf interface dead	555
ip ospf interface password	556
ip ospf linkStateData databaseSummary	557
ip ospf linkStateData router	558
ip ospf linkStateData network	560
ip ospf linkStateData summary	561
ip ospf linkStateData external	563
ip ospf neighbors display	564
ip ospf neighbors add	565
ip ospf neighbors remove	566
ip ospf routerID	567
ip ospf partition display	569
ip ospf partition modify	570
ip ospf stubDefaultMetric display	571
ip ospf stubDefaultMetric define	572
ip ospf stubDefaultMetric remove	573
ip ospf virtualLinks summary	574
ip ospf virtualLinks detail	575
ip ospf virtualLinks statistics	577
ip ospf virtualLinks define	581
ip ospf virtualLinks remove	582

ip ospf virtualLinks areaID 583
ip ospf virtualLinks router 584
ip ospf virtualLinks delay 585
ip ospf virtualLinks hello 586
ip ospf virtualLinks retransmit 587
ip ospf virtualLinks dead 588
ip ospf virtualLinks password 589
ip ospf policy summary 590
ip ospf policy detail 591
ip ospf policy define 593
ip ospf policy modify 598
ip ospf policy remove 602
ip ospf statistics 603

20 IPX

Menu Structure 606
ipx interface display 607
ipx interface define 608
ipx interface modify 610
ipx interface remove 612
ipx interface SAPadvertising 613
ipx interface RIPadvertising 614
ipx route display 615
ipx route secondary 617
ipx route static 618
ipx route remove 620
ipx route flush 621
ipx server display 622
ipx server static 624
ipx server remove 626
ipx server flush 627
ipx server secondary 628
ipx forwarding 629
ipx rip mode 630
ipx rip triggered 631
ipx rip policy summary 632
ipx rip policy define 633
ipx rip policy modify 635
ipx rip policy remove 637
ipx sap mode 638
ipx sap triggered 639
ipx sap policy summary 640

- ipx sap policy detail 641
- ipx sap policy define 642
- ipx sap policy modify 645
- ipx sap policy remove 648
- ipx output-delay 649
- ipx statistics summary 650
- ipx statistics rip 651
- ipx statistics sap 652
- ipx statistics forwarding 653
- ipx statistics interface 655
- ipx oddLengthPadding 657
- ipx NetBIOS 658
- ipx secondary 659

21 APPLETALK

- Menu Structure 662
 - appletalk interface summary 663
 - appletalk interface detail 664
 - appletalk interface define 665
 - appletalk interface modify 667
 - appletalk interface remove 669
 - appletalk interface statistics 670
 - appletalk route display 672
 - appletalk route flush 673
 - appletalk aarp display 674
 - appletalk aarp remove 675
 - appletalk aarp flush 676
 - appletalk zone display network 677
 - appletalk zone display zone 678
 - appletalk forwarding 679
 - appletalk checksum 680
 - appletalk sourceSocket 681
 - appletalk ping 682
 - appletalk statistics ddp 683
 - appletalk statistics rtmp 684
 - appletalk statistics zip 685
 - appletalk statistics nbp 686

PART VII TRAFFIC POLICY

22 QUALITY OF SERVICE (QOS) AND RSVP

Menu Structure	690
qos classifier summary	691
qos classifier detail	692
qos classifier define	694
qos classifier modify	701
qos classifier remove	706
qos control summary	707
qos control detail	708
qos control define	710
qos control modify	718
qos control remove	724
qos ldap display	725
qos ldap enable	726
qos ldap disable	727
qos rsvp summary	728
qos rsvp detail	729
qos rsvp enable	730
qos rsvp disable	732
qos bandwidth display	733
qos bandwidth modify	734
qos excessTagging display	735
qos excessTagging enable	736
qos excessTagging disable	737
qos statistics interval	738
qos statistics receive	739
qos statistics transmit	741

PART VIII MONITORING

23 EVENT LOG

Menu Structure	748
log display	749
log devices	750
log services	752

24 ROVING ANALYSIS

- Menu Structure 756
 - analyzer display 757
 - analyzer add 758
 - analyzer remove 760
 - analyzer start 761
 - analyzer stop 763

PART IX REFERENCE

A TECHNICAL SUPPORT

- Online Technical Services 767
 - World Wide Web Site 767
 - 3Com Knowledgebase Web Services 767
 - 3Com FTP Site 768
 - 3Com Bulletin Board Service 768
 - 3Com Facts Automated Fax Service 769
- Support from Your Network Supplier 769
- Support from 3Com 769
- Returning Products for Repair 771

INDEX

ABOUT THIS GUIDE

This *Command Reference Guide* provides information about the commands that you use to configure and manage your system or module after you install it. Before you use this guide, you should have already consulted documents such as your system *Getting Started Guide* or module *Quick Start Guide* and physically installed your system or module.

Several CoreBuilder® and SuperStack® II platforms are documented in this book. Table 1 lists the specific platforms and the current software release level of that platform as it relates to the information contained in this book:

Table 1 Platforms Covered in This Document

Platform	Release
CoreBuilder® 3500	3.0
SuperStack® II Switch 3900	3.0
CoreBuilder 9000	3.0
SuperStack II Switch 9300	3.0
CoreBuilder 9400	3.0

This guide is intended for the system or network administrator who is responsible for configuring, using, and managing the system. It assumes a working knowledge of local area network (LAN) operations and familiarity with communications protocols that are used on interconnected LANs.



If the information in the release notes that are shipped with your product differs from the information in this guide, follow the instructions in the release notes.

Using This Book

This guide contains information for every command for the platforms listed at the beginning of this chapter. It includes specific information about command syntax, field descriptions, default values, and the possible range of values. Some command descriptions include a section called "Important Considerations" that contains additional information to be aware of when using the command. Where appropriate, examples help you to understand the commands.

This guide does not contain troubleshooting information or instructional material about why or when to use a particular command. For information about troubleshooting and networking tasks, see the *Implementation Guide* that is shipped with your system on a CD-ROM.

Finding Specific Information in This Guide

Use this chart to help you find information about specific tasks:

If you are looking for information about	Turn to
System administration and configuration tasks Using command abbreviations Summary of commands for all platforms	Part I: Getting Started
Displaying the system or module configuration Using the snapshot feature Baselining statistics Configuring system parameters, such as name, date/time, and passwords Configuring system security Establishing system access through a Web browser Saving, restoring, and resetting nonvolatile data Running scripts of Console tasks	Part II: System-Level Functions
Setting up the system for out-of-band management access through serial ports or using IP and setting up SNMP Administering the IP management interface Configuring SNMP community strings Administering trap reporting	Part III: Establishing Management Access
Administering Ethernet ports Displaying statistics for and labelling Ethernet ports Administering Fiber Distributed Data Interface (FDDI) ports	Part IV: Physical Port Parameters

If you are looking for information about	Turn to
Configuring bridge parameters such as bridge display, agingTime, stpState, and Class of Service	Part V: Bridging Parameters
Managing trunks	
Configuring bridge port parameters such as listing addresses, setting the port priority, and controlling the Spanning Tree Protocol (STP) on a bridge	
Displaying MultiPoint Link Aggregation (MPLA) parameters	
Configuring resilient links	
Configuring virtual LANs (VLANs)	
Configuring packet filters	
Configuring IP interfaces and IP protocol parameters	Part VI: Routing Protocols
Configuring Virtual Router Redundancy Protocol (VRRP) parameters	
Configuring IP multicast routing and filtering	
Configuring Open Shortest Path First (OSPF) routing	
Configuring IPX routing	
Configuring AppleTalk routing	
Configuring Quality of Service (QoS) classifiers, controls, Resource Reservation Protocol (RSVP), bandwidth, and excess tagging	Part VII: Traffic Policy
Viewing statistics	
Administering the event log	Part VIII: Monitoring
Administering roving analysis	
Technical support	Part IX: Reference
Quickly locating information on tasks and topics	Index

Command Information

Each software command has its own description in this guide. Each command description begins at the top of a page. A command description begins with these items:

- The full command name
- Platforms on which this command is valid

Under the command name is a list of 3Com switch platforms. The command is valid on every platform that has a check mark (✓) next to it.

Sample platform list

✓✓3500
 ✓✓9000
 ✓✓9400

✓✓3900
 ✓✓9300

- A short description of the purpose of the command



Some command descriptions begin with a sentence similar to this one: "For CoreBuilder 9000: Applies to Layer n switching modules only." where n is either 2 or 3. Because the CoreBuilder 9000 system can house both Layer 2 modules and Layer 3 modules, this sentence alerts you to the fact that this particular command is valid only on Layer 2 modules or Layer 3 modules.

The command description continues with one or more of the following sections:

- **Valid Minimum Abbreviation** — This section lists the shortest number of characters that you can type to issue the command.
- **Important Considerations** — These usage notes identify potential problems before you use the command.
- **Options** — If the command begins a configuration process or other procedure, this section presents each prompt that you see, its description, the possible values that you can enter, and the default value.
- **Fields** — If the command prompts the system to display information, this section lists the display parameters and their definitions.

- **Procedure** — Numbered steps walk you through complex commands.
- **Example** — Examples show the interactive display when the system provides additional useful information.

Recommendations for Entering Commands

Before you enter any command, 3Com recommends that you:

- Examine the system menu carefully for the full command string:
- Consult the documentation for the valid minimum abbreviation for the command string.



If you are unfamiliar with a particular system, always enter the entire command, even though the system accepts abbreviated commands. If you abbreviate commands, you may make errors or omissions that have undesirable consequences.

For example, on the CoreBuilder 9000, to list all addresses for a port, you use the `bridge port address list all` command. If you mistakenly enter `bridge port address all`, the system interprets it as an abbreviated version of the `bridge port address flushAll` command, which flushes the entire address table for the port and does not request that you confirm the command.


Conventions

Table 2 and Table 3 list icon and text conventions that are used throughout this guide.

Table 2 Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
	Warning	Information that alerts you to potential personal injury

Table 3 Text Conventions

Convention	Description
Screen displays	This typeface represents information as it appears on the screen.
Command	<p>The word “command” means that you enter the command exactly as shown in the text and then press Return or Enter. Commands appear in bold. Example:</p> <p>To set flow control, enter the following command:</p> <p>ethernet flowControl</p> <p> <i>This guide always gives the full form of a command. However, you can abbreviate commands by entering just enough characters to distinguish one command from another similar command, as shown in “Valid Minimum Abbreviations” under each command description. Commands are not case sensitive.</i></p>
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press Return or Enter when an instruction simply says “type.”
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example:
	Press Ctrl+C.
Words in <i>italics</i>	<p>Italics are used to:</p> <ul style="list-style-type: none"> ■ Emphasize a point ■ Denote a new term when it is defined in text

**Documentation
Comments**

Your suggestions are very important to us. They help us to make our documentation more useful to you.

Please send e-mail comments about this guide to:

`sdtechpubs_comments@ne.3com.com`

Include the following information when commenting:

- Document title
- Document part number (found on the front or back page of each document)
- Page number (if appropriate)

Example:

Command Reference Guide

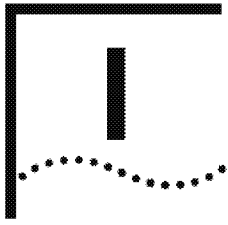
Part Number 10013505

Page 347

**Year 2000
Compliance**

For information on Year 2000 compliance and 3Com products, visit the 3Com Year 2000 Web page:

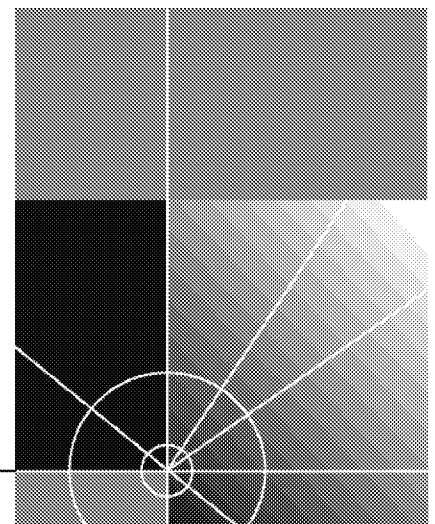
<http://www.3com.com/products/yr2000.html>

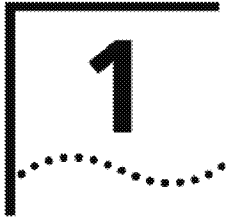


GETTING STARTED

Chapter 1 Administration Overview

Chapter 2 Command Summary





ADMINISTRATION OVERVIEW

This chapter introduces the Administration Console software that is supplied with your system, the types of commands that you use to perform network tasks, the valid syntax for command abbreviations, and some shortcuts to help you navigate through the menus. It also provides an overview of the management software that is specific to the CoreBuilder® 9000 Enterprise Switch. It introduces the EME (Enterprise Management Engine) Management Console for the CoreBuilder 9000 and describes its relationship to the Administration Console software.

The following topics are covered in this chapter:

- Administration Console Overview
- CoreBuilder 9000 System Management Overview
- CoreBuilder 9000 Management Features
- Configuration Tasks
- Accessing the Administration Console
- Using Menus to Perform Tasks

Administration Console Overview

The Administration Console software is installed at the factory in flash memory on the system processor. Because this software boots automatically from flash memory when you power on your system, the system is immediately ready for use in your network. However, you may need to:

- Configure certain parameters before the system can operate effectively in your networking environment.
- Connect to the Administration Console, if you have a CoreBuilder 9000.
- View important MAC, port, bridge, virtual LAN (VLAN), and IP statistics while you manage your system.

You use the Administration Console software to configure your system parameters (or, on the CoreBuilder 9000, to configure your module parameters) and display statistics and counters.



For more complete network management, you can use an external application, such as 3Com's Transcend® Network Control Services tool suite.



On the CoreBuilder 3500, CoreBuilder 9000, and CoreBuilder 9400, and on the SuperStack® II Switch 3900 and Switch 9300, you can also configure parameters and view statistics using the Web Management suite of HTML-based applications. See the Web Management User Guide for your system for additional information.

CoreBuilder 9000 System Management Overview

The CoreBuilder 9000 comes in a 7-slot, 8-slot, or 16-slot chassis in which you install switch fabric modules and interface modules. Before you begin to manage your CoreBuilder 9000 system, review the management-related information in this section.

The CoreBuilder 9000 system supports the following management interfaces:

- **EME Management Console**

Use the EME Management Console to manage EME and Enterprise Management Controller (EMC) functions, such as login table management, IP connectivity, event and trap logs, and software downloads to all modules. The EME Management Console also manages chassis functions, such as system inventory and power management features.

- **Administration Console**

Use the Administration Console to manage the CoreBuilder 9000 switch fabric modules and intelligent interface modules. These modules contain an on-board network management agent that allows this direct management.

- **ATM Local Management Application (LMA)**

Use the ATM LMA to manage the ATM Enterprise Switch, ATM Switch Fabric Module, and ATM interface modules. These modules contain an on-board network management agent to allow this direct management.

ATM LMA management of ATM switch fabric modules and ATM interface modules is outside of the scope of this guide. To learn about managing the ATM Enterprise Switch and ATM modules using the ATM LMA, see the *CoreBuilder 9000 ATM Enterprise Switch Management Guide*.

You cannot manage the EME using the ATM LMA, and you cannot manage ATM Switch Fabric Modules or ATM interface modules using the EME Management Console.

- **Web Management**

The Web Management suite of applications are an embedded part of the CoreBuilder 9000 system software image. They include the WebConsole and DeviceView applications. Additional installable applications include online Help. After you have set up your IP address for your system, you can access the Web Management applications directly from your Web browser by entering its IP address.

See the *Web Management User Guide for the CoreBuilder 9000 Enterprise Switch* for additional information about Web Management.

You manage the EME from a command line interface using EME management commands. You manage the switch fabric modules or interface modules through the Administration Console using module management commands or through the Web Management interface.

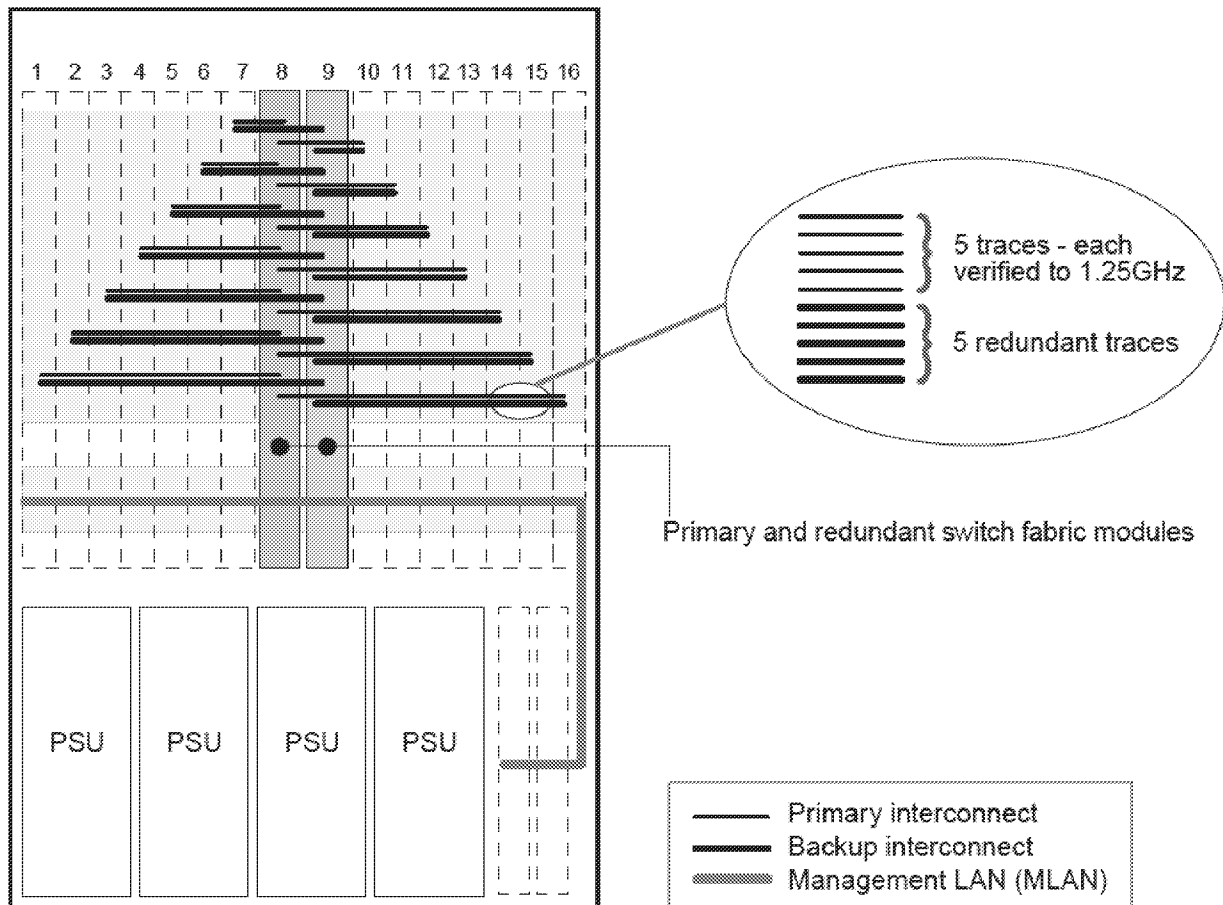
Management and Data Channels

The CoreBuilder 9000 system uses separate channels for network traffic and management traffic:

- The private management LAN (MLAN) handles management traffic. Management traffic travels to and from the EME, which acts as the single point of contact for all management traffic in the chassis.
- Switch fabric module backplane channels handle network traffic. Each interface module has one or two backplane ports that connect to the switch fabric module backplane, which allows network traffic to pass through the CoreBuilder 9000 system.

Figure 1 illustrates the MLAN channel and the switch fabric module backplane channels in the CoreBuilder 9000 16-slot chassis.

Figure 1 System Data Channels in the 16-slot Chassis



CoreBuilder 9000 Management Features

You can manage the CoreBuilder 9000 system through a terminal interface, through the Simple Network Management Protocol (SNMP), and through the 3Com Transcend[®] Network Control Services. The EME is the primary communication mechanism into the chassis and modules. You manage other intelligent modules within the chassis through the EME.

EME Overview

The EME is an SNMP-based network management module that manages and controls the 3Com CoreBuilder 9000 chassis and its modules. The EME has the following features:

- **Chassis Management Architecture** — Provides a cost-efficient management architecture that:
 - Provides a central point of contact for chassis management
 - Provides all controller functions, as well as EME functions
- **Intelligent Power Management** — Manages power use in the chassis by:
 - Preventing newly installed modules from receiving power when there is not enough power available
 - Allowing you to prioritize the order in which modules power off (if there is insufficient power available)
 - Allowing you to implement fault-tolerant power, which allows the chassis to reserve some of its power capacity to protect against a power supply failure

In the chassis:

- The EME exchanges information with all modules through the MLAN.
- Interface modules pass data through the switch fabric module.
- On modules that include their own agent, the EME "connects" to that module and then you can use the Administration Console management interface to manage that module.

Configuration Tasks To help you configure your system, the top-level menu of the Administration Console groups the commands into types for certain tasks, as listed in Table 4.



Not all menus and tasks are available on all systems.

Table 4 Types of Commands Associated with Configuration Tasks

Type of Command	Top-Level Menus	Tasks
General	system	Set system or module parameters, handle nonvolatile (NV) data, set security, reboot
	module	
	script	Run scripts
Management setup	logout, disconnect	Leave the Administration Console
	management	Set up the out-of-band management interface
Port-based management	snmp	Set up the system for SNMP and trap reporting
	ethernet	Manage Ethernet ports
Bridging	fddi	Manage Fiber Distributed Data Interface (FDDI) ports
	bridge	Set bridge parameters for the entire system, including for Spanning Tree Protocol (STP) and Class of Service (CoS) Manage trunking of bridge ports Set and display MultiPoint Link Aggregation (MPLA) parameters Manage resilient links Set bridge parameters for specific bridge ports Manage virtual LANs (VLANs) Manage packet filtering for port groups
Routing	ip	Set up IP, IP multicast, and IP Open Shortest Path First (OSPF) routing
	ipx	Set up IPX routing
	appletalk	Set up AppleTalk routing

Table 4 Types of Commands Associated with Configuration Tasks (continued)

Type of Command	Top-Level Menus	Tasks
Quality of Service management	qos	Set up classifiers and controls for traffic-policy-based services
Monitoring	log	Set severity levels and services for event logging
	analyzer	Monitor the network using a network analyzer

Accessing the Administration Console

Depending on which system you are managing, you access the Administration Console in either two steps (for the CoreBuilder 9000) or one step (for all other systems). See "Accessing Your System" later in this section for details.

For all systems, the Administration Console supports three password levels, allowing you to provide different levels of access for a range of users.

Password Access Levels

Your access level determines which types of menu commands you can use, as described in Table 5.

Table 5 Password Access Levels

Access Level	For users who need to	Allows users to
Administer	Perform system or module setup and management tasks (usually a single network administrator)	Perform system-level or module-level administration (such as resetting the module or changing passwords)
Write	Perform active network management	Configure network parameters (such as setting the aging time for a bridge)
Read	Only view system or module parameters	Access only "display" menu items (like display, summary, and detail)

Accessing Your System

You access the Administration Console for your system in one of two ways:

- **For all systems except the CoreBuilder 9000** — Access the Administration Console for the first time at the *Administer* level and press Return at the password prompt (the initial password is null). Subsequently, every time that you access the Administration Console, it prompts you for an access level and password, as shown here:

```
Select access level (read, write, administer):
Password:
```

The passwords are stored in nonvolatile (NV) memory. You must enter the password correctly before you can continue.
- **For the CoreBuilder 9000** — On this system, the Enterprise Management Engine (EME) controls passwords and access levels to manage the chassis and its installed modules.

To access a module in a CoreBuilder 9000 system, follow these steps:

- 1 Log in to the EME.
- 2 Access the module that you want to manage using the EME `connect` command.

Example: To connect to a module in slot 10, subslot 1, enter:

```
connect 10.1
```



All modules use subslot 1.

The system displays a prompt similar to the following:

```
CB9000@slot10.1 [20-E/FEN-TX-L2]
```

When you have connected to a module, you manage the module from the Administration Console with the same level of access that you have on the EME. For example, if you have logged in to the EME with *administer* privileges, you also have *administer* privileges for the module to which you are connected.



For additional information about the EME, see the CoreBuilder 9000 Enterprise Switch Getting Started Guide and the CoreBuilder 9000 Enterprise Management Engine User Guide.

- Access Examples** The examples in this section show how the top-level menu structure of the Administration Console changes. The menus that you see in the Administration Console vary depending on:
- Which 3Com system you are viewing (as described in "Accessing Your System" earlier in this chapter).
 - Your level of access.
 - The optional interface modules, switch fabric modules, and other hardware options that you configure into your system. For example, you see the `fddi` menu only if you have installed the FDDI module on your CoreBuilder 3500 system.



These examples show the CoreBuilder 3500 menus. Menus for other platforms may differ. See the Command Quick Reference for your system for the list of commands on your system.

Administer Access Example

When you enter the Administration Console with *Administer* access, each menu contains all of the options for the system. Here is an example of a system menu for users with *Administer* access on the CoreBuilder 3500:

Select menu option: `system`

```
Menu options (CoreBuilder-2B4200): -----
display           - Display the system configuration
console           - Administer console-level functions
fileTransfer      - Set the file transfer protocol
snapshot          - Display all configuration and status information
softwareUpdate    - Load a new revision of system software
baseline          - Administer a statistics baseline
serialPort        - Administer the terminal and modem serial ports
name              - Set the system name
time              - Set the date and time
nvData            - Save, restore, or reset nonvolatile data
clearDiagBlock    - Clear the diagnostic block
diagErrLog        - Display Diagnose Error Log
snTP              - Administer the Simple Network Time Protocol
reboot            - Reboot the system
```

Type "q" to return to the previous menu or ? for help.

Select menu option (system):

Write Access Example

When you enter the Administration Console with *write* access, the system menu contains a subset of the complete menu, focusing on the network, as shown in this example on the CoreBuilder 3500:

Select menu option: **system**

```
Menu options (CoreBuilder-2B4200): -----
display          - Display the system configuration
console          - Administer console-level functions
fileTransfer     - Set the file transfer protocol
snapshot         - Display all configuration and status information
baseline         - Administer a statistics baseline
serialPort       - Administer the terminal and modem serial ports
name             - Set the system name
diagErrLog       - Display Diagnose Error Log
sntp             - Administer the Simple Network Time Protocol
```

Type "q" to return to the previous menu or ? for help.

Read Access Example

When you enter the Administration Console with *read* access, the system menu contains the fewest options, as shown in this example on the CoreBuilder 3500:

Select menu option: **system**

```
Menu options (CoreBuilder-293300): -----
display          - Display the system configuration
snapshot         - Display all configuration and status information
baseline         - Administer a statistics baseline
diagErrLog       - Display Diagnose Error Log
sntp             - Administer the Simple Network Time Protocol
```

Type "q" to return to the previous menu or ? for help.

Using Menus to Perform Tasks

When you access the Administration Console, the top-level menu appears. You perform administrative tasks by selecting options from this menu and its submenus. A brief description accompanies each option in the display. The commands that you can use depend on the system that you have, your level of access, and the types of modules and other hardware options that are configured for your system. The “Menu Structure” diagrams at the beginning of most chapters show the complete list of commands for all systems. See the checklist at the beginning of each command description in each chapter for whether your system supports the command.

The following example shows the CoreBuilder 9000 top-level menu when a Layer 2 switching module is installed:

Menu options:

```
-----  
module           - Administer module-level functions  
ethernet         - Administer Ethernet ports  
bridge          - Administer bridging/VLANs  
snmp            - Administer SNMP  
disconnect      - Disconnect and return to the Management Console
```

Type ? for help.

Select a menu option:



These examples show the CoreBuilder 9000 menu options for a Layer 2 switching interface module. Menus on other platforms may differ. See the Command Quick Reference for the list of commands on your system.

Selecting Menu Options

To select a menu option, at the prompt enter the menu option or enough of the name to uniquely identify it within the particular menu. Example: to access the `module` menu from the top level of the Administration Console on a module in the CoreBuilder 9000, enter:

```
Select a menu option: module
```



Menu options are not case sensitive.

When you enter a menu option or command correctly, either you move to the next menu in the hierarchy, or the Administration Console displays information (a prompt or a screen display) for the option that you entered.

If you enter the menu option incorrectly, a message indicates that your entry is not valid or is ambiguous. Reenter the option from the point at which it became incorrect or expand a truncated command until it becomes unambiguous.

When a new menu appears, the selection prompt (with its choices in parentheses) changes to reflect your progression through the menus.

Example: If you enter `bridge` at the top-level menu and then `agingTime` at the `module` prompt, the prompt changes to reflect the current level:

```
Select a menu option (bridge/agingTime):
```

Entering a Command String

After you become familiar with the menu structure, you can enter a string of menu options or commands to move immediately to a task. Example: The command string for setting the path cost for a port on a module looks like this:

```
Select a menu option: bridge port stpCost
```

Entering Abbreviated Commands

You can abbreviate command strings by typing only as much of the command as is necessary to make it unique:

```
Select a menu option: b po stpc
```

When you correctly enter either a full or an abbreviated command string, you move to the last menu level or option that is specified in the string. Information that is relevant to that option appears as a menu, a prompt, or a display.

If you enter a command string incorrectly, the Administration Console displays a message indicating that your entry was not valid or was ambiguous. Reenter the command from the point at which it became incorrect, or expand a truncated command until it becomes unambiguous.

Entering Values

When you reach the level at which you perform a task, the Administration Console prompts you for a value. The prompt usually shows all valid values (if applicable) and typically suggests a default value. The default may be the factory default value or the current value that you have defined for that parameter.

The Administration Console displays the valid values in parentheses and the default or current value in brackets. For example:

```
Enter a new value (disabled,enabled) [enabled]:
```

To accept the default or current value, press Enter.

Entering Values in Command Strings

A command string can also contain the value of a command parameter. If you enter a value at the end of a command string, the Administration Console executes the task and the previous menu appears on the screen.

For example, to set the path cost to the root through a port, from the top level of the Administration Console, enter:

```
bridge port stpcost 20
```

or

```
b po stpc 20
```

Navigating Through the Menus

The Administration Console provides several shortcuts:

- **Press Esc (the Escape key)** — To move quickly to the top-level menu without backtracking through each intermediate menu. The top-level menu immediately appears.
- **Enter q** —
 - To move up through the hierarchy, that is, to move to the menu that is one level higher in the hierarchy
 - To cancel an operation that is currently in progress. The previous menu appears.

2

COMMAND SUMMARY

Table 6 gives an overview of all the commands in this book.

Table 6 Command Summary

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
PART II: System-Level Functions						
Chapter 3 System Environment						
system display	✓			✓	✓	✓
system fileTransfer	✓					
system console webHelpConfig	✓			✓	✓	✓
system console webAccess	✓			✓	✓	✓
system console consoleAccess	✓			✓	✓	✓
system console ctiKeys	✓			✓	✓	✓
system console password	✓			✓	✓	✓
system console screenHeight	✓			✓	✓	✓
system console security display	✓			✓	✓	✓
system console security define	✓			✓	✓	✓
system console security remove	✓			✓	✓	✓
system console security access	✓			✓	✓	✓
system console security message	✓			✓	✓	✓
system console timeout timeOut	✓			✓	✓	✓
system console timeout interval	✓			✓	✓	✓

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
system snapshot summary	✓			✓	✓	✓
system snapshot detail	✓			✓	✓	✓
system snapshot save	✓			✓	✓	✓
system softwareUpdate	✓			✓	✓	✓
system baseline display	✓			✓	✓	✓
system baseline set	✓			✓	✓	✓
system baseline requestedState	✓			✓	✓	✓
system serialPort terminalSpeed	✓					
system serialPort modemSpeed	✓					
system serialPort baudRate				✓	✓	✓
system serialPort serialPortMode				✓	✓	✓
system serialPort configModem	✓			✓	✓	✓
system serialPort enableModem	✓			✓	✓	✓
system name	✓			✓	✓	✓
system time dateTime	✓			✓	✓	✓
system time timezone	✓			✓	✓	✓
system time dst	✓			✓	✓	✓
system nvData save	✓			✓	✓	✓
system nvData restore	✓			✓	✓	✓
system nvData examine	✓			✓	✓	✓
system clearDiagBlock	✓			✓	✓	✓
system diagErrLog	✓					
system sntp display	✓			✓	✓	✓
system sntp define	✓			✓	✓	✓

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
system sntp modify	✓			✓	✓	✓
system sntp remove	✓			✓	✓	✓
system sntp state	✓			✓	✓	✓
system sntp pollInterval	✓			✓	✓	✓
system sntp tolerance	✓			✓	✓	✓
system reboot	✓			✓	✓	✓
script	✓			✓	✓	✓
logout	✓			✓	✓	✓
Ch 4 Module Environment						
module display		✓	✓			
module snapshot summary		✓	✓			
module snapshot detail		✓	✓			
module baseline display		✓	✓			
module baseline set		✓	✓			
module baseline requestedState		✓	✓			
module redundancy display		✓				
module redundancy reset NonRedundant		✓				
module name		✓	✓			
module time		✓	✓			
module screenHeight		✓	✓			
module nvData reset		✓	✓			
module nvData emergencyDownload		✓	✓			
module nvData displayDownload		✓	✓			
module nvData staging		✓	✓			

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
module clearDiagBlock		✓	✓			
module diagErrLog			✓			
module reboot		✓	✓			
disconnect		✓	✓			
PART III: Establishing Management Access						
Ch 5 Out-of-Band Management						
management summary	✓			✓		✓
management detail	✓			✓		✓
management ip	✓					
management ip interface summary	✓					
management ip interface define	✓					
management ip interface modify	✓					
management ip interface remove	✓					
management ip route display	✓					
management ip route static	✓					
management ip route remove	✓					
management ip route flush	✓					
management ip route default	✓					
management ip route noDefault	✓					
management ip route findRoute	✓					
management ip arp display	✓					
management ip arp static	✓					
management ip arp remove	✓					
management ip arp flushAll	✓					

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
management ip arp flushDynamic	✓					
management ip rip display	✓					
management ip rip mode	✓					
management ip rip statistics	✓					
management ip ping	✓					
management ip advancedPing	✓					
management ip traceRoute	✓					
management ip advancedTraceRoute	✓					
management ip statistics	✓					
Ch 6 SNMP						
snmp display	✓	✓	✓	✓	✓	✓
snmp community	✓			✓	✓	✓
snmp trap display	✓	✓	✓	✓	✓	✓
snmp trap addModify	✓	✓	✓	✓	✓	✓
snmp trap remove	✓	✓	✓	✓	✓	✓
snmp trap flush	✓	✓	✓	✓	✓	✓
snmp trap smtProxyTraps	✓		✓			
snmp rmonConfiguration	✓		✓			
snmp writeDisable	✓		✓	✓	✓	✓
Part IV Physical Port Parameters						
Ch 7 Ethernet Ports						
ethernet summary	✓	✓	✓	✓	✓	✓
ethernet detail	✓	✓	✓	✓	✓	✓
ethernet autoNegotiation	✓	✓	✓	✓	✓	✓

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
ethernet portMode	✓	✓	✓		✓	
ethernet flowControl	✓	✓	✓	✓	✓	✓
ethernet paceInteractiveAccess	✓		✓			
ethernet paceAccess		✓			✓	
ethernet label	✓	✓	✓	✓	✓	✓
ethernet portState	✓	✓	✓	✓	✓	✓
ethernet monitoring summary		✓			✓	
ethernet monitoring mode		✓			✓	
Ch 8 FDDI						
fddi station display	✓		✓			
fddi station connectPolicy	✓		✓			
fddi station tNotify	✓		✓			
fddi station statusReporting	✓		✓			
fddi path display	✓		✓			
fddi path tvxLowerBound	✓		✓			
fddi path tmaxLowerBound	✓		✓			
fddi path maxTreq	✓		✓			
fddi mac summary	✓		✓			
fddi mac detail	✓		✓			
fddi mac frameErrorThreshold	✓		✓			
fddi mac notCopiedThreshold	✓		✓			
fddi mac llcService	✓		✓			
fddi mac path	✓		✓			
fddi port display	✓		✓			

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
fddi port lerAlarm	✓		✓			
fddi port lerCutoff	✓		✓			
fddi port label	✓		✓			
fddi port path	✓		✓			
fddi stationMode display	✓		✓			
fddi stationMode modify	✓		✓			
Part V Bridging Parameters						
Ch 9 Bridge-wide Parameters						
bridge display	✓	✓	✓	✓	✓	✓
bridge ipFragmentation	✓		✓			
bridge ipxSnapTranslation	✓		✓			
bridge addressThreshold	✓		✓			
bridge agingTime	✓	✓	✓	✓	✓	✓
bridge spanningTree stpState	✓	✓	✓	✓	✓	✓
bridge spanningTree stpPriority	✓	✓	✓	✓	✓	✓
bridge spanningTree stpMaxAge	✓	✓	✓	✓	✓	✓
bridge spanningTree stpHelloTime	✓	✓	✓	✓	✓	✓
bridge spanningTree stpForwardDelay	✓	✓	✓	✓	✓	✓
bridge spanningTree stpGroupAddress	✓	✓	✓	✓	✓	✓
bridge gvrpState	✓		✓			
bridge cos enable		✓		✓	✓	✓
bridge cos summary		✓		✓	✓	✓
bridge cos modify		✓		✓	✓	✓
bridge multicast igmp summary		✓		✓	✓	✓

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
bridge multicast igmp snoopMode		✓		✓	✓	✓
bridge multicast igmp queryMode		✓		✓	✓	✓
bridge multicast igmp queryIpAddress		✓		✓	✓	✓
bridge multicast igmp vlans		✓		✓	✓	✓
bridge multicast igmp groups		✓		✓	✓	✓
bridge multicast igmp desQuerier		✓		✓	✓	✓
bridge multicast igmp rPorts		✓		✓	✓	✓
bridge multicast igmp qPort		✓		✓	✓	✓
Ch 10 Bridge Ports						
bridge port summary	✓	✓	✓	✓	✓	✓
bridge port detail	✓	✓	✓	✓	✓	✓
bridge port multicastLimit	✓	✓	✓	✓	✓	✓
bridge port stpState	✓	✓	✓	✓	✓	✓
bridge port stpCost	✓	✓	✓	✓	✓	✓
bridge port stpPriority	✓	✓	✓	✓	✓	✓
bridge port gvrpState	✓		✓			
bridge port address list	✓	✓	✓	✓	✓	✓
bridge port address add	✓	✓	✓	✓	✓	✓
bridge port address remove	✓	✓	✓	✓	✓	✓
bridge port address find	✓	✓	✓	✓	✓	✓
bridge port address flushAll	✓	✓	✓	✓	✓	✓
bridge port address flushDynamic	✓	✓	✓	✓	✓	✓

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
Ch 11 Trunks						
bridge trunk autoMap summary		✓				
bridge trunk autoMap enable		✓				
bridge trunk autoMap disable		✓				
bridge trunk autoMap test		✓				
bridge trunk summary	✓	✓	✓	✓	✓	✓
bridge trunk detail	✓	✓	✓	✓	✓	✓
bridge trunk define	✓	✓	✓	✓	✓	✓
bridge trunk modify	✓	✓	✓	✓	✓	✓
bridge trunk remove	✓	✓	✓	✓	✓	✓
Ch 12 MultiPoint Link Aggregation						
bridge mpla summary				✓		
bridge mpla detail				✓		
bridge mpla mode				✓		
bridge mpla peerMacAddress				✓		
Ch 13 Resilient Links						
bridge link summary		✓		✓	✓	✓
bridge link detail		✓		✓	✓	✓
bridge link define		✓		✓	✓	✓
bridge link linkState		✓		✓	✓	✓
bridge link activePort		✓		✓	✓	✓
bridge link modify		✓		✓	✓	✓
bridge link remove		✓		✓	✓	✓

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
Ch 14 Virtual LANs (VLANs)						
bridge vlan summary	✓	✓	✓	✓	✓	✓
bridge vlan detail	✓	✓	✓	✓	✓	✓
bridge vlan define	✓	✓	✓	✓	✓	✓
bridge vlan modify	✓	✓	✓	✓	✓	✓
bridge vlan remove	✓	✓	✓	✓	✓	✓
bridge vlan mode	✓	✓	✓	✓	✓	✓
bridge vlan stpMode	✓		✓			
bridge vlan vlanAwareMode	✓		✓			
Ch 15 Packet Filters						
bridge packetFilter list	✓		✓			
bridge packetFilter display	✓		✓			
bridge packetFilter create	✓		✓			
bridge packetFilter delete	✓		✓			
bridge packetFilter edit	✓		✓			
bridge packetFilter load	✓		✓			
bridge packetFilter assign	✓		✓			
bridge packetFilter unassign	✓		✓			
bridge packetFilter portGroup list	✓		✓			
bridge packetFilter portGroup display	✓		✓			
bridge packetFilter portGroup create	✓		✓			
bridge packetFilter portGroup delete	✓		✓			
bridge packetFilter portGroup addPort	✓		✓			
bridge packetFilter portGroup removePort	✓		✓			

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
Part VI Routing Protocols						
Ch 16 IP						
ip interface summary	✓		✓	✓	✓	✓
ip interface detail	✓		✓			
ip interface define	✓		✓	✓	✓	✓
ip interface modify	✓		✓	✓	✓	✓
ip interface remove	✓		✓	✓	✓	✓
ip interface arpProxy	✓		✓			
ip interface broadcastAddress	✓		✓			
ip interface directedBroadcast	✓		✓			
ip interface icmpRedirect	✓		✓			
ip interface icmpRouterDiscovery	✓		✓			
ip interface statistics	✓		✓			
ip route display	✓		✓	✓	✓	✓
ip route static	✓		✓	✓	✓	✓
ip route remove	✓		✓	✓	✓	✓
ip route flush	✓		✓	✓	✓	✓
ip route default	✓		✓	✓	✓	✓
ip route noDefault	✓		✓	✓	✓	✓
ip route findRoute	✓		✓	✓	✓	✓
ip arp display	✓		✓	✓	✓	✓
ip arp static	✓		✓	✓	✓	✓
ip arp remove	✓		✓	✓	✓	✓
ip arp flushAll	✓		✓	✓	✓	✓

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
ip arp flushDynamic	✓		✓	✓	✓	✓
ip arp age	✓		✓			
ip arp statistics	✓		✓			
ip dns display	✓		✓	✓	✓	✓
ip dns domainName	✓		✓	✓	✓	✓
ip dns define	✓		✓	✓	✓	✓
ip dns modify	✓		✓	✓	✓	✓
ip dns remove	✓		✓	✓	✓	✓
ip dns nslookup	✓		✓	✓	✓	✓
ip udpHelper display	✓		✓			
ip udpHelper define	✓		✓			
ip udpHelper remove	✓		✓			
ip udpHelper hopCountLimit	✓		✓			
ip udpHelper threshold	✓		✓			
ip udpHelper interface first	✓		✓			
ip udpHelper interface even	✓		✓			
ip udpHelper interface sequential	✓		✓			
ip routing	✓		✓			
ip rip display	✓		✓	✓	✓	✓
ip rip mode	✓		✓	✓	✓	✓
ip rip compatibilityMode	✓		✓			
ip rip cost	✓		✓			
ip rip poisonReverse	✓		✓			
ip rip routeAggregationMode	✓		✓			

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
ip rip password	✓		✓			
ip rip addAdvertisement	✓		✓			
ip rip removeAdvertisement	✓		✓			
ip rip policy summary	✓		✓			
ip rip policy detail	✓		✓			
ip rip policy define	✓		✓			
ip rip policy modify	✓		✓			
ip rip policy remove	✓		✓			
ip rip statistics	✓		✓	✓	✓	✓
ip ping	✓		✓	✓	✓	✓
ip advancedPing	✓		✓	✓	✓	✓
ip traceRoute	✓		✓	✓	✓	✓
ip advancedTraceRoute	✓		✓	✓	✓	✓
ip statistics	✓		✓	✓	✓	✓
Ch 17 VRRP						
ip vrrp summary	✓		✓			
ip vrrp detail	✓		✓			
ip vrrp define	✓		✓			
ip vrrp modify	✓		✓			
ip vrrp remove	✓		✓			
ip vrrp mode	✓		✓			
ip vrrp neighbor	✓		✓			
ip vrrp statistics	✓		✓			

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
Ch 18 IP Multicast						
ip multicast dvmrp interface summary	✓		✓			
ip multicast dvmrp interface detail	✓		✓			
ip multicast dvmrp interface mode	✓		✓			
ip multicast dvmrp interface metric	✓		✓			
ip multicast dvmrp tunnels summary	✓		✓			
ip multicast dvmrp tunnels define	✓		✓			
ip multicast dvmrp tunnels remove	✓		✓			
ip multicast dvmrp tunnels address	✓		✓			
ip multicast dvmrp tunnels threshold	✓		✓			
ip multicast dvmrp tunnels metric	✓		✓			
ip multicast dvmrp routeDisplay	✓		✓			
ip multicast dvmrp cacheDisplay	✓		✓			
ip multicast dvmrp default	✓		✓			
ip multicast igmp interface summary	✓		✓			
ip multicast igmp interface detail	✓		✓			
ip multicast igmp interface TTL	✓		✓			
ip multicast igmp snooping	✓		✓			
ip multicast igmp querying	✓		✓			
ip multicast cache	✓		✓			
ip multicast traceRoute	✓		✓			

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
Ch 19 OSPF						
ip ospf areas display	✓		✓			
ip ospf areas defineArea	✓		✓			
ip ospf areas modifyArea	✓		✓			
ip ospf areas removeArea	✓		✓			
ip ospf areas addRange	✓		✓			
ip ospf areas modifyRange	✓		✓			
ip ospf areas removeRange	✓		✓			
ip ospf defaultRouteMetric display	✓		✓			
ip ospf defaultRouteMetric define	✓		✓			
ip ospf defaultRouteMetric remove	✓		✓			
ip ospf interface summary	✓		✓			
ip ospf interface detail	✓		✓			
ip ospf interface statistics	✓		✓			
ip ospf interface mode	✓		✓			
ip ospf interface priority	✓		✓			
ip ospf interface areaID	✓		✓			
ip ospf interface cost	✓		✓			
ip ospf interface delay	✓		✓			
ip ospf interface hello	✓		✓			
ip ospf interface retransmit	✓		✓			
ip ospf interface dead	✓		✓			
ip ospf interface password	✓		✓			
ip ospf linkStateData databaseSummary	✓		✓			

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
ip ospf linkStateData router	✓		✓			
ip ospf linkStateData network	✓		✓			
ip ospf linkStateData summary	✓		✓			
ip ospf linkStateData external	✓		✓			
ip ospf neighbors display	✓		✓			
ip ospf neighbors add	✓		✓			
ip ospf neighbors remove	✓		✓			
ip ospf routerID	✓		✓			
ip ospf partition display	✓		✓			
ip ospf partition modify	✓		✓			
ip ospf stubDefaultMetric display	✓		✓			
ip ospf stubDefaultMetric define	✓		✓			
ip ospf stubDefaultMetric remove	✓		✓			
ip ospf virtualLinks summary	✓		✓			
ip ospf virtualLinks detail	✓		✓			
ip ospf virtualLinks statistics	✓		✓			
ip ospf virtualLinks define	✓		✓			
ip ospf virtualLinks remove	✓		✓			
ip ospf virtualLinks areaID	✓		✓			
ip ospf virtualLinks router	✓		✓			
ip ospf virtualLinks delay	✓		✓			
ip ospf virtualLinks hello	✓		✓			
ip ospf virtualLinks retransmit	✓		✓			
ip ospf virtualLinks dead	✓		✓			

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
ip ospf virtualLinks password	✓		✓			
ip ospf policy summary	✓		✓			
ip ospf policy detail	✓		✓			
ip ospf policy define	✓		✓			
ip ospf policy modify	✓		✓			
ip ospf policy remove	✓		✓			
ip ospf statistics	✓		✓			
Ch 20 IPX						
ipx interface display	✓		✓			
ipx interface define	✓		✓			
ipx interface modify	✓		✓			
ipx interface remove	✓		✓			
ipx interface SAPadvertising	✓		✓			
ipx interface RIPadvertising	✓		✓			
ipx route display	✓		✓			
ipx route secondary	✓		✓			
ipx route static	✓		✓			
ipx route remove	✓		✓			
ipx route flush	✓		✓			
ipx server display	✓		✓			
ipx server static	✓		✓			
ipx server remove	✓		✓			
ipx server flush	✓		✓			
ipx server secondary	✓		✓			

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
ipx forwarding	✓		✓			
ipx rip mode	✓		✓			
ipx rip triggered	✓		✓			
ipx rip policy summary	✓		✓			
ipx rip policy define	✓		✓			
ipx rip policy modify	✓		✓			
ipx rip policy remove	✓		✓			
ipx sap mode	✓		✓			
ipx sap triggered	✓		✓			
ipx sap policy summary	✓		✓			
ipx sap policy detail	✓		✓			
ipx sap policy define	✓		✓			
ipx sap policy modify	✓		✓			
ipx sap policy remove	✓		✓			
ipx output-delay	✓		✓			
ipx statistics summary	✓		✓			
ipx statistics rip	✓		✓			
ipx statistics sap	✓		✓			
ipx statistics forwarding	✓		✓			
ipx statistics interface	✓		✓			
ipx oddLengthPadding	✓		✓			
ipx NetBIOS	✓		✓			
ipx secondary	✓		✓			

Table 6 Command Summary (continued)

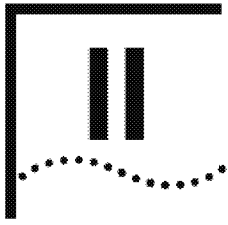
Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
Ch 21 AppleTalk						
appletalk interface summary	✓		✓			
appletalk interface detail	✓		✓			
appletalk interface define	✓		✓			
appletalk interface modify	✓		✓			
appletalk interface remove	✓		✓			
appletalk interface statistics	✓		✓			
appletalk route display	✓		✓			
appletalk route flush	✓		✓			
appletalk aarp display	✓		✓			
appletalk aarp remove	✓		✓			
appletalk aarp flush	✓		✓			
appletalk zone display network	✓		✓			
appletalk zone display zone	✓		✓			
appletalk forwarding	✓		✓			
appletalk checksum	✓		✓			
appletalk sourceSocket	✓		✓			
appletalk ping	✓		✓			
appletalk statistics ddp	✓		✓			
appletalk statistics rtrmp	✓		✓			
appletalk statistics zip	✓		✓			
appletalk statistics nbp	✓		✓			

Table 6 Command Summary (continued)

Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
Part VII Traffic Policy						
Ch 22 Quality of Service and RSVP						
qos classifier summary	✓		✓			
qos classifier detail	✓		✓			
qos classifier define	✓		✓			
qos classifier modify	✓		✓			
qos classifier remove	✓		✓			
qos control summary	✓		✓			
qos control detail	✓		✓			
qos control define	✓		✓			
qos control modify	✓		✓			
qos control remove	✓		✓			
qos ldap display	✓					
qos ldap enable	✓					
qos ldap disable	✓					
qos rsvp summary	✓		✓			
qos rsvp detail	✓		✓			
qos rsvp enable	✓		✓			
qos rsvp disable	✓		✓			
qos bandwidth display	✓		✓			
qos bandwidth modify	✓		✓			
qos excessTagging display	✓		✓			
qos excessTagging enable	✓		✓			
qos excessTagging disable	✓		✓			

Table 6 Command Summary (continued)

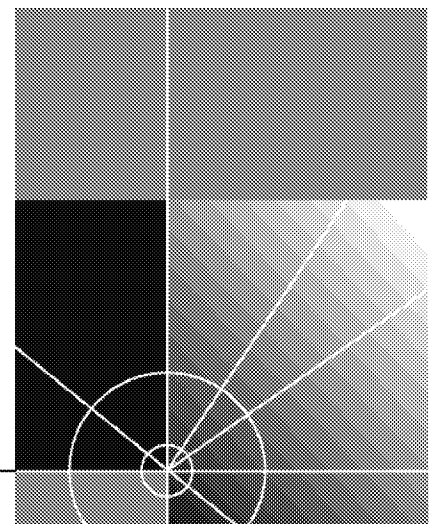
Commands	3500	9000: Layer 2	9000: Layer 3	9400	3900	9300
qos statistics interval	✓		✓			
qos statistics receive	✓		✓			
qos statistics transmit	✓		✓			
Part VIII Monitoring						
Ch 23 Event Log						
log display	✓					
log devices	✓					
log services	✓					
Ch 24 Roving Analysis						
analyzer display	✓	✓	✓	✓	✓	✓
analyzer add	✓	✓	✓	✓	✓	✓
analyzer remove	✓	✓	✓	✓	✓	✓
analyzer start	✓	✓	✓	✓	✓	✓
analyzer stop	✓	✓	✓	✓	✓	✓



SYSTEM-LEVEL FUNCTIONS

Chapter 3 System Environment

Chapter 4 Module Environment



3

SYSTEM ENVIRONMENT

This chapter provides guidelines and other key information about how to use `system` commands to:

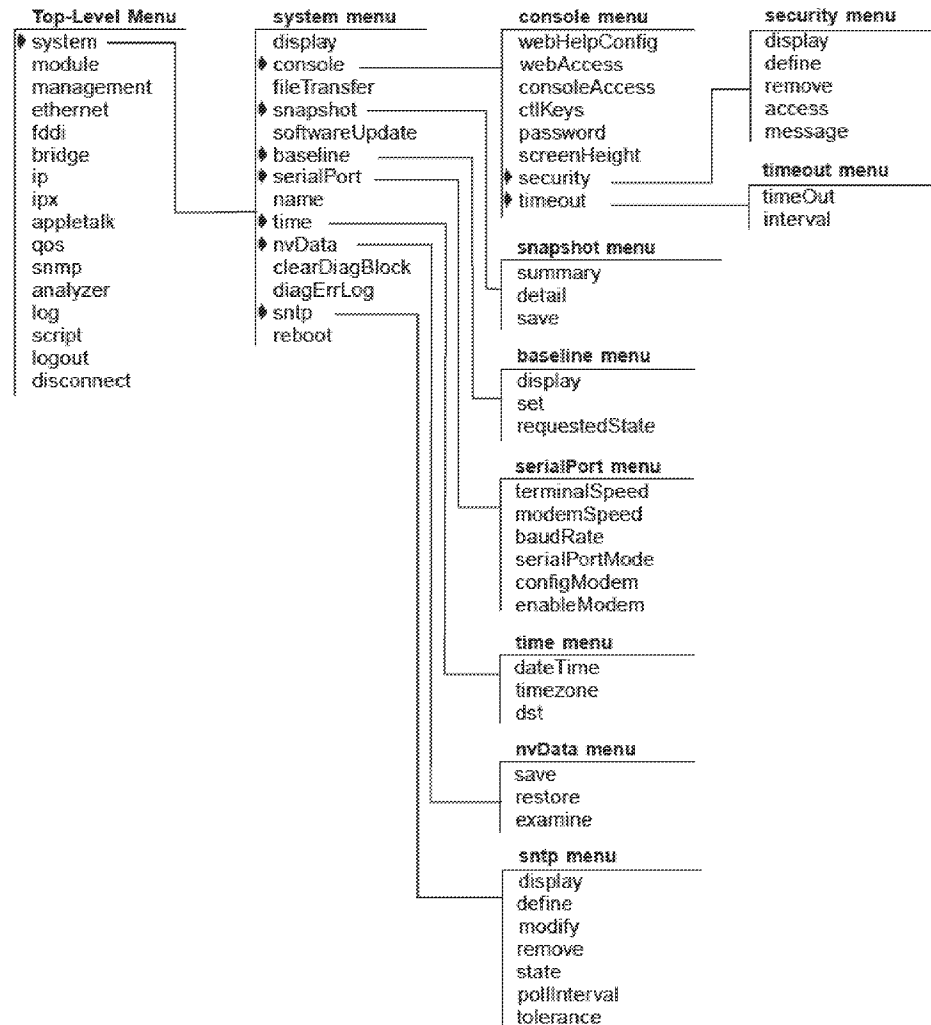
- Set and modify general system parameters. Important considerations and options are also provided where applicable
- Configure management access to the system (through one of two serial connection types)
- Configure management access through the serial port. (For information about commands for configuring an out-of-band management interface, see Chapter 5.)



For more information about administering your system environment, see the Implementation Guide for your system.

Menu Structure

The commands that you can use depend on the system that you have, your level of access, and the types of modules and other hardware that are configured for your system. The following diagram shows the complete list of commands for all systems. See the checklist at the beginning of each command description in this chapter for whether your system supports the command.



In addition, this chapter describes the `script` and `logout` options from the top-level menu.

system display

Generates a system configuration display that includes software and hardware revision numbers, module status information, and warning messages for certain system conditions.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy d

Important Consideration

- A message appears in the display if any module fails a diagnostic test at start-up.

Fields in the System Display

Field	Description
Diagnostics	Whether a module has passed or failed diagnostics
Memory size (AP, FP, Flash, and Buffer)	Memory capacities of the system processors
POV	Power on verification
SysBoot	Boot software revision
ExtDiags	Extended diagnostics version number
Part number	Each module's 3Com part identification number
Product number	Each module's 3Com 3C product identification number
Rev	Unique number assigned to the hardware build by 3Com
Serial number	Each module's unique serial number
Slot number	Slot position of each hardware module
System ID	Unique number that is assigned to the system by 3Com
System name	64-character (maximum) user-defined alphanumeric name that uniquely identifies the system on your network
System up time	Time since the last system reboot
Time in service	Total operational time since the system was manufactured
Type of module	Type of physical ports
Version, build date, and time	System software version number, and date and time when the software was built



You configure the system parameters for the CoreBuilder® 9000 system through the Enterprise Management Engine (EME). See the CoreBuilder 9000 Enterprise Management Engine User Guide for a complete list and detailed explanation of the CoreBuilder 9000 system commands.

system fileTransfer Sets the file transfer protocol to either Trivial File Transfer Protocol (TFTP) or File Transfer Protocol (FTP). Use this protocol to retrieve or store files across the network for system functions such as scripts, snapshots, software updates, and nvData save and restore.

✓ 3500
9000
9400

3900
9300

Valid Minimum Abbreviation

sy £

Options

Prompt	Description	Possible Values	[Default]
File transfer protocol	File transfer protocol for the system	<ul style="list-style-type: none"> ■ TFTP ■ FTP 	TFTP

**system console
webHelpConfig**

Sets the Uniform Resource Locator (URL) for access to the Web Management Help system.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy co wh

Options

Prompt	Description	Possible Values	[Default]
Enter Web help installation URL	URL where the Web Management Help system files are located	–	–

system console
webAccess

Enables or disables access to the Web Management software.

Valid Minimum Abbreviation

sy co w

Options

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Prompt	Description	Possible Values	[Default]
Web management	Whether remote access to the Web Management system is allowed	<ul style="list-style-type: none"> ■ enabled ■ disabled 	enabled

**system console
consoleAccess**

Controls remote access via Telnet or modem to the system console.

Valid Minimum Abbreviation

sy co co

Options

- 3500
- 9000
- ✓ 9400
- ✓ 3900
- ✓ 9300

Prompt	Description	Possible Values	[Default]
Console access	Whether remote access to the system console is allowed	<ul style="list-style-type: none"> ■ enabled ■ disabled 	enabled

system console Enables or disables the control key combination (default: Ctrl+X) that
ctlKeys allows you to reboot the system from the Administration Console.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy co ct

Options

Prompt	Description	Possible Values	[Default]
Control keys	Whether you want to enable or disable the reboot control key combination	<ul style="list-style-type: none"> ■ enabled ■ disabled 	enabled

**system console
password**

Sets one of the password levels for the Administration Console. There are three levels of password for the Administration Console.

✓ 3500
9000
✓ 9400

Valid Minimum Abbreviation

sy co p

✓ 3900
✓ 9300

Important Considerations

- The Administration Console supports three levels of access:
 - One for only browsing or viewing (*read*)
 - One for configuring network parameters (*write*)
 - One for full system administration (*administer*)
- When you log on for the first time, press Return or Enter at the password prompt because the initial passwords that are stored in the nonvolatile memory of the system are null for all access levels.
- To change passwords, you must enter the Console at the *administer* access level.
- The system does not display the password in the field as you type.
- Set a password for each access level that you want to configure.

Options

Prompt	Description	Possible Values	[Default]
Access level	Level of access for the person logging on to the system	<ul style="list-style-type: none"> ■ read ■ write ■ administer 	read
Password	Text string typed by the person logging on	<ul style="list-style-type: none"> ■ A string of up to 32 case-sensitive characters ■ Enter (for a null password) 	–

**system console
screenHeight**

Changes the Administration Console's screen height to increase or decrease the space available for displaying information.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy co sc

Important Considerations

- The setting controls the way that the system displays statistical summaries or other information that results from your use of the menus, not the way that the system displays the menus themselves.
- Each time that the screen output reaches the designated screen height, the system prompts you to press a key to display more information. Set the screen height to infinite (0) if you do not want the system to display this prompt. At 0, however, the screen output can scroll beyond the screen, depending on your screen size.
- Most terminal screens are 24 lines high.

Options

Prompt	Description	Possible Values	[Default]
New screen height	New screen height in lines	<ul style="list-style-type: none"> ■ 20 – 200 ■ 0 (to receive no prompts) 	24
Default value	Default screen height for future Administration Console sessions	<ul style="list-style-type: none"> ■ y (yes) ■ n (no) 	y

**system console
security display**

Displays a summary of trusted IP client information.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy co se di

Important Consideration

- If you do not have any trusted IP clients configured, this command displays only the first two fields.

Fields in the System Console Security Display

Field	Description
Trusted client access only	Whether the trusted IP client feature is enabled or disabled
Deny message	Text of the current message that is sent to a user who is not a trusted client
Index	Index number that is associated with the trusted IP client
Trusted IP address	IP address of the trusted IP client
Mask	Subnet mask that is associated with the trusted IP address

**system console
security define**

Gives a client trusted access to your system by adding the client IP address and subnet mask to an access list.

✓ 3500
9000
✓ 9400

Valid Minimum Abbreviation

sy co se de

✓ 3900
✓ 9300

**Important Considerations**

CAUTION: Be careful when you define trusted IP clients. If you specify an incorrect IP address or subnetwork address when you define a trusted IP client, you can affect your own ability to access the system. See the Implementation Guide for your system.

- Configure trusted IP clients in this order:
 - Define the trusted IP clients using `system console security define`.
 - Display the list of configured trusted IP clients using `system console security display` to verify that you have configured the trusted IP clients correctly.
 - Enable the system to verify trusted IP clients using `system console security access`.
- You can configure up to five IP addresses or five subnetwork addresses as trusted IP clients.
- An IP address or subnetwork address can be used to access the system only if it is on the trusted IP client list.
- Use the subnet mask to allow trusted access to all addresses on a particular subnetwork. Examples: The IP address 158.99.112.219 with a subnet mask of 255.255.255.0 allows trusted access to all addresses on the 158.99.112 subnetwork. The IP address 158.99.112.219 with a subnet mask of 255.255.255.255 allows access only by the single IP address 158.99.112.219.
- The trusted IP client information is retained after a system reboot; that is, it is saved in nvData.

Options

Prompt	Description	Possible Values	[Default]
IP address	IP address of the interface, chosen from the range of addresses that are assigned to your organization. This address is specific to your network and system.	Any valid IP address	–
Subnet mask	32-bit number that uses the same format and representation as an IP address. The subnet mask determines which bits in the IP address are interpreted as the network number, the subnet number, and the host number. Each IP address bit that corresponds to a 1 in the subnet mask is in the network/subnet part of the address. Each IP address bit that corresponds to a 0 is in the host part of the IP address.	A valid subnet mask in accordance with the bits used for network number, subnet, and host number	Depends on specified IP address

**system console
security remove**

Removes an IP address from the trusted IP client access list.

Valid Minimum Abbreviation

sy co se r

Important Considerations

- If you remove a trusted IP client definition through the Administration Console, the definition is also removed in the Web Management Console, and vice versa.
- This command takes effect immediately. You are not prompted to confirm the deletion.

Options

Prompt	Description	Possible Values	[Default]
Trusted IP client index	One or more index numbers of the IP addresses that you want to remove	<ul style="list-style-type: none"> ■ 1 – 5 ■ all ■ ? (for a list of selectable indexes) 	1 (if only one client)

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

system console security access

Enables or disables whether the system verifies trusted IP clients on your system.

- ✓ 3500
- 9000
- ✓ 9400

Valid Minimum Abbreviation

sy co se a

- ✓ 3900
- ✓ 9300

**Important Considerations**

CAUTION: Be careful when you define trusted IP clients. If you specify an incorrect IP address or subnetwork address when you define a trusted IP client, you can affect your own ability to access the system. See the Implementation Guide for your system.

- Configure trusted IP clients in this order:
 - Define the trusted IP clients using `system console security define`.
 - Display the list of configured trusted IP clients using `system console security display` to verify that you have configured the trusted IP clients correctly.
 - Enable the system to verify trusted IP clients using `system console security access`.

Options

Prompt	Description	Possible Values	[Default]
Trusted client access only	Whether you want to allow or disallow your system to restrict access according to your list of trusted IP clients	<ul style="list-style-type: none"> ■ enabled ■ disabled 	disabled

**system console
security message**

Defines the text that is displayed to a prospective user when access to your system is denied.

✓ 3500

9000

✓ 9400

Valid Minimum Abbreviation

sy co se m

Important Consideration

- Use `system console security display` to view the text of the current deny message.

✓ 3900

✓ 9300

Options

Prompt	Description	Possible Values	[Default]
Deny message	Text that is displayed to a prospective user whose IP address does not appear on the list of trusted users	Alphanumeric text of up to 85 characters and spaces	"You are not considered a trusted user. Please see your network administrator."

**system console
timeout timeOut**

Configures the system to disconnect remote sessions after a specified interval of no activity.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy co t t

Important Considerations

- The default inactive time interval is 30 minutes.
- To change the timeout interval value before the system disconnects remote sessions, see "system console timeout interval" next for details.

Options

Prompt	Description	Possible Values	[Default]
Timeout state	Whether you want to enable or disable the timeout state	<ul style="list-style-type: none"> ■ enabled ■ disabled 	disabled

**system console
timeout interval**

Sets the remote timeout interval to a value from 1 minute through 60 minutes.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy co t i

Important Consideration

- To enable or disable the inactive timeout interval for remote sessions, see the preceding command, “system console timeout timeOut” for details.

Options

Prompt	Description	Possible Values	[Default]
Telnet timeout interval	Timeout interval	1 – 60 minutes	30

**system snapshot
summary**

Captures an image of all system summary display screens. This display reflects each application's status at the time that you use the snapshot feature.

✓ 3500

9000

✓ 9400

Valid Minimum Abbreviation

sy sn su

✓ 3900

✓ 9300

**system snapshot
detail**

Captures an image of all system detail screens. The display reflects the current values of all fields and counters at the time that you use the snapshot feature.

✓ 3500

9000

✓ 9400

Valid Minimum Abbreviation

sy sn d

✓ 3900

✓ 9300

system snapshot save Sends detail screens to a file on the host machine that you specify.

- ✓ 3500
- 9000
- ✓ 9400

Valid Minimum Abbreviation

sy sn sa

Important Considerations

- ✓ 3900
 - ✓ 9300
- The CoreBuilder 3500 uses the Trivial File Transfer Protocol (TFTP) or File Transfer Protocol (FTP) to transfer the files to the host, depending on the setting for the `system fileTransfer` option. The SuperStack® II Switch 3900, Switch 9300, and the CoreBuilder 9400 use TFTP to transfer files.

Before you transfer files:

- You must create the file to receive the snapshot images on an FTP or TFTP server *before* you send the images to the file.
- You supply the IP address of the host and specify the file according to the requirements of your TFTP or FTP implementation.
- Some TFTP implementations require that you store the file in the same directory in which the TFTP daemon (server) is running on the remote host.
- Because TFTP provides no user authentication, give the file *loose* permissions to make it publicly readable and writable. TFTP servers do not grant requests for file access.
- On the CoreBuilder 3500, if you use FTP for `system fileTransfer`, you must enter a login name and password if you are sending a file to an FTP server.

TFTP Procedure

- 1 Create an empty file with open write permissions on the host to store the system display images.
- 2 From the top level of the Administration Console, enter:
`system snapshot save`
- 3 Enter the IP address of the host on which you want to save the display images.
- 4 If your TFTP implementation requires a full path name, enter the full path of the file that is designated to contain the display images. (Some implementations allow you to specify only the file name and the system uses the default TFTP directory.)

While the system sends the files to the host, it displays the name of each display image that it transfers. When the transmission is complete, the system displays a message that the transfer is complete and displays the file name and the name of the host on which it stored the file.

FTP Procedure (3500 Only)

- 1 Create an empty file with open write permissions on the host to store the system display images.
- 2 From the top level of the Administration Console, enter:
`system snapshot save`
- 3 Enter the IP address of the host on which you want to save the display images.
- 4 Enter the full pathname of the file that you designated.
- 5 Enter your username and password.

While the system sends the files to the host, it displays the name of each display image that it transfers. When the transmission is complete, the system displays a message that the transfer is complete and displays the file name and the name of the host on which it stored the file.

**system
softwareUpdate**

Loads a new revision of system software.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy so

Important Considerations

- The CoreBuilder 3500 uses the Trivial File Transfer Protocol (TFTP) or File Transfer Protocol (FTP) to transfer the files to the host, depending on the setting for the `system fileTransfer` option. The SuperStack II Switch 3900, Switch 9300, and the CoreBuilder 9400 use TFTP to transfer files.
- Before you attempt to install the system software, make sure that you have extended memory installed on your system.
- You can load the system software into flash memory while the system is operating. The system does not have to be powered down.
- Make sure that the FTP server or TFTP server software is running on the device from which you are installing the software.
- Make sure that you have defined an IP address on your system.
- Some FTP servers or TFTP servers do not accept the full pathname. If this is true on your server, enter the image filename only.
- On the CoreBuilder 3500, if you are using the FTP file transfer protocol, you must enter a login name and password.

Options

Prompt	Description	Possible Values	[Default]
Host IP address	IP address of the machine from which to load the software update	Any valid IP address	–
Install file name	Name of the image to be loaded	–	–

**system baseline
display**

Displays when the current baseline was last set.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy b d

Important Considerations

- Use this command to determine if you need a newer baseline for viewing statistics.
- The system also indicates if you have not yet set a baseline on the system.

system baseline set Resets the baseline counters to zero.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy b s

Important Considerations

- Baselining is automatically enabled when you set a baseline.
- The system maintains the accumulated totals since power-up.
- The baseline is time-stamped.

**system baseline
requestedState**

Enables or disables a baseline.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy b r

Important Considerations

- When you reenable a baseline, the counters return to the values that have accumulated since the most recent baseline that you set.
- Disabling a baseline returns the counters to the total accumulated values since the last power-up.

Options

Prompt	Description	Possible Values	[Default]
New value	Whether you want to enable or disable the baseline	<ul style="list-style-type: none"> ■ enabled ■ disabled 	enabled

**system serialPort
terminalSpeed**

Sets the terminal speed of your system serial port. The terminal speed is set by changing the terminal connection port baud rates.

✓ 3500
9000
9400

3900
9300

Valid Minimum Abbreviation

sy se t

Important Considerations

- When you change the terminal port baud rate to something other than 9600, the new setting becomes the new default, even after you use the `system nvData reset` option.
- You must adjust the baud setting of your terminal or terminal emulator to match your system serial port's baud rate before you can reestablish communication using the terminal port.
- You can use this command through the terminal serial port or through a Telnet session. However, if you change the terminal speed while you are in a Telnet session, you must reboot the system for the change to take effect.

Options

Prompt	Description	Possible Values	[Default]
Terminal speed	Signal speed for the terminal connection	<ul style="list-style-type: none"> ■ 19200 ■ 9600 ■ 4800 ■ 2400 ■ 1200 	9600
Confirmation	Confirmation of terminal speed change	<ul style="list-style-type: none"> ■ y (yes) ■ n (no) 	–

Procedure (Local Connection)

- 1 To set the terminal speed for the serial port, from the top level of the Administration Console, enter:

```
system serialPort terminalSpeed
```

- 2 Enter the terminal speed setting for the serial port. See the Options table for supported terminal speed rates.

The system response depends on the cable status.



The terminal speed is referred to as baud rate in the following messages.

If the cable is connected to the terminal port when you set the terminal speed for that port, the system displays the following message:

```
Changing the baud rate may cause a loss of communication
since you are currently connected via the serial port.
```

```
Are you sure you want to change the baud rate? (y/n):
```

- If you respond **y** (yes), the serial port's baud rate is changed immediately, and you lose the ability to communicate with any devices connected to the port until you adjust the device baud setting to match.
- If you respond **n** (no), the rate does not change, and the display returns to the previous menu.

Procedure (IP Interface)

- 1 From the top level of the Administration Console, enter:
`system serialPort terminalSpeed`
- 2 Enter the terminal speed setting for the terminal port.



The terminal speed is referred to as baud rate in the following messages.

After you select the new terminal speed rate, the system displays the following message:

```
The baud rate will not change until the system is rebooted.
```

```
To have your change take effect without rebooting, perform
this command via the serial port.
```

```
Are you sure you want to change the baud rate? (y/n):
```

- If you respond **y** (yes), the rate is not changed until you reboot.
- If you respond **n** (no), the rate does not change, and the display returns to the previous menu.

**system serialPort
modemSpeed**

Sets the port speed for the modem port to match your external modem baud setting.

✓ 3500
9000
9400

3900
9300

Valid Minimum Abbreviation

sy se m

Important Considerations

- After you use this command, you must establish a connection between your current Console session and the modem port before you dial in. (See "system serialPort configModem" later in this chapter for details.)
- Be sure that the baud setting of the modem port matches that of your external modem.
- The system immediately changes the modem port baud setting.

Options

Prompt	Description	Possible Values	[Default]
Modem speed	Signal speed for the connection	<ul style="list-style-type: none"> ■ 19200 ■ 9600 ■ 4800 ■ 2400 ■ 1200 	9600

**system serialPort
baudRate**

Sets the baud rate of your system serial port.

Valid Minimum Abbreviation

sy se b

Important Considerations

- The default setting for the serial port is 9600. You can change the setting to match the port speed on your terminal or modem. The default setting for the serial port is 9600. You can change the setting to match the port speed on your terminal or modem.
- When you change the baud rate to something other than 9600, the new setting becomes the new default, even after you use the `system nvData reset` option.
- You must adjust the baud rate setting of your terminal or terminal emulator's terminal interface processor (tip) to match your system serial port's speed before you can reestablish communication using the terminal port.
- You can use this command through the terminal serial port or through a Telnet session. However, if you change the terminal speed while you are in a Telnet session, you must reboot the system for the change to take effect.

Options

Prompt	Description	Possible Values	[Default]
New value	Baud rate for the serial port connection	<ul style="list-style-type: none"> ■ 19200 ■ 9600 ■ 4800 ■ 2400 ■ 1200 	9600
Confirmation	Confirmation of baud rate change	<ul style="list-style-type: none"> ■ y (yes) ■ n (no) 	–

Procedure (Local Connection)

- 1 To set the baud rate for the serial port, from the top level of the Administration Console, enter:

```
system serialPort baudRate
```

2 Enter the baud setting for the serial port. The system supports the following baud rates:

- 19200
- 9600
- 4800
- 2400
- 1200

The system response depends on the cable status. If the cable is connected to the terminal port when you set the baud rate for that port, the system displays the following message:

Changing the baud rate may cause a loss of communication since you are currently connected via the serial port.

Are you sure you want to change the baud rate? (y/n):

- If you respond **y** (yes), the serial port's baud rate is changed immediately, and you lose the ability to communicate to any devices connected to it until you adjust the device baud setting to match.
- If you respond **n** (no), the rate does not change, and the display returns to the previous menu.

Procedure (IP Interface)

1 From the top level of the Administration Console, enter:

```
system serialPort baudRate
```

2 Enter the baud setting for the terminal port.

After you select the new baud, the system displays the following message:

The baud rate will not change until the system is rebooted. To have your change take effect without rebooting, perform this command via the serial port.

Are you sure you want to change the baud rate? (y/n):

- If you respond **y** (yes), the rate is not changed until you reboot the system.
- If you respond **n** (no), the rate does not change, and the display returns to the previous menu.

**system serialPort
serialPortMode**

Configures the system serial port to establish either a terminal connection or a modem connection.

3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy se s

Options

Prompt	Description	Possible Values	[Default]
Serial port	Type of serial port configuration that you want	<ul style="list-style-type: none"> ■ console ■ modem 	console

Procedures

To change the serial port configuration from `console` to `modem`, perform the following steps:

- 1 Change the serial port configuration from `console` to `modem`.
- 2 Disconnect the console cable.
- 3 Connect the modem cable.

The system is ready for you to establish a modem connection. See “system serialPort configModem” next for details.

To change the serial port configuration from `modem` to `console`, perform the following steps:

- 1 Change the serial port configuration from `modem` to `console`.
- 2 Disconnect the modem cable.
- 3 Connect the console cable.

The system is ready for you to establish a console connection. (See “system serialPort baudRate” earlier in this chapter.)

**system serialPort
configModem**

Configures the external modem from the Administration Console.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy se c

Important Considerations

- The system transmits characters that you have entered as output on the modem port. The system echoes characters that it receives as input on the modem port to the current Console session. Thus, the Console appears to be directly connected to the external modem.
- You may need to change the baud of the modem to match that of your modem port.

Procedure

- 1 From the top level of the Administration Console, enter:

```
system serialPort configModem
```

You can now enter commands that support the appropriate parameters for your network. All characters that you enter are transmitted to the modem port until you type the escape sequence in step 2.

- 2 When the modem is configured, enter the escape sequence ~] with no intervening characters or spaces.

Entering the escape sequence breaks the connection to the modem serial port and returns you to the previous Administration Console menu.

**system serialPort
enableModem**

Enables the external modem from the Administration Console.

Valid Minimum Abbreviation

sy se e

Important Consideration

- You must configure the external modem before you can enable it. See the configModem command description on the previous page.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

system name Assigns or changes the name of the system. The system name identifies the system to users on other systems in the network.

- ✓ 3500
- 9000
- ✓ 9400

Valid Minimum Abbreviation

sy na

- ✓ 3900
- ✓ 9300

Important Considerations

- Assign an easily recognizable and unique name for each system. For example, name the system according to its physical location, as in PARIS-ENGLAB1.
- Use quotation marks (") around any string that has embedded spaces.
- Use double quotation marks ("") to enter an empty string.
- The new system name appears the next time that you display the system configuration.

Options

Prompt	Description	Possible Values	[Default]
New string	New or changed name for the system	<ul style="list-style-type: none"> ■ A string of up to 64 case-sensitive characters ■ ? (to get information about the naming guidelines) 	-

system time Displays and changes the system's current date and time, timezone, and daylight saving time.

✓ 3500

9000

✓ 9400

Valid Minimum Abbreviation

sy t

✓ 3900

✓ 9300

Important Considerations

- The system's internal clock is set at the factory. You may want to reset the system date and time to match the system's physical location.
- 00 specifies the year 2000 for all 3Com products. See the 3Com Web site for more details.

Options

Field	Description
DateTime	Starting date and time in the following format: yyyy-mm-ddThh:mm:ss
Timezone	User-configured time zone (for example, GMT for Greenwich Mean Time)
dst	<ul style="list-style-type: none"> ■ If you enter y to the prompt, a sub-menu appears that lists the Daylight Savings Time around the world and a user specified option for start and end dates ■ If you enter n, you are returned to the Time menu

system time datetime Sets the system's date and time.

- ✓ 3500
- 9000
- ✓ 9400

- ✓ 3900
- ✓ 9300

Valid Minimum Abbreviation

sy t d

Important Considerations

- The system's internal clock is set at the factory. You may want to reset the system date and time to match the system's physical location.
- *00* specifies the year 2000 for all 3Com products. See the 3Com Web site for more details.

Procedure

- 1 To change the system date or time, enter:

da

The system displays the current date and time and then prompts you to change the time.

- 2 Enter *y* (yes) or *n* (no) at the prompt.

If you respond *n*, the top-level menu appears.

If you respond *y*, the system prompts you for the correct date and time.

- 3 Enter the correct date and time in this format:

ccyy-mm-ddThh:mm:ss

Format	Description
<i>yyyy</i>	century and last two digits of the year (00-99)
<i>first mm</i>	date (1 – 31)
<i>dd</i>	month (1 – 12)
<i>T</i>	Time designator
<i>hh</i>	hour (1 – 12)
<i>second mm</i>	minute (00 – 59)
<i>ss</i>	second (00 – 59)

system time timezone Configures the local time zone and daylight savings time values.

✓ 3500
9000
9400

Valid Minimum Abbreviation

sy t timez

Important Considerations

- Displays the current time zone table, with time zone indexes and the time zone identifiers before it prompts you to select a time zone index.
- The local time zone value adjusts the server reply universal time to local time properly.
- The default time zone is Greenwich Mean Time (GMT).

Options

Prompt	Description	Possible Values	[Default]
Time zone index	Index number of the time zone that you want to configure	<ul style="list-style-type: none"> ■ 1 – 28* ■ ? (lists the default selection and selectable values) 	1 (GMT)

* Index number 28 prompts for an offset from the GMT in the following time format: ±hh:mm.

System Time Timezone Example (3500)

Select menu option (system/sntp): **timez**

Index	Time Zone
1	[GMT+0:00] GMT/WET/UT
2	[GMT-1:00] WAT
3	[GMT-2:00] AT
4	[GMT-3:00] Brasilia/Buenos Ar/GeorgeTown
5	[GMT-4:00] AST
6	[GMT-5:00] EST
7	[GMT-6:00] CST
8	[GMT-7:00] MST
9	[GMT-8:00] PST
10	[GMT-9:00] YST
11	[GMT-10:00] AHST/CAT/HST
12	[GMT-11:00] NT
13	[GMT-12:00] IDLW
14	[GMT+1:00] CET/FWT/MET/MEWT/SWT
15	[GMT+2:00] EET
16	[GMT+3:00] BT
17	[GMT+4:00] ZP4
18	[GMT+5:00] ZP5
19	[GMT+5:30] Bombay/Calcutta/Madras/New Dehli/Colombo
20	[GMT+6:00] ZP6
21	[GMT+7:00] WAST
22	[GMT+8:00] CCT
23	[GMT+9:00] JST
24	[GMT+9:30] Darwin/Adelaide
25	[GMT+10:00] EAST/GST
26	[GMT+11:00] Magadan/Solomon Is/N. Caledonia
27	[GMT+12:00] IDLE/NZST/NZT
28	Input an offset from GMT

Select timezone index {1-28|?} [1]:

system time dst Sets daylight savings time.

✓ 3500

9000

9400

3900

9300

Valid Minimum Abbreviation

sy t ds

Important Consideration

- Displays the daylight savings time periods for various parts of the world.

Procedure

- 1 To set daylight savings time, enter:

ds

The system displays the following prompt:

Do you want to set the Daylight Saving Time?(n,y) [n]:

- 2 Enter **y** (yes) or **n** (no) at the prompt.

If you respond **n**, the Time menu appears.

If you respond **y**, the system displays the following:

1 First Sunday in April to last Sunday in October (North America)

2 Last Sunday in March to last Sunday in October (Europe, parts of Asia)

3 Last Sunday in October to last Sunday in March (Parts of Australia)

4 Last Sunday in October to the Sunday on/after March 15th (New Zealand, parts of Australia)

5 Enter a start and an end dates for the current year

Select daylight saving time option {1-5|?} [1]:

The format for option 5 is: ccyy-mm-ssThh:mm:ss

Example: 1999-05-20T12:30:34

- 3 Enter a daylight saving time option.

system nvData save Stores nonvolatile (NV) data on a server. The CoreBuilder 3500 uses the Trivial File Transfer Protocol (TFTP) or File Transfer protocol (FTP) to transfer the files to the host, depending on the setting for the `system fileTransfer` option. The SuperStack II Switch 3900, Switch 9300, and the CoreBuilder 9400 use TFTP to transfer files.

✓ 3500
9000
✓ 9400

✓ 3900
✓ 9300

Valid Minimum Abbreviation

`sy nv s`

Important Considerations (TFTP)

- To store NV data, you must first create two files on the TFTP server *before* you send the data:
 - **Control file** — Use any filename that is meaningful to you.
Example: `ctrlfile`
 - **NV data file** — Use the control filename plus the `.nvd` extension.
Example: `ctrlfile.nvd`
- When the system saves NV data, it writes it to a disk file on a host computer (that is, a server) using TFTP or FTP. You can then retrieve the data from the disk file with the `restore` option.
- Some TFTP implementations require that you store the files in the same directory in which the TFTP daemon (server) is running on the remote host.
- Some TFTP implementations require a full path, while other implementations allow you to specify only the file name, and the system saves the file to the default TFTP directory. Consult your network administrator or TFTP documentation for details about your host system's TFTP implementation.
- Because TFTP provides no user authentication, give *loose* permissions to the control file and the NV data file on the remote host (that is, make the files publicly readable and writable). TFTP servers do not grant requests for file access.

Important Consideration (FTP and TFTP)

- During the save procedure, the current configuration can be altered. To detect this event, the software runs checksum on the NVRAM before and after the save.

If the checksum is different, you are notified and prompted to save the configuration again. In abnormal situations, this reiteration can continue indefinitely, so you are given the option to terminate the save. You are also prompted for a retry request after a network (TFTP) I/O failure.

Options

Prompt	Description	Possible Values	[Default]
Host IP address	IP address of the host on which you want to store the data file	Any valid IP address	Previous IP address used
NV control file	Full path of the file where you want to store the NV data	–	–
File label (optional)	Meaningful description of the file	32-character text string	–

Procedure

- 1 To save NV data, from the top level of the Administration Console, enter:

```
system nvData save
```

The system prompts you for information about saving the data. To accept the value in brackets, press Return. Any entry for IP address, filename, and user name becomes the new default.

- 2 Enter the IP address of the TFTP or FTP server.
- 3 If you are using TFTP and your implementation requires a full path, enter the full pathname of the control file. (Some implementations allow you to specify only the file name, and the server uses the default TFTP directory.)



The system prompt says NV Control file, so enter the name of the control file without the NVD extension.

- 4 Optionally, enter a label for the file.

Example:

```
Host IP Address [158.101.100.1]: 158.101.112.34
NV Control file (full pathname): nvdata
Enter an optional file label: Labdata
```


If the information is incorrect or if a connection cannot be made with the specified host, the system displays a message similar to this one:

```
Login incorrect.
```

```
Error: Transfer Timed Out
```

```
Error - I/O error while writing nonvolatile data
```

If a session is successfully opened, a system message notifies you of the success or failure of your save, as in the following examples:

Success System NV data successfully stored on host 158.101.112.34.

Failure Saving system...transfer timed out.

```
Error - I/O error while writing nonvolatile data. Do you wish  
to retry the save using the same parameters? (n,y) [y].
```

5 To save the data as proposed, enter **y**

If you enter **n**, the NV data is not saved and the previous menu appears.

The text of the failure message depends on the problem that the system encountered while it saved the NV data.

At the end of a successful save, the system display returns to the previous menu.

system nvData restore Restores the NV data that was previously saved to a file.

Valid Minimum Abbreviation

`sy nv r`

Important Considerations

- Before you attempt to restore the data to a system that has a different system ID, be aware that the following types of NV data may cause problems when they are restored:
 - Management IP addresses (defined in IP interface configurations) are saved as NV data and restored. To avoid duplicate IP address problems, you may need to change the IP address of defined interfaces before you connect the restored system to the network.
 - Statically configured Ethernet addresses are saved as NV data. Verify that you have no duplicate addresses when you restore the NV data.

Options

Prompt	Description	Possible Values	[Default]
Host IP address	IP address of the host on which the NV data file resides	Any valid IP address	Previous IP address that was used
NV control file	Location of the NV data file	<ul style="list-style-type: none"> ■ file name ■ full path 	Previous nv control file that was used
Do you wish to continue?	Confirmation of the operation. (You may not want to reboot because resetting nonvolatile data may leave the system in an inconsistent state, so the system reboots after each reset.)	<ul style="list-style-type: none"> ■ n (no) ■ y (yes) 	y

Procedure

- 1 To restore the NV data, from the top level of the Administration Console, enter:

```
system nvData restore
```

The system prompts you to enter information for restoring the NV data that was saved to a file.

✓ 3500
9000
✓ 9400

✓ 3900
✓ 9300

Press Return at any prompt to accept the current or default value in brackets.

- 2 Enter the IP address of the host on which the NV data file resides.
- 3 If you are using TFTP and your implementation requires a full path name, enter the full NV data file path and filename. Some implementations allow you to specify only the file name; the system uses the default TFTP directory.

When you restore system NV data, the software compares the system IDs, module types, and module revisions (if applicable) between the saved configuration and the system on which you are restoring the image.

- If the system finds an exact match between system IDs, module types, and module revisions, the system displays a reminder message and prompts you for verification before performing the restoration (see step 4).
- If there is *not* an exact match between system IDs, module types, and module revisions, the system displays a warning message and prompts you as follows:

```
WARNING - mismatch between saved system IDs (27DA00) and
current system (28E100)
Do you want to disregard this and continue the restore (n,y)
[y]:
```

If you want to continue the restoration, enter **y** (yes). If you do not want to continue, enter **n** (no).

- 4 At the next prompt, to have the system NV data restored as requested, enter **y** (yes). To terminate the restoration, enter **n** (no).

For example:

```
Restoring nonvolatile data may leave the system
in an inconsistent state and therefore a reboot is necessary
after each restore.
Do you wish to continue? (y/n): y
```

- If you enter **y**, the system displays the following messages:

```
Restoring nonvolatile data...done
Nonvolatile data successfully restored
```

The system automatically reboots itself after it restores the NV data.

- If you enter **n**, the restoration ends and the previous menu appears.

**system nvData
examine**

Displays the header information of the NV data file.

Valid Minimum Abbreviation

sy nv e

Important Considerations

- Some TFTP implementations allow you to specify only the file name, and the system uses the default TFTP directory.
- If a session is successfully opened, the system displays the header information that corresponds to the file name that you entered.

Options

Prompt	Description	Possible Values	[Default]
Host IP address	IP address of the host on which the NV data file resides	Any valid IP address	Previous IP address used
NV control file	Location of the NV data file	<ul style="list-style-type: none"> ■ file name ■ full path 	System NV data file

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

system nvData reset

Resets the system values to the factory defaults. You can then reconfigure the system from its original settings.

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

`sy nv rese`

- ✓ 3900
- ✓ 9300

Important Considerations

- You are not permitted to perform an NV data reset from a Telnet session. An NV data Reset over Telnet clears all of your configurable information, including the IP interface of the box, and prevents you from managing the system without a direct console connection.
- If you enter `n` (no) when you are prompted to confirm the reset, the system displays the previous menu.



CAUTION: As a precaution, consider saving the existing NV data to a file before you reset all values to the factory defaults. Resetting NV data means that NV memory is set back to the factory defaults (except for the serial port baud rate, modem baud rate, and system boot parameters). Before you proceed, be sure that you want to reset your NV data.

Options

Prompt	Description	Possible Values	[Default]
Do you wish to continue?	Confirmation of the reset operation. (You may not want to reboot because resetting nonvolatile data may leave the system in an inconsistent state, so the system reboots after each reset.)	<ul style="list-style-type: none"> ■ n (no) ■ y (yes) 	y

system clearDiagBlock Prevents diagnostic information about failed modules from appearing in system display screens.

✓ 3500

9000

✓ 9400

Valid Minimum Abbreviation

sy cl

Important Consideration

✓ 3900

✓ 9300

- After you enter this command, the system immediately removes diagnostic information about failed modules from the SNMP MIB *swSysDiagnosticsGroup*.

Options

Prompt	Description	Possible Values	[Default]
Clear the diagnostic block	Confirmation of your decision to clear the diagnostic information	<ul style="list-style-type: none"> ■ n (no) ■ y (yes) 	y

system diagErrLog

Displays hardware diagnostic errors that have been saved in the flash memory. When the system is initializing, if the diagnostic software detects errors, and if the system completes initializing, the detected errors are written to flash memory and stored in a dynamic error log.

✓ 3500

9000

✓ 9400

Valid Minimum Abbreviation

mo dia

✓ 3900

✓ 9300

Important Consideration

- The error messages are saved to flash memory until you power down the system or clear the error log with the `system clearDiagBlock` command.

system sntp display Displays Simple Network Time Protocol (SNTP) information.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy snt di

Important Considerations

- SNTP handles the synchronization of system clocks in the network to the national time standards via distributed time servers.
- Your system provides the SNTP client.
- The display has two types of information:
 - **Configuration information** — User configurable parameters appear.
 - **Servers information** — Information returned by the server appears if you have defined SNTP servers. Otherwise, the `No Servers are defined` message appears.

Fields in the System SNTP Display

Field	Description
Configuration Information	
State	SNTP state. It is either <code>enabled</code> or <code>disabled</code> .
PollInterval	Interval for the client to send requests to a specific server.
Tolerance	Threshold for updating the local system time.
Servers Information	
Server	Server IP address.
Mode	Client's SNTP operating mode. This field always displays <code>Unicast</code> .
Version	Version number of the responding server (for example, 4 represents version 4, which is suitable for IPv4, IPv6, and OSI). The client version number is 3.
Stratum	8-bit integer that indicates the stratum level of the local clock (for example, a stratum value of 3 indicates a secondary reference via SNTP).
Poll	Maximum interval between successive messages.
Delay	Roundtrip propagation delay from the server's reply.
LastPktRcv	Date and time stamp of the last packet that was received from the specific server.

system sntp define Specifies up to three Simple Network Time Protocol (SNTP) server IP addresses.

✓ 3500
9000
✓ 9400

Valid Minimum Abbreviation

sy snt de

Important Considerations

✓ 3900
✓ 9300

- You can define up to three SNTP servers for backup purposes.
- Your system provides the SNTP client.
- The system indicates that it is adding the IP address to the SNTP database. The server is assigned an index number.

Options

Prompt	Description	Possible Values	[Default]
Server's IP address	IP address of a server to add to the SNTP database	Valid IP address (except 0.0.0.0)	–

system sntp modify Replaces an existing Simple Network Time Protocol (SNTP) server IP address.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy snt m

Options

Prompt	Description	Possible Values	[Default]
Index	Index number of the server that you want to modify	Available Server index number	–
Server address	IP address of each configured server	Valid IP address	–

system sntp remove Removes a Simple Network Time Protocol (SNTP) server IP address from the SNTP server list.

✓ 3500

9000

✓ 9400

Valid Minimum Abbreviation

sy snt r

✓ 3900

✓ 9300

Options

Prompt	Description	Possible Values	[Default]
Index	Index number of the server that you want to remove	Available Server index number	–
Server address	IP address of each configured server	Valid IP address	–

system sntp state Enables or disable the Simple Network Time Protocol (SNTP) state for the system.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy sntp s

Options

Prompt	Description	Possible Values	[Default]
SNTP state	Whether you want to implement SNTP on the system	<ul style="list-style-type: none"> ■ disabled ■ enabled 	disabled

system sntp pollInterval Sets a poll interval value. This value determines how often the Simple Network Time Protocol (SNTP) client sends a request to the SNTP server.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy snt p

Important Consideration

- The default pollInterval value is once an hour (3600 seconds). The value 86400 (the pollInterval limit) is the number of seconds in a day.

Options

Prompt	Description	Possible Values	[Default]
Request poll interval	In seconds, the poll interval	64 – 86400 seconds	3600

system sntp tolerance Sets a tolerance threshold that is used to update the local system time.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sy snt to

Important Consideration

- If the difference between the server time and the local time exceeds the specified tolerance threshold, the client drops the server time and maintains the current local system time unchanged.

Options

Prompt	Description	Possible Values	[Default]
Time tolerance	Time threshold value, in seconds, that is used to update the local system time	0 – 3600 seconds	900

system reboot Reboots the system.

✓ 3500
9000
✓ 9400

Valid Minimum Abbreviation

sy r

Important Considerations

✓ 3900
✓ 9300

- This command disconnects the present Administration Console session and starts another session whether your system is connected to the Administration Console by an external modem or through an rlogin or Telnet session.
- To view diagnostic information during reboots, connect your system through the Console serial port.

Options

Prompt	Description	Possible Values	[Default]
Reboot the system?	Confirmation that you want to reboot	<ul style="list-style-type: none"> ■ n (no) ■ y (yes) 	–

script Executes a command file that you have written to expedite and automate Administration Console tasks.

✓ 3500

9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

`sc`

Important Considerations

- Any command that you can enter in the Administration Console can be part of a script. You can even script your entire system setup so that you can repeat the exact setup on other systems.
- You create scripts in an ASCII-based line editor, such as *EMACS* or *vi*. Scripts must be stored on the TFTP server. For the CoreBuilder 3500, you can select TFTP or FTP as the file transfer method. See “system fileTransfer” earlier in this chapter for more details.
- Some TFTP implementations require that you store the script file in the same directory in which the TFTP daemon (server) is running on the remote host.
- Because TFTP provides no user authentication, make the file permissions *loose* so that the public can read and write to the file. TFTP servers do not grant requests for file access.

Procedure

- 1 From the top level of the Administration Console, enter:

```
script
```

The system prompts you for information about where you have stored the script that you want to run: host IP address and file path

Press Return at any prompt to accept the current or default value in brackets.

- 2 Enter the path name to the script file. If you are using TFTP, see “system snapshot save” earlier in this chapter for more details about pathname requirements.

The task that you scripted runs in the Administration Console.

Example Script (3500)

This example scripts these tasks to initially configure your system:

- Changes the modem port baud
- Sets the system name
- Assigns an IP address for management
- Verifies the IP connection by pinging the system
- Enables Spanning Tree
- Sets up SNMP trap reporting

```
# This script performs some start-up configurations.
#
# Set the modem serial port baud.
#
system serialPort modemSpeed
4800          # modem serial port baud
#
# Set the system name
#
system name
Eng_CoreBuilder_4
#
# Assign an IP address to the system.
#
ip interface define
158.101.112.99 # IP address for the system
255.255.0.0   # subnet mask
1            # VLAN interface index

ip interface summary all
#
# Validate access to management workstation
#
ip ping
158.101.112.26 # management workstation address
#
# Enable the Spanning Tree Protocol
#
bridge stpState enabled
#
# Configure my node as an SNMP trap destination
#
snmp trap add
158.101.112.26 # management workstation address
all           # turn on all traps
q            # no more trap destinations
#
snmp trap display
#
```

✓ 3500
9000
✓ 9400

logout Terminates a Telnet session or returns control to the password prompt in a serial port session.

Valid Minimum Abbreviation

logo

✓ 3900
✓ 9300

Important Consideration

- Press Escape to return to the top level before you log out.

4

MODULE ENVIRONMENT

This chapter describes how to use `module` commands for modules that are installed in the CoreBuilder® 9000 7-slot, 8-slot, and 16-slot chassis to:

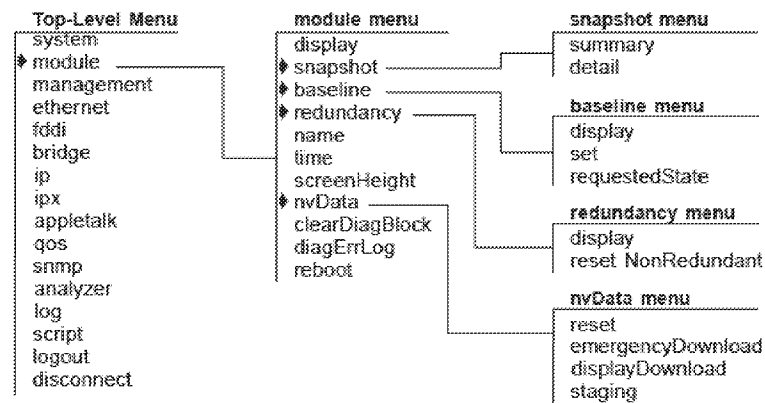
- Display the module configuration and status
- Administer a statistics baseline and module redundancy
- Set the module name and the console screen height
- View the date and time
- Manage nonvolatile data (nvData)
- Clear the module diagnostic block
- Reboot a module



For more information about administering your module parameters, see the CoreBuilder 9000 Implementation Guide.

Menu Structure

The commands that you can use depend on the system that you have, your level of access, and the types of modules and other hardware options that are configured for your system. The following diagram shows the complete list of commands for all systems. See the checklist at the beginning of each command description in this chapter for whether your system supports the command.



The redundancy option appears if you have a CoreBuilder 9000 8-slot and 16-slot chassis and if you have one or two GEN Switch Fabric Modules installed.

In addition to the `module` options, you must also use the `disconnect` option from the top-level menu to return to the Enterprise Management Engine (EME).

module display Generates software and hardware revision numbers, module status information, and warning messages for certain module conditions.

3500
 ✓ 9000
 9400

3900
 9300

Valid Minimum Abbreviation

mo d

Important Considerations

- The module display provides the configuration information for the module to which you are currently connected. To display configuration information for another module, disconnect from the current module through the Enterprise Management Engine (EME) and then connect to the module that you want to display.
- After you have logged in to the EME, you can access the module that you want to manage.
- Diagnostic messages appear in the display only if a module fails any of the tests at start-up.

Fields in the Module Display

Field	Description
24 port Gigabit Switching Fabric	32-character alphanumeric name that uniquely identifies this module
3C number	Each module's 3Com 3C product identification number
Built	Date and time when this software version was built
Diagnostics	Whether a module has passed or failed diagnostics. Additional diagnostic messages describe a failure.
Memory size (AP, FP, Flash, Buffer)	Memory capacities of the processors
Module ID	ID number that the system assigns to that module
Rev	Unique number assigned to the hardware build by 3Com
Serial	Each module's unique serial number
Slot	Location of the module in the chassis (slot.subslot)
System name	Name of the system
System up time	Time that this module has been up and running
Time in service	Total operational time since the module was manufactured
Version	Software release number

**module snapshot
summary**

Captures an image of all the module's display screens. The values in each screen reflect the current values of all fields and counters at the time that you use the snapshot feature.

3500

✓ 9000

9400

Valid Minimum Abbreviation`mo sn su`

3900

9300

Important Consideration

- If a feature or protocol has only one display option (`display`), the module includes the same image in the snapshot of both the summary and the detail display images.

**module snapshot
detail**

Captures an image of all module detail display screens. The display screens contain the current values of all fields and counters at the time that you use the snapshot feature.

3500
✓ 9000
9400

Valid Minimum Abbreviation

mo sn de

Important Consideration

- If a feature or protocol has only one display option (`display`), the module includes that image with both the summary and detail display images.

**module baseline
display**

Displays when the current baseline was last set.

Valid Minimum Abbreviation

mo ba dis

Important Considerations

- Use this command to determine if you need a newer baseline for viewing statistics.
- The display indicates if you have not set the baseline on a module.

3500

✓ 9000

9400

3900

9300

module baseline set Resets the baseline counters to zero and time-stamps the baseline.

3500

✓ 9000

9400

3900

9300

Valid Minimum Abbreviation

mo ba set

Important Considerations

- Baselining is automatically enabled when a baseline is set.
- The module maintains the accumulated totals since power-on.
- After you disconnect from a module on which you set a baseline, the baseline is disabled. You must reconnect to that module and use the `module baseline requestedState` option to reenables the baseline.

**module baseline
requestedState**

Enables or disables a baseline.

Valid Minimum Abbreviation

mo ba req

Important Considerations

- When you reenable a baseline, the counters return to the values that have accumulated since the most recent baseline that you set.
- Disabling a baseline returns the counters to the total accumulated values since the last power on.
- After you disconnect from a module on which you set a baseline, the baseline is disabled. You must reconnect to that module and use the `module baseline requestedState` option to reenable the baseline.

Options

Prompt	Description	Possible Values	[Default]
Baseline	Whether you want to enable or disable the baseline	<ul style="list-style-type: none"> ■ enabled ■ disabled 	disabled

3500
✓ 9000
9400

3900
9300

module redundancy Establishes a fault-tolerant environment for your CoreBuilder 9000 system.

3500

✓ 9000

9400

3900

9300

Valid Minimum Abbreviation

mo red

Important Considerations

- You must be using a CoreBuilder 9000 8-slot or 16-slot chassis.
- The Redundancy option appears on the module menu if you have one or two switch fabric modules installed. If you only have one switch fabric module installed in the chassis, the status of the second switch fabric slot is `Not Responding`.

Options

Prompt	Description	Possible Values	[Default]
Display	Module redundancy configuration and status	–	–
reset nonRedundant	Whether the module's non-redundant indicator resets	–	–

module name Assigns or changes an easily recognizable and unique module name to help you manage it.

3500

✓ 9000

9400

3900

9300

Valid Minimum Abbreviation

mo nam

Important Considerations

- Assign an easily recognizable and unique name for each module. For example, name the module according to its physical location, such as CB9000-ENGLAB1.
- Use quotation marks (") around any string with embedded spaces.
- The new module name appears the next time that you display the configuration.

Options

Prompt	Description	Possible Values	[Default]
New name	New or changed name for the module	<ul style="list-style-type: none"> ■ A string of up to 32 case-sensitive characters ■ ? (for information about the naming guidelines) 	Current system and module name

module time Displays the module's current date and time.

3500
 ✓ 9000
 9400

Valid Minimum Abbreviation

mo ti

Important Considerations

- You cannot change the system time from the module. You can only change the date and time from the Enterprise Management Engine (EME).
- The CoreBuilder 9000 module's internal clock is initialized when the module is shipped from the factory. You may want to reset the EME date and time to match the system's physical location.

Module Time Example

```
CB9000@slot10.1 [12-E/FEN-TX-L3] (module): time
The current module time is 05/20/98 04:37:57 PM.
```

module screenHeight

Changes the Administration Console's screen height to increase or decrease the space available for displaying information.

3500
 ✓ 9000
 9400

Valid Minimum Abbreviation

no scr

3900
 9300

Important Considerations

- The setting controls the way that the module displays statistical summaries and other information that results from your use of the menus, not the way that the module displays the menus themselves.
- Each time that the screen output reaches the designated screen height, the module prompts you to press a key to display more information. Set the screen height to infinite (o) if you do not want the modules to display this prompt. At o, however, the screen output can scroll beyond the screen, depending on your screen size.
- Most terminal screens are 24 lines.

Options

Prompt	Description	Possible Values	[Default]
New screen height	New screen height in lines	<ul style="list-style-type: none"> ■ 1 – 200 ■ 0 (for infinite height) 	24
Set this value as the default?	Default screen height for future Administration Console sessions	<ul style="list-style-type: none"> ■ y (yes) ■ n (no) 	y

module nvData reset Resets the module's nonvolatile data (NV) values to the factory defaults.

3500

✓ 9000

9400

3900

9300

Valid Minimum Abbreviation

mo nv res

Important Considerations

- At times you may want to reset the values to the factory defaults so that you can reconfigure the module from its original settings.
- Resetting the NV data means that all NV memory is set back to the factory defaults. Before you proceed, be sure that you want to reset your NV data. Rebooting a module returns you to the Enterprise Management Engine (EME) prompt, so that you must reconnect to the module.

Prompts

Prompt	Description	Possible Values	[Default]
Do you wish to continue?	Confirmation prompt. Resetting nonvolatile data may leave the module in an inconsistent state; a reboot is necessary after each reset.	<ul style="list-style-type: none"> ■ n (no) ■ y (yes) 	y

module nvData emergencyDownload

Performs an emergency download.

3500
✓ 9000
9400

Valid Minimum Abbreviation

mo nv sta

Important Consideration

- If you hot swap a module and the staging flag is set to `oEE`, the new module uses the module default settings for the new module.

3900
9300

Options

Prompt	Description	Possible Values	[Default]
Staging setting	Whether you want to enable or disable the NV staging flag	<ul style="list-style-type: none"> ■ off ■ on 	off

**module nvData
displayDownload**

Displays emergency download information for your module.

Valid Minimum Abbreviation

mo nv dis

Important Consideration

■ The download display shows the following information:

- File Type
- File Name
- Server IP

3500

✓ 9000

9400

3900

9300

**module nvData
staging**

Enables either default module settings or retention of nonvolatile data settings when you hot swap a module.

3500

✓ 9000

9400

3900

9300

Valid Minimum Abbreviation

```
mo nv sta
```

Important Considerations

- If you hot swap a module and the staging flag is set to `on`, the new module adopts the nonvolatile data settings from the old module.
- If you hot swap a module and the staging flag is set to `off`, the new module uses the module default settings for the new module.

Options

Prompt	Description	Possible Values	[Default]
Staging setting	Whether you want to enable or disable the NV staging flag	<ul style="list-style-type: none"> ■ off ■ on 	off

module Prevents diagnostic information about failed modules from accumulating
clearDiagBlock in module display screens.

3500

✓ 9000

9400

3900

9300

Valid Minimum Abbreviation

mo cle

Important Considerations

- The module immediately removes diagnostic information about failed modules from the SNMP MIB *swSysDiagnosticsGroup*.
- If you enter **y** (yes), the module immediately removes the diagnostic information about failed modules from the SNMP MIB *swSysDiagnosticsGroup*.
- If you enter **n** (no), the module displays the previous menu.

module diagErrLog

Displays hardware diagnostic errors that have been saved in the flash memory. When the system is initializing, if the diagnostic software detects errors, and if the system completes initializing, the detected errors are written to flash memory and stored in a dynamic error log.

3500

✓ 9000

9400

Valid Minimum Abbreviation`mo dia`

3900

9300

Important Consideration

- The error messages are saved to flash memory until you power down the system or clear the error log with the `system clearDiagBlock` command.

module reboot Reboots the specified module.

3500

✓ 9000

9400

3900

9300

Valid Minimum Abbreviation

mo reboot

Important Considerations

- Rebooting a module returns you to the Enterprise Management Engine (EME) prompt, so that you must reconnect to the module.
- If you enter **y**, the module reboots.
- If you enter **n**, the previous menu appears on the screen.

disconnect Disconnects you from the Administration Console and returns you to the Enterprise Management Engine (EME) module.

3500

✓ 9000

9400

Valid Minimum Abbreviation

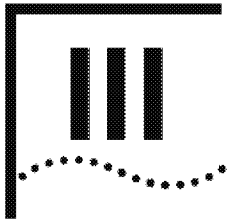
`disc`

3900

9300

Important Consideration

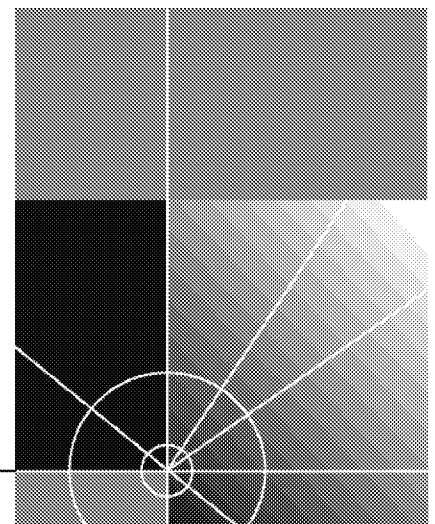
- Disconnecting from the Administration Console does not disconnect you from a Telnet session.



ESTABLISHING MANAGEMENT ACCESS

Chapter 5 **Out-of-Band Management**

Chapter 6 **Simple Network Management Protocol (SNMP)**



5

OUT-OF-BAND MANAGEMENT

The Internet Protocol (IP) is a standard networking protocol that is used for communications among various networking devices. To gain access to the system using the Transmission Control Protocol/Internet Protocol (TCP/IP) or to manage the system using the Simple Network Management Protocol (SNMP), you must set up an IP interface to manage your system, either in-band (with your regular network traffic) or out-of-band (with a dedicated network).

- **In-Band Management** — Set up an IP routing interface and at least one virtual local area network (VLAN). See Chapter 14 for information about how to define a VLAN.
- **Out-of-Band Management** — Assign an IP address and subnet mask for the out-of-band Ethernet port on your system through the management menu. This chapter focuses on out-of-band management. The out-of-band Ethernet port is the 10BASE-T port on the system processor module. It is not associated with a port number. (See Chapter 16 for background information about IP addresses and subnet masks.)

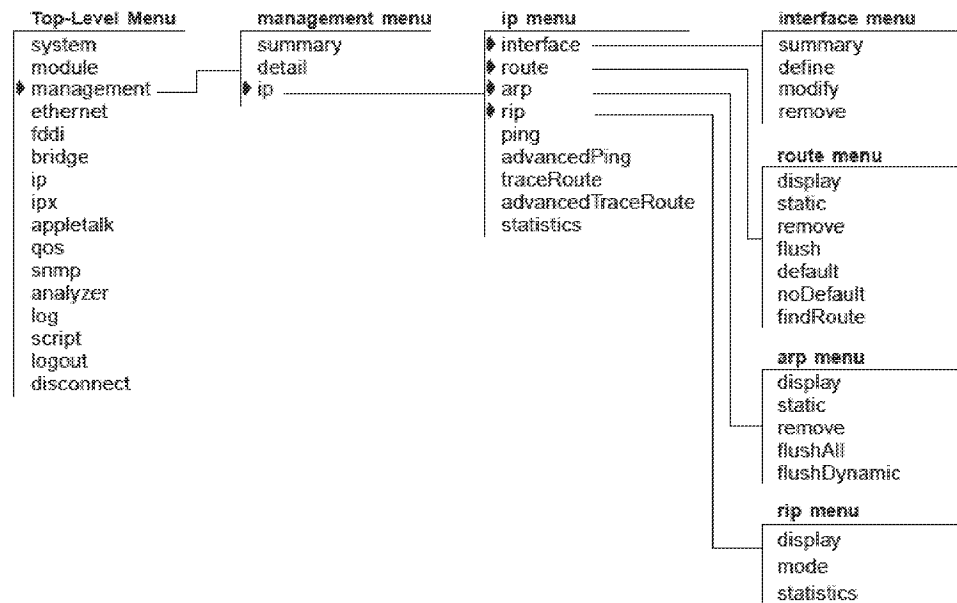
This chapter provides guidelines and other key information about how to set up an out-of-band management interface for your system.



The CoreBuilder® 9000 and SuperStack® II Switch 3900 use in-band management only. For more information about management interfaces, see the Implementation Guide for your system.

Menu Structure

The commands that you can use depend on the system that you have, your level of access, and the types of modules and other hardware options that are configured for your system. The following diagram shows the complete list of commands for all systems. See the checklist at the beginning of each command description in this chapter for whether your system supports the command.



management summary Displays Ethernet summary information about the out-of-band system management port.

✓ 3500

9000

✓ 9400

3900

✓ 9300

Valid Minimum Abbreviation

m sum

Important Considerations

- The management summary and management detail displays contain the same fields as the Ethernet summary and Ethernet detail displays.
- Fields that do not apply to the management port contain n/a in the management summary and management detail displays.

Fields in the Management Summary Display

Field	Description
actualFlowControl	Actual flow control setting (for Gigabit Ethernet ports). When autonegotiation is completed, the value is the autonegotiated setting. When autonegotiation is disabled, the value is the user-selected flow control value.
actualPortMode	Actual operating port mode. When autonegotiation is completed, the value shown is the autonegotiated setting. When autonegotiation is disabled, the value is the user-selected port mode.
autoNegMode	Autonegotiation mode configured for port. Possible values are <code>enabled</code> or <code>disabled</code> .
autoNegState	Current negotiation state. Possible values are <code>disabled</code> , <code>configuring</code> , <code>completed</code> , and <code>failed</code> .
linkStatus	Boolean value indicating the current state of the physical link status for this port (either <code>enabled</code> or <code>disabled</code>)
macAddress	MAC address of this port
noRxBuffers	Number of frames that were discarded because no buffer space was available
portLabel	User-defined label name. The maximum length of the string is 32 characters, including the null terminator.
portState	Current software operational state of this port. Possible values are <code>on-line</code> and <code>off-line</code> .
portType	Specific description of this port's type. Value for port type: <code>10/100BASE-TX (RJ-45)</code>
reqFlowControl	If autonegotiation is disabled, a configurable parameter that sets the flow control option on the ports. If autonegotiation is enabled, flow control values are ignored.

Field	Description
reqPortMode	If autonegotiation is disabled, a configurable parameter that sets the port mode on Ethernet ports that have port mode options. If autonegotiation is enabled, port mode values are ignored.
rxBytes	Number of bytes received by this port, including framing characters
rxErrs	Sum of all receive errors that are associated with this port (summary report only)
rxFrames	Number of frames that were copied into receive buffers by this port
txBytes	Number of bytes that were transmitted by this port, including framing characters
txErrs	Sum of all transmit errors that are associated with this port (summary report only)
txFrames	Number of frames that were transmitted by this port
txQOverflows	Number of frames that were lost because transmit queue was full

management detail Displays Ethernet detailed information about the out-of-band system management port.

✓ 3500

9000

✓ 9400

3900

✓ 9300

Valid Minimum Abbreviation

m det

Important Considerations

- The `management summary` and `management detail` displays contain the same fields as the `Ethernet summary` and `Ethernet detail` displays.
- Fields that do not apply to the management port contain n/a in the `management summary` and `management detail` displays.

Fields in the Management Detail Display

Field	Description
<code>actualFlowControl</code>	Actual flow control setting for the port. When autonegotiation is completed, the value is the autonegotiated setting. When autonegotiation is disabled, the value is the user-selected flow control value.
<code>actualPortMode</code>	Actual operating port mode. When autonegotiation is completed, the value shown is the autonegotiated setting. When autonegotiation is disabled, the value is the user-selected port mode.
<code>alignmentErrs</code>	Number of frames received by this port that are not an integral number of octets in length and do not pass the FCS check
<code>autoNegMode</code>	Autonegotiation mode configured for port. Possible values are <code>enabled</code> or <code>disabled</code> .
<code>autoNegState</code>	Current negotiation state. Possible values are <code>disabled</code> , <code>configuring</code> , <code>completed</code> , and <code>failed</code> .
<code>carrierSenseErr</code>	Number of frames discarded because the carrier sense condition was lost while attempting to transmit a frame from this port
<code>collisions</code>	Number of collisions detected on this port
<code>excessCollision</code>	Number of frames that could not be transmitted on this port because the maximum allowed number of collisions was exceeded
<code>excessDeferrals</code>	Number of frames that could not be transmitted on this port because the maximum allowed deferral time was exceeded
<code>fcsErrs</code>	Number of frames received by this port that are an integral number of octets in length but do not pass the FCS check

Field	Description
lateCollisions	Number of times that a collision was detected on this port later than 512 bit-times into the transmission of a frame
lengthErrs	Number of frames received by this port that are longer than 1518 bytes or shorter than 64 bytes
linkStatus	Boolean value indicating the current state of the physical link status for this port (either <code>enabled</code> or <code>disabled</code>)
macAddress	MAC address of this port
multiCollisions	Number of times that multiple collisions were detected on this port.
noRxBuffers	Number of frames that were discarded because no buffer space was available
portLabel	User-defined label name. The maximum length of the string is 32 characters, including the null terminator.
portState	Current software operational state of this port. Possible values are <code>on-line</code> and <code>off-line</code> .
portType	Specific description of this port's type. Values for each port type: <code>10/100BASE-TX (RJ-45)</code> , <code>100BASE-FX (SC)</code> , <code>1000BASE-SX (SC)</code> , <code>1000BASE-LX (SC)</code> .
reqFlowControl	If autonegotiation is disabled, a configurable parameter that sets the flow control option on the port. If autonegotiation is enabled, flow control values are ignored.
reqPortMode	If autonegotiation is disabled, a configurable parameter that sets the port mode on Ethernet ports that have port mode options. If autonegotiation is enabled, port mode values are ignored.
requestedState	Configurable parameter that enables or disables this port. The default is <code>enabled</code> .
rxByteRate	Average number of bytes received per second by this port during the most recent sampling period
rxBytes	Number of bytes received by this port, including framing characters
rxDiscards	Number of received frames that were discarded because there was no higher layer to receive them or because the port was disabled
rxErrs	Sum of all receive errors that are associated with this port (summary report only)
rxFrameRate	Average number of frames that were received per second by this port during the most recent sampling period. Sampling periods are 1 second long and not configurable.
rxFrames	Number of frames that were copied into receive buffers by this port

Field	Description
rxInternalErrs	Number of frames that were discarded because of an internal error during reception
rxMulticasts	Number of multicast frames that were delivered to a higher-level protocol or application by this port
rxPeakByteRate	Peak value of ethernetPortByteReceiveRate for this port since the station was last initialized
rxPeakFrameRate	Peak value of ethernetPortFrameReceiveRate for this port since the station was last initialized
rxUnicasts	Number of unicast frames that were delivered by this port to a higher-level protocol or application
txByteRate	Average number of bytes transmitted per second by the port during the most recent sampling period
txBytes	Number of bytes that were transmitted by this port, including framing characters
txDiscards	Number of transmitted frames that were discarded because the port was disabled
txErrs	Sum of all transmit errors that are associated with this port (summary report only)
txFrameRate	Average number of frames transmitted per second by this port during the most recent sampling period. Sampling periods are 1 second long (not configurable).
txFrames	Number of frames that were transmitted by this port
txInternalErrs	Number of frames that were discarded because of an internal error during transmission
txMulticasts	Number of multicast frames that are queued for transmission by a higher-level protocol or application, including those not transmitted successfully
txPeakByteRate	Peak value of ethernetPortByteTransmitRate for this port since the station was last initialized
txPeakFrameRate	Peak value of ethernetPortFrameTransmitRate for this port since the station was last initialized
txQOverflows	Number of frames that were lost because transmit queue was full
txUnicasts	Number of unicast (nonmulticast) frames that are queued for transmission by a higher-level protocol or application, including frames not transmitted successfully

**management ip
interface summary**

Displays a summary table about the out-of-band system IP management interface configuration, including parameter settings.

✓ 3500
9000
9400

Valid Minimum Abbreviation

m ip i sum

3900
9300

Fields in the Management IP Interface Summary Display

Field	Description
Index	Unique number that identifies the out-of-band interface
IP address	IP address of the out-of-band interface, chosen from the range of addresses that the central agency assigned to your organization. This address is specific to your network and system.
IP routing status	Whether the interface is available to route IP traffic (<i>enabled</i>) or not (<i>disabled</i>)
RIP status	Whether RIP is dynamically configuring its routing tables (<i>active</i>) or on request (<i>passive</i>)
State	State of the IP interface, indicating whether the interface is available for communications (<i>up</i>) or unavailable (<i>down</i>).
Subnet mask	32-bit number that uses the same format and representation as an IP address. The subnet mask determines which bits in the IP address are interpreted as the network number, the subnet number, and the host number. Each IP address bit that corresponds to a 1 in the subnet mask is in the network/subnet part of the address. Each IP address bit that corresponds to a 0 is in the host part of the IP address.
Type	Type of device that is connected to the interface

**management ip
interface define**

Defines the IP address of the IP management out-of-band port.

Valid Minimum Abbreviation

m ip i d

Options✓ 3500
9000
94003900
9300

Prompt	Description	Possible Values	[Default]
IP address	IP address of the out-of-band interface, chosen from the range of addresses that the central agency assigned to your organization. This address is specific to your network and system.	Any valid IP address	–
Subnet mask	32-bit number that uses the same format and representation as an IP address. The subnet mask determines which bits in the IP address are interpreted as the network number, the subnet number, and the host number. Each IP address bit that corresponds to a 1 in the subnet mask is in the network/subnet part of the address. Each IP address bit that corresponds to a 0 is in the host part of the IP address.	Any subnet mask valid for use with the current IP address	255.255.0.0, or the subnet mask value currently stored in the system

**management ip
interface modify**

Changes the configuration of an IP management interface that you have already defined.

✓ 3500
9000
9400

Valid Minimum Abbreviation

```
m ip i m
```

Important Consideration

- Use the `management ip statistics` command to periodically monitor IP activity for your system. The statistics can help determine whether you need to change the IP management interface using the `management ip interface modify` command.

**management ip
interface remove**

Removes an IP management interface if you no longer need it.

Valid Minimum Abbreviation

```
m ip i r
```

Important Consideration

- Use the `management ip statistics` command to periodically monitor IP activity for your system. The statistics can help determine whether you need to remove the IP management interface using the `management ip interface remove` command.

✓ 3500
9000
9400

3900
9300

management ip route display

Displays the system's routing table to determine which routes to other IP networks are configured and whether the routes are operational.

✓ 3500
9000
9400

Valid Minimum Abbreviation

```
m ip ro di
```

Important Considerations

- The system prompts you for an IP address and subnet mask. This information enables you to display only a subset of routes instead of all routes. To see all entries in the table, press Return at the prompts.
- The first line in the output (the status line) indicates whether IP routing is enabled (in-band only):
 - IP interface options (such as ICMP router discovery) appear under `ip interface detail` and are set on a per-interface basis.
- The route table display includes a range for the routing table entries as follows:

```
There are n of m possible Routing Table entries.
```

```
Where n is the minimum and m is the maximum number of entries.
```

Options

Prompt	Description	Possible Values	[Default]
IP address	IP address that directs the system to display only those routes that match the bits set in the specified IP address (and its corresponding subnet mask) Press Enter to take the default, which displays all entries	A valid IP address	0.0.0.0
Subnet mask	Subnet mask that directs the system to display only those routes that match the bits set in the subnet mask for the specified IP address	A valid subnet mask	Based on specified IP address

Fields in the Management IP Route Display

Field	Description
Destination	IP address of the destination network, subnetwork, or host. This field can also identify a default route, which the system uses to forward packets that do not match any other routing table entry. You may want to use the default route in place of routes to numerous destinations that all have the same gateway IP address.
Gateway	Address that directs the router how to forward packets whose destination addresses match the route's IP address and subnet mask. The system forwards such packets to the indicated gateway.
Metric	Number of networks through which a packet must pass to reach a given destination. The system includes the metric in its RIP updates to allow other routers to compare routing information that is received from different sources.
Status	Status of the route. See the following route status table.
Subnet mask	Subnet mask that is associated with the IP address of the destination network, subnet, or host.

Status for Routes

Value	Description
Direct	Route is for a directly connected network
Learned	Route was learned using indicated protocol
Learned RIP	Route was learned using RIP-1 protocol
Learned RIP-Zombie	Route was learned but is partially timed out
Learned RIP2	Route was learned using RIP-2 protocol
Local	Actual interface address
Static	Route was statically configured
Timed out	Route has timed out and is no longer valid

management ip route static

Defines a static route.

✓ 3500
9000
9400

3900
9300

Valid Minimum Abbreviation

m ip r o s

Important Considerations

- Before you can define static routes, you must define at least one IP interface. See “ip interface define (3500/9000 Layer 3)” in Chapter 16 for more information.
- You can define up to 128 static routes.
- Static routes remain in the table until you remove them or the corresponding interface.
- Static routes take precedence over dynamically learned routes to the same destination.
- Static routes are not included in periodic Routing Information Protocol (RIP) updates sent by the system.

Options

Prompt	Description	Possible Values	[Default]
Destination IP address	IP address of the destination network, subnet, or host for this route	A valid IP address	–
Subnet mask	Subnet mask for the specified IP address	A valid subnet mask	Based on specified IP address
Gateway IP address	IP address of the gateway used by this route	A valid router address	–

**management ip route
remove**

Deletes an existing route.

✓ 3500
9000
9400

Valid Minimum Abbreviation

m ip ro r

Important Consideration

- When you enter the command, the system deletes the route immediately from the routing table. You are not prompted to confirm the deletion.

3900
9300

Options

Prompt	Description	Possible Values	[Default]
Destination IP address	IP address associated with the route that you want to delete	A valid IP address	—
Subnet mask	Subnet mask for the specified IP address	A valid subnet mask	Based on specified IP address

**management ip route
flush**

Deletes all learned routes from the routing table.

✓ 3500
9000
9400

Valid Minimum Abbreviation

m ip ro fl

Important Considerations

- The system deletes all learned routes from the routing table immediately. You are not prompted to confirm the deletion.
- Flushing the routing table causes Routing Information Protocol (RIP) to regenerate the routing table. The system repopulates the routing table a few seconds after you flush it.

**management ip route
default**

Adds a default route to the routing table immediately.

✓ 3500
9000
9400

3900
9300

Valid Minimum Abbreviation

m ip ro de

Important Considerations

- If you define a default route, the system uses it to forward packets that do not match any other routing table entry. The system can learn a route using the Routing Information Protocol (RIP), or you can statically configure a default route.
- If the routing table does not contain a default route, the system cannot forward a packet that does not match any other routing table entry. When the system drops the packet, it sends an ICMP destination unreachable message to the host that sent the packet.

Options

Prompt	Description	Possible Values	[Default]
Gateway IP address	IP address that is associated with the default route that you want to add (for example, 158.101.112.253)	A valid IP address	–

**management ip route
noDefault**

Deletes the default route.

✓ 3500
9000
9400

Valid Minimum Abbreviation

m ip r o n

Important Consideration

- The system deletes the default route from the routing table immediately after you enter the command. You are not prompted to confirm this deletion.

**management ip route
findRoute**

Searches for a route in the routing table.

✓ 3500
9000
9400

Valid Minimum Abbreviation

```
m ip route fi
```

Important Considerations

- This command enables you to find a route using an IP address or a host name, as long as Domain Name System (DNS) is configured.
- When you enter this command with a valid IP address or host name, the system displays the routing table entry.

3900
9300

Options

Prompt	Description	Possible Values	[Default]
IP address (or host name)	IP address that is associated with the route you that want to find, or a host name, if DNS is configured	A valid IP address or host name	0.0.0.0

management ip arp display

Display the contents of the Address Resolution Protocol (ARP) cache for each interface on the system.

✓ 3500
9000
9400

Valid Minimum Abbreviation

m ip ar d

Important Considerations

- The system uses the ARP cache to find the MAC addresses that correspond to the IP addresses of hosts and other routers on the same subnets. Each device that participates in routing maintains an *ARP cache*, which is a table of known IP addresses and their corresponding MAC addresses.
- The first line in the output (the status line) indicates whether IP routing is enabled (in-band only):
 - IP interface options (such as ICMP router discovery) appear under `ip interface detail` and are set on a per-interface basis. The second status line indicates the number of entries in the ARP cache.

Fields in the Management IP ARP Display

Field	Description
Hardware address	MAC address that is mapped to the IP address
IP address	IP address of the interface
Type	Type of entry, <code>static</code> or <code>dynamic</code>

**management ip arp
static**

Defines a static ARP cache entry on the system.

✓ 3500
9000
9400

3900
9300

Valid Minimum Abbreviation

```
m ip ar s
```

Important Consideration

- You can define up to 128 static ARP entries.

Options

Prompt	Description	Possible Values	[Default]
Interface index	Index number of the interface for which you want to define a static ARP entry	<ul style="list-style-type: none"> ■ A valid index number ■ ? (for a list of selectable indexes) 	–
IP address	IP address to use in the entry	A valid IP address	–
MAC address	Hardware address to use in the entry (in the format XX-XX-XX-XX-XX-XX)	A valid MAC address	–

Management IP ARP Static Example

```
Select interface index {1-2|?} 2
Enter IP address: 158.101.12.12
Enter MAC address: 00-00-00-00-00-01
```

management ip arp remove Deletes an entry from the ARP cache (for example, if the MAC address has changed).

✓ 3500
9000
9400

Valid Minimum Abbreviation

m ip ar rem

Important Considerations

- When you enter the command, the system deletes the entry immediately from the cache. You are not prompted to confirm the deletion.
- If necessary, the system subsequently uses ARP to find the new MAC address that corresponds to that IP address.

Options

Prompt	Description	Possible Values	[Default]
IP address	IP address that is associated with the entry that you want to delete	A valid IP address	–

**management ip arp
flushAll**

Deletes all entries from the ARP cache.

Valid Minimum Abbreviation

m ip ar flushA

Important Considerations

- This command applies to the CoreBuilder 3500 only; other platforms use `ip arp flush`. To flush dynamic entries only, see the “management ip arp flushDynamic” command next.
- When you enter the command, the system deletes all entries immediately from the cache. You are not prompted to confirm the deletions.

✓ 3500
9000
9400

3900
9300

**management ip arp
flushDynamic**

Deletes all dynamic (automatically learned) entries from the ARP cache.

Valid Minimum Abbreviation

m ip ar flushD

✓ **3500**
9000
9400

Important Considerations

- This command applies to the CoreBuilder 3500 only; other platforms use `ip arp flush`. To flush all entries, static and dynamic, see the previous “management ip arp flushAll” command.
- When you enter the command, the system deletes all dynamic entries immediately from the cache. You are not prompted to confirm the deletions.

management ip rip display

✓ 3500
9000
9400

3900
9300

Displays information about the Routing Information Protocol (RIP) interfaces on the system. RIP is one of the IP Interior Gateway Protocols (IGPs). When enabled, RIP allows the system to dynamically configure its routing tables.

Valid Minimum Abbreviation

```
m ip ri d
```

Important Considerations

- The first line in the output (the status line) indicates whether IP routing is enabled (in-band only):
 - IP interface options (such as ICMP router discovery) appear under `ip interface detail` and are set on a per-interface basis. The rest of the output contains more RIP interface information.
- The two available RIP modes are as follows:
 - **Disabled** — The system ignores all incoming RIP packets and does not generate any RIP packets of its own.
 - **Learn** — The system processes all incoming RIP packets, but it does not transmit RIP updates.

Fields in the Management IP RIP Display

Field	Description
Index	Index number of the interface
RIP-1 mode	Mode for RIP-1. If you disable RIP-1, the output lists the state as <code>off</code> . Other modes are <code>learn</code> (default), <code>advertise</code> , and <code>enabled</code> .
RIP-2 mode	Mode for RIP-2. If you disable RIP-2, the output lists the state as <code>off</code> . Other modes are <code>learn</code> (default), <code>advertise</code> , and <code>enabled</code> .

management ip rip mode

On a per-interface basis, sets one of four RIP Version 1 (RIP-1) modes and one of four RIP Version 2 (RIP-2) modes on the system.

✓ 3500
9000
9400

3900
9300

Valid Minimum Abbreviation

m ip ri m

Important Considerations

- The CoreBuilder 3500 supports RIP Version 1 as well as RIP Version 2. For each interface, you select a RIP Version 1 mode and a RIP Version 2 mode. The default RIP Version 1 mode for all platforms is `learn`. The default RIP Version 2 mode for the CoreBuilder 3500 is `disabled`.
- The four available RIP modes are as follows:
 - **Disabled** — The interface ignores all incoming RIP packets and does not generate any RIP packets of its own.
 - **Learn** — The interface processes all incoming RIP packets, but it does not transmit RIP updates. This is the default RIP mode.
 - **Advertise** — The interface broadcasts RIP updates, but it does not process incoming RIP packets.
 - **Enabled** — The interface broadcasts RIP updates and processes incoming RIP packets.

Options

Prompt	Description	Possible Values	[Default]
IP interfaces	Index number of the interface for which you want to set the RIP mode	<ul style="list-style-type: none"> ■ Selected interfaces ■ all ■ ? (for a list of selectable indexes) 	Previous entry, if applicable
RIP mode, Version 1	Selected RIP Version 1 mode that determines how the interface handles RIP 1 packets and updates	<ul style="list-style-type: none"> ■ disabled ■ learn ■ advertise ■ enabled 	learn, or current value
RIP mode, Version 2	How the interface handles RIP 2 packets and updates	<ul style="list-style-type: none"> ■ disabled ■ learn ■ advertise ■ enabled 	disabled, or current value

Management IP RIP Mode Example

```
Select menu option (management/ip/rip): mode
Select IP interfaces (1|all|?) [1]: 1
Interface 1 - Enter RIP Version 1 mode (disabled,learn) [learn]: disabled
Interface 1 - Enter RIP Version 2 mode (disabled,learn) [learn]: disabled
```

**management ip rip
statistics**

Displays general RIP statistics.

✓ 3500
9000
9400**Valid Minimum Abbreviation**

m ip rip s

3900
9300**Fields in the Management IP RIP Statistics Display**

Field	Description
queries	Number of queries
routeChanges	Number of route changes

management ip ping

Tries to reach or “ping” a specified destination using the default ping options.

✓ 3500

9000

9400

3900

9300

Valid Minimum Abbreviation

m ip p

Important Considerations

- This tool is useful for network testing, performance measurement, and management. It uses the Internet Control Message Protocol (ICMP) echo facility to send ICMP echo request packets to the IP destination that you specify.
- If you need to change the default ping options, use `management ip advancedPing`.
- You can either supply the host name or IP address as part of the command string, or you can supply the information at the prompt.
- When you specify a host name, the host name and its associated IP address *must* be configured on a network name server. Also, you must add the IP address on the name server to the list of name server addresses that are associated with the network domain name. See “ip dns define” in Chapter 16 for more information.
- When the system sends an echo request packet to an IP station using ping, the system waits for an ICMP echo reply packet. Possible responses:
 - If the host is reachable, the system displays information about the ICMP reply packets and the response time to the ping.
 - If the host does not respond, the system displays the ICMP packet information and this message: `Host is Not Responding`. You may not have configured your gateway IP address.
 - If the packets cannot reach the host, the system displays the ICMP packet information and this message: `Host is Unreachable`. A host is unreachable when there is no route to that host.
- To interrupt the command, press Enter.

Options

Prompt	Description	Possible Values	[Default]
Host name or IP address	Host name or IP address of the destination that you want to ping	A valid host name or IP address	0.0.0.0

Management IP Ping Example

```
Select menu option (ip): ping
Enter host name/IP address [0.0.0.0]: 158.101.111.50
Press "Enter" key to interrupt.

PING 158.101.111.50: 64 byte packets
64 bytes from 158.101.111.50: icmp_seq=0. time=16. ms
64 bytes from 158.101.111.50: icmp_seq=1. time=19. ms
64 bytes from 158.101.111.50: icmp_seq=2. time=24. ms

---- 158.101.111.50 PING Statistics ----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 16/20/24
```

**management ip
advancedPing**

Tries to reach or “ping” a host with one or more of the advanced ping options.

✓ 3500
9000
9400

Valid Minimum Abbreviation

m ip advancedP

Important Considerations

- When you specify a host name, the host name and its associated IP address *must* be configured on a network name server. Also, you must add the IP address on the name server to the list of name server addresses that are associated with the network domain name. See the `ip dns` commands in Chapter 16 for more information.
- The Burst option, when enabled, overrides the value that is set in the Quiet or Wait option.
- The Burst option floods the network with Internet Control Message Protocol (ICMP) echo packets and can cause network congestion. Do *not* use the Burst option during periods of heavy network traffic. Use this option only as a diagnostic tool in a network that has many routers to determine if one of the routers is not forwarding packets. For example, you can set a high count value (1000 packets), and then observe the run lights on the units: the run lights blink rapidly on routers that are forwarding packets successfully, but remain unlit, or blink slowly, on routers that are not forwarding packets successfully.
- To interrupt the command, press Enter.

Options

Prompt	Description	Possible Values	[Default]
Host name or IP address	Host name or IP address of the destination that you want to ping.	A valid host name or IP address	0.0.0.0
Number of ICMP Request packets	Number of ICMP echo request packets that are sent to ping a host. If the destination host does not respond after it is pinged by the number of packets that you specify, the system displays a <code>Host is Unreachable</code> or <code>Host is not Responding</code> message.	1 – 9999 packets	3

Prompt	Description	Possible Values	[Default]
Packet size	Number of bytes in each ICMP echo request packet. The packet size includes both the IP and the ICMP headers.	28 – 4096 bytes	64
Burst Transmit Ping mode	When <code>enabled</code> , sends out the ICMP echo request packets as rapidly as possible. The system displays a period (.) upon receiving an ICMP echo replay packet. Use this display to determine how many packets are being dropped during the burst. This is unique to the Burst option.	<ul style="list-style-type: none"> ■ disabled ■ enabled 	disabled
Quiet mode	How much packet information the system displays after a ping. When <code>enabled</code> , the system displays information about the number of packets that the system sent and received, any loss of packets, and the average time that it took a packet to travel to and from the host. When <code>disabled</code> , the system displays more detailed status information about each ICMP echo request packet.	<ul style="list-style-type: none"> ■ disabled ■ enabled 	disabled
Time between sending each packet (wait)	Number of seconds that the system waits before it sends out successive ICMP echo request packets. Set this option to a high value if network traffic is heavy and you do not want to add to the network traffic with pings in fast succession.	1 – 20 seconds	1
ICMP sourceAddress	Forces the source address of the ICMP packets to be something other than the IP address of the interface from which the packet originated. You can use this option if you have more than one IP interface defined.	<ul style="list-style-type: none"> ■ n (no) ■ y (yes) 	y
Interface index	Index number of the ICMP source IP address that you want to use.	Currently defined interfaces and their indexes	0 (the router picks the best interface)

Management IP Advanced Ping Example

```
Select menu option (ip): advancedPing
Enter host IP address [0.0.0.0]: 158.101.112.56
Enter number of ICMP request packets (1-9999) [3]:
Enter packet size (bytes) (28-4096) [64]:
Enter Burst Transmit Ping mode (disabled,enabled) [disabled]:
Enter Quiet mode (disabled,enabled) [disabled]:
Enter time (sec) waits between sending each packet (1-20) [1]: 2
Configure ICMP sourceAddress? (n,y) [y]:
      Index      Interface address
      0          Best interface (default)
      1          158.101.117.151
      2          158.101.10.1
Select interface index {0-2|?} [0]: 1
Press "Enter" key to interrupt.

PING 158.101.112.56 from 158.101.117.151: 64 byte packets
64 bytes from 158.101.112.56: icmp_seq=0.  time=26. ms
64 bytes from 158.101.112.56: icmp_seq=1.  time=18. ms
64 bytes from 158.101.112.56: icmp_seq=2.  time=18. ms

---- 158.101.112.56 PING Statistics ----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 18/21/26
```

management ip traceRoute

Traces a route to a destination using the default traceRoute options.

✓ 3500
9000
9400

3900
9300

Valid Minimum Abbreviation

m ip t

Important Considerations

- TraceRoute information includes all of the nodes in the network through which a packet passes to get from its origin to its destination. It uses the IP time-to-live (TTL) field in User Datagram Protocol (UDP) probe packets to elicit an Internet Control Message Protocol (ICMP) Time Exceeded message from each gateway to a host.
- To change the default traceRoute options, use the `management ip advancedTraceRoute` command.
- You can either supply the host name or IP address as part of the command string, or you can supply the information at the prompt.
- When you specify a host name, the host name and its associated IP address *must* be configured on a network name server. Also, you must add the IP address on the name server to the list of name server addresses that are associated with the network domain name. See Chapter 16 for more information about `ip dns` commands.
- To track the route of an IP packet, traceRoute launches UDP probe packets with a small TTL value and then listens for an ICMP Time Exceeded reply from a gateway. Probes start with a small TTL of 1 and increase the value by 1 until one of the following events occurs:
 - The system receives a Port Unreachable message, indicating that the packet reached the host.
 - The probe exceeds the maximum number of hops (default 30).
- At each TTL setting, the system launches three UDP probe packets, and the traceRoute display shows a line with the TTL value, the address of the gateway, and the round-trip time of each probe. If a probe answers from different gateways, the traceRoute feature prints the address of each responding system. If no response occurs in the 3-second timeout interval, traceRoute displays an asterisk (*) for that probe.

Other characters that can be displayed include the following:

- !N — Network is unreachable
- !H — Host is unreachable
- !P — Protocol is unreachable
- !F — Fragmentation is needed
- !<n> — Unknown packet type
- To interrupt the command, press Enter.

Options

Prompt	Description	Possible Values	[Default]
Host name or IP address	Host name or IP address of the destination to which you want to trace a route	A valid host name or IP address	0.0.0.0

Management IP Trace Route Example

```
Select menu option (ip): traceRoute
Enter host name/IP address [0.0.0.0]: 158.101.101.40
Press "Enter" key to interrupt.
```

```
Traceroute to 158.101.101.40: 30 hops max, 28 bytes packet
```

```
 1 158.101.117.254  9 ms 22 ms 5 ms
 2 158.101.112.254  8 ms 22 ms 8 ms
 3 158.101.96.22   7 ms 22 ms 7 ms
 4 158.101.101.40  7 ms 23 ms 6 ms
```

management ip advancedTraceRoute

Traces a route to a host with one or more of the advanced traceRoute options.

✓ 3500
9000
9400

Valid Minimum Abbreviation

m ip advancedT

Important Considerations

- When you specify a host name, the host name and its associated IP address *must* be configured on a network name server. Also, you must add the IP address on the name server to the list of name server addresses that are associated with the network domain name. See “ip dns define” in Chapter 16 for more information.
- To interrupt the command, press Enter.

Options

Prompt	Description	Possible Values	[Default]
Host name or IP address	Host name or IP address of the destination that you want to ping	<ul style="list-style-type: none"> ■ A valid host name ■ IP address 	0.0.0.0
Maximum ttl	Maximum number of hops that the system can use in outgoing probe packets	1 – 255 hops	30
Destination port	Destination (or base) UDP port number that the system uses in probe packets. Set the destination UDP port number to be very high to ensure that an application at the destination is not using that port.	30000 – 65535	33434
probeCount	Maximum number of probes that the system sends at each TTL level	1 – 10	3
Wait	Wait interval (in seconds) that determines the maximum amount of time that the system waits for a response to a probe	1 – 10 seconds	3
packetSize	Number of bytes that the system sends in each UDP probe packet	28 – 4096 bytes	28

Prompt	Description	Possible Values	[Default]
sourceAddress	Source address other than the one from which the probe packets originate. This option is available if you have more than one IP interface defined on the system.	<ul style="list-style-type: none"> ■ n (no) ■ y (yes) 	y
Interface index	Index number of the ICMP source IP address that you want to use. The system lists defined interfaces and their indexes.	A selectable interface	0 (the router picks the best interface)
Numeric mode	Whether the system shows hop addresses numerically or symbolically.	<ul style="list-style-type: none"> ■ disabled ■ enabled 	default

Management IP Advanced Trace Route Example (TTL value of 10):

```

Select menu option (ip): advancedTraceRoute
Enter host IP address [158.101.101.27]:
Enter maximum Time-to-Live (ttl) (1-255) [30]: 10
Enter Destination Port number (30000-65535) [33434]:
Enter the number of probes to be sent at each ttl level (1-10) [3]:
Enter time (sec) to wait for a response (1-10) [3]:
Enter the packet size (bytes) (28-4096) [28]:
Configure TRACEROUTE sourceAddress? (n,y) [y]:
      Index      Interface address
      0          Best interface (default)
      1          158.101.117.151
      2          158.101.10.1
Select interface index {0-2|?} [0]:
Enter Numeric mode (disabled,enabled) [disabled]:
Press "Enter" key to interrupt.

```

Traceroute to 158.101.101.27: 10 hops max, 28 bytes packet

```

1  158.101.117.254  12 ms   7 ms   5 ms
2  158.101.112.254  51 ms   9 ms   7 ms
3  158.101.96.22   21 ms  15 ms   6 ms
4  158.101.101.27  18 ms  90 ms  80 ms

```

management ip statistics

Displays different types of IP statistics: general statistics and those specific to the User Datagram Protocol (UDP) or the Internet Control Message Protocol (ICMP).

✓ 3500
9000
9400

Valid Minimum Abbreviation

m ip sta

3900
9300

Options

Prompt	Description	Possible Values	[Default]
Statistics	Type of IP statistics that you want to display	<ul style="list-style-type: none"> ■ ip ■ udp ■ icmp ■ all 	ip

Fields in the Management IP Statistics Display

Field	Description
forwDatagrams	Number of datagrams that the IP station tried to forward
fragCreates	Number of IP datagram fragments that were generated as a result of fragmentation on this system
fragFails	Number of IP datagrams that were discarded because they needed to be fragmented but could not be (for example, because their Don't Fragment bit was set)
fragOks	Number of IP datagrams that were successfully fragmented
inAddrErrors	Number of datagrams that the IP station discarded because of an error in the source or destination IP address
inDelivers	Number of datagrams that the IP station delivered to local IP client protocols
inDiscards	Number of packet receive discards
inHdrErrors	Number of datagrams that the IP station discarded because the IP header contained errors
inReceived	Total number of IP datagrams that were received, including those with errors
osReceives	Number of packets received that are destined to higher-level protocols such as Telnet, DNS, TFTP, and FTP
osTransmits	Number of packets that were sent through the router by higher-level protocols such as Telnet, DNS, TFTP, and FTP
outDiscards	Number of packet transmit discards

Field	Description
outNoRoutes	Number of datagrams that the IP station discarded because there was no route to the destination
outRequests	Number of datagrams that local IP client protocols passed to IP for transmission
reasmFails	Number of packet reassembly failures
reasmReqs	Number of packet reassembly requests
reasmOks	Number of successful packet reassemblies
rtDiscards	Number of packets that were discarded due to system resource errors
unkProtos	Number of packets whose protocol is unknown

Fields in the Management UDP Statistics Display

Field	Description
inDatagrams	Number of UDP packets that were received and addressed to the router or broadcast address
inErrors	Number of received UDP or ICMP packets that contain header errors
noPorts	Number of UDP packets that were received but addressed to an unsupported UDP port
outDatagrams	Number of UDP packets that were sent by the router

Fields in the Management ICMP Statistics Display

Field	Description
inAddrMaskReps	Number of ICMP address mask reply frames that were received
inAddrMasks	Number of ICMP address mask request packets that were received
inDestUnreach	Number of ICMP destination unreachable packets that were received
inEchoReps	Number of ICMP echo reply packets that were received
inEchos	Number of ICMP echo request packets that were received
inParmProbs	Number of ICMP parameter problem frames that were received
inRedirects	Number of ICMP redirect packets that were received
inSrcQuenchs	Number of ICMP source quench packets that were received
inTimeExcds	Number of ICMP time exceeded packets that were received

Field	Description
inTimeStamps	Number of ICMP time stamp request packets that were received
inTimeStampsReps	Number of ICMP time stamp reply packets that were received
messages	Number of ICMP packets that were received
outAddrMaskReps	Number of ICMP address mask reply packets that were sent
outAddrMasks	Number of ICMP address mask request packets that were sent
outDatagrams	Number of UDP packets that the router sent
outDestUnreach	Number of ICMP destination unreachable packets that were sent
outEchoReps	Number of ICMP echo reply packets that were sent
outEchos	Number of ICMP echo request packets that were sent
outErrors	Number of ICMP packets sent that were dropped due to system resource errors
outMsgs	Number of ICMP packets that were sent
outParmProbs	Number of ICMP parameter problem packets that were sent
outRedirects	Number of ICMP redirect packets that were sent
outSrcQuenchs	Number of ICMP source quench packets that were sent
outTimeExcds	Number of ICMP time exceeded packets that were sent
outTimeStampReps	Number of ICMP time stamp reply packets that were sent
outTimeStamps	Number of ICMP time stamp request packets that were sent

6

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

You can manage the system using a Simple Network Management Protocol (SNMP)-based external management application (called the SNMP manager) that sends requests to the system.

The SNMP agent provides access to the collection of information about the system, called Management Information Bases (MIBs). Your views of MIB information differ depending on the SNMP management method that you choose. In addition, you can configure an SNMP agent to send traps to an SNMP manager to report significant events. Access to system information through SNMP is controlled by community strings. You can use either an in-band or an out-of-band IP interface to manage the system with SNMP.

This chapter provides guidelines and other key information about how to set up SNMP in your system.

To configure SNMP for system management with SNMP:

- 1 Assign an IP address to either the system processor out-of-band Ethernet port or an in-band Ethernet port.
- 2 Set the destination IP address to which the traps are forwarded by the system agent.



For more information about setting up SNMP, see the Implementation Guide for your system.



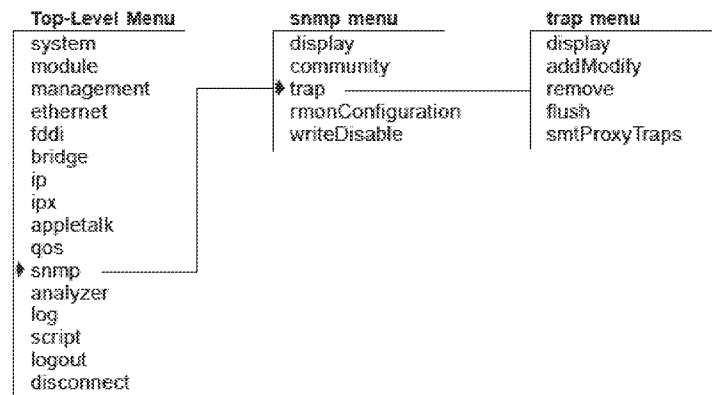
To set community strings, `snmp authentication_trap`, and `snmp extensions` on a CoreBuilder® 9000 Enterprise Switch, see the CoreBuilder 9000 Enterprise Management Engine User Guide.



You can access the Remote Monitoring (RMON) capabilities of the CoreBuilder 3500 through SNMP applications such as Transcend® Network Control Services software.

Menu Structure

The commands that you can use depend on the system that you have, your level of access, and the types of modules and other hardware options that are configured for your system. The following diagram shows the complete list of commands for all systems. See the checklist at the beginning of each command description in this chapter for whether your system supports the command.



snmp display Displays the current SNMP configurations for the community strings.

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

sn d

Fields in the SNMP Display

- ✓ 3900
- ✓ 9300

Field	Description
community string	Community strings setting that controls access to the system: <ul style="list-style-type: none"> ■ Read-only community strings with the default public ■ Read-write community strings with the default private

snmp community Sets two SNMP community strings: read-only and read-write.

✓ 3500
9000
✓ 9400



To set the community strings for the CoreBuilder 9000, see the CoreBuilder 9000 Enterprise Management Engine User Guide.

✓ 3900
✓ 9300

Valid Minimum Abbreviation

sn c

Important Considerations

- When an SNMP agent receives an SNMP request, the agent compares the community string in the request with the community strings that are configured for the agent:
 - SNMP *get*, *get-next*, and *set* requests are valid if the community string in the request matches the agent's read-write community.
 - SNMP *get* and *get-next* requests are valid if the community string in the request matches the agent's read-only community string or read-write community string.
- You can specify any string value up to 48 characters long. Do not use embedded spaces or the # symbol.
- If you do not want to change the value of a community string, press Return or Enter at either prompt.

Options

Prompt	Description	Possible Values	[Default]
Read-only	Octet string, included in each SNMP message, that provides read-only access to system information	<ul style="list-style-type: none"> ■ public ■ A string up to 48 characters long 	public
Read-write	Octet string, included in each SNMP message, that controls read-write access to system information	<ul style="list-style-type: none"> ■ private ■ A string up to 48 characters long 	private

SNMP Community Example (3500)

```
Select menu option (snmp): community
Enter new read-only community [public]:our_app
Enter new read-write community [private]: my_mail
```

snmp trap display Displays the SNMP traps and their currently configured destinations.

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

sn t d

Fields in the SNMP Trap Display

Field	Description
Trap description	Description of the system event that triggers the trap
Trap destinations configured	IP address of the system that is to receive event notification
Trap number	Identifying number of the trap that is associated with a system event
Trap numbers enabled	Traps that are active

snmp trap addModify

Adds or modifies trap reporting destination configurations. When an event occurs, the system sends the trap that you specify here to the destination address.

✓ 3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation`sn t a`**Important Considerations**

- You can define up to 10 destination addresses and the set of traps that are sent to each destination address.
- No unlisted traps are transmitted.
- Specify a range of more than two trap numbers with a hyphen (-) and nonsequential trap numbers with commas.
- If the destination address that you entered is not a valid end station, if a valid IP interface is not defined on the system, or if the agent does not have a route to the destination, the agent displays this message:

`Trap address invalid or unreachable`

If you see this message, verify the IP address of the end station, that it is online, and that a route exists to the intended management station.

- See the “Device Monitoring” chapter in the *Implementation Guide* for your system for an explanation of what the individual traps mean.

Options

Prompt	Description	Possible Values	[Default]
Trap destination address	Destination IP address of the SNMP manager	A valid destination IP address	-
Trap numbers to enable	Traps that you want to direct to the SNMP Manager	<ul style="list-style-type: none"> ■ A valid trap #, range, or sequence of valid trap #s ■ all ■ ? (for a list of available trap numbers) 	-

Procedure

- 1 From the top level of the Administration Console, enter:

```
snmp trap addModify
```

The system displays the list of traps.
- 2 Enter the IP address of the SNMP manager (destination address).
- 3 Enter one or more trap numbers for that destination, `all`, or `?` to get a list of selectable values.

SNMP Trap addModify Example (3500)

Select menu option (snmp/trap): `addModify`

Trap Descriptions:

Trap #	Description
1	MIB II: Coldstart
2	MIB II: Link Down
3	MIB II: Link Up
4	MIB II: Authentication Failure
5	Bridge MIB: New Root
6	Bridge MIB: Topology Change
7	3C System MIB: System Overtemperature
8	3C System MIB: Power Supply Failure
13	3C System MIB: Address Threshold
14	3C System MIB: System Fan Failure
15	3C FDDI MIB: SMT Hold Condition
16	3C FDDI MIB: SMT Peer Wrap Condition
17	3C FDDI MIB: MAC Duplicate Address Condition
18	3C FDDI MIB: MAC Frame Error Condition
19	3C FDDI MIB: MAC Not Copied Condition
20	3C FDDI MIB: MAC Neighbor Change
21	3C FDDI MIB: MAC Path Change
22	3C FDDI MIB: Port LER Condition
23	3C FDDI MIB: Port Undesired Connection
24	3C FDDI MIB: Port EB Error Condition
25	3C FDDI MIB: Port Path Change
26	RMON MIB: Rising Alarm
27	RMON MIB: Falling Alarm
28	POLL MIB: Response Received
29	POLL MIB: Response Not Received
32	VRRP MIB: New Master
33	VRRP MIB: Authentication Failure
35	QOS MIB: QOS INTRUDER Trap

Enter the trap destination address: `158.102.31.22`

Enter the trap numbers to enable (1-8,13-29,32-33,35|all|?)

`[1-8,13-29,32-33,35]: 35`

snmp trap remove Removes a destination, so that no SNMP traps are reported to that destination.

✓ 3500

✓ 9000

✓ 9400

Valid Minimum Abbreviation

sn t r

✓ 3900

✓ 9300

Important Consideration

- When the system removes the destination address, it displays the previous menu.

snmp trap flush Removes all SNMP trap reporting destinations.

✓ 3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sn t f

Important Consideration

- When you flush the SNMP trap reporting destinations, you remove all trap destination address information for the SNMP agent.

**snmp trap
smtProxyTraps**

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Controls SNMP's ability to alert you, by means of an SNMP-to-SMT proxy, that a significant event is occurring in the Fiber Distributed Data Interface (FDDI) station statistics.

✓ 3500

✓ 9000

9400

3900

9300

Valid Minimum Abbreviation

sn t s

Options

Prompt	Description	Possible Values	[Default]
SNMP-to-SMT proxy mode	Whether the SMT proxy agent is enabled or disabled	<ul style="list-style-type: none"> ■ enabled ■ disabled 	disabled

**snmp
rmonConfiguration**

✓ 3500
✓ 9000
9400

3900
9300

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Configures the transmit and receive mode to monitor Ethernet and Fiber Distributed Data Interface (FDDI) statistics as follows:

- **receive** — Monitors incoming port data
- **transmitAndReceive** — Monitors incoming and outgoing port data

Valid Minimum Abbreviation

sn r

Options

Prompt	Description	Possible Values	[Default]
Transmit/receive mode	Whether RMON is configured for only incoming port data, or for both incoming and outgoing port data	<ul style="list-style-type: none"> ■ receive ■ transmitAndReceive 	Current setting

snmp writeDisable Allows or disallows SNMP write requests.

✓ 3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

sn w

Options

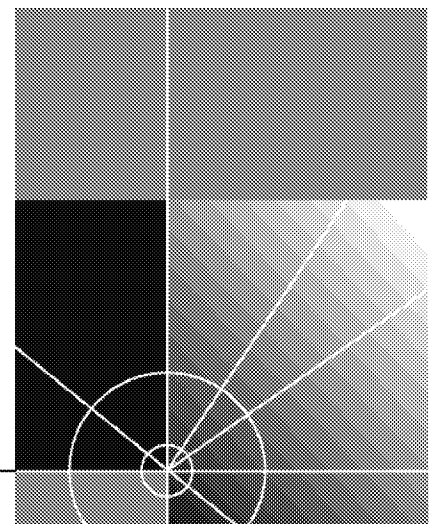
Prompt	Description	Possible Values	[Default]
SNMP write request mode	Whether SNMP write access is enabled or disabled	<ul style="list-style-type: none"> ■ off ■ on 	off



PHYSICAL PORT PARAMETERS

Chapter 7 Ethernet Ports

Chapter 8 Fiber Distributed Data Interface (FDDI)





ETHERNET PORTS

Before you configure your system, become familiar with the physical port numbering scheme on the system. Understanding the port numbering scheme enables you to:

- Manage your bridge ports (especially if you use trunking), as described in the *Implementation Guide* for your system
- Accurately define your virtual LANs (VLANs), as described in the *Implementation Guide* for your system

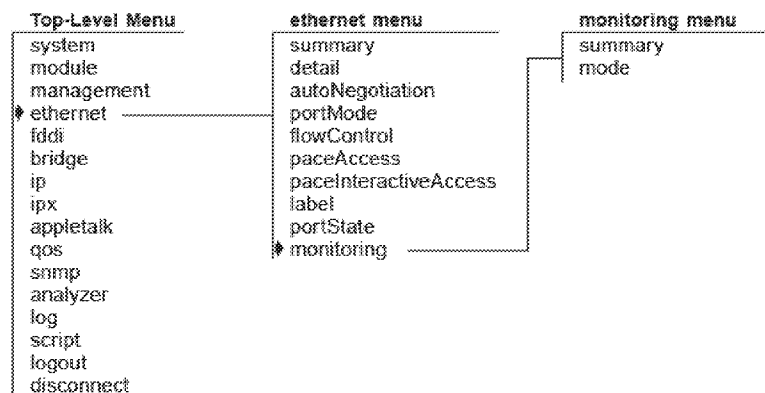
This chapter provides guidelines and other key information about how to configure Ethernet ports in your system.



For more information about port numbering and how to configure Ethernet ports, see the Implementation Guide for your system.

Menu Structure

The commands that you can use depend on your system, your level of access, and the modules and other hardware options that are configured for your system. The following diagram shows the list of commands for all systems. The checklist at the beginning of each command description in this chapter shows whether your system supports the command.



ethernet summary

Displays a summary of Ethernet port information. The summary shows the port's label and status, as well as the most pertinent statistics about general port activity and port errors.

✓ 3500
✓ 9000
✓ 9400

✓ 3900
✓ 9300

Valid Minimum Abbreviation

e s

Important Considerations

- Port numbering is consecutive, regardless of module type (if you are using a system that has modules).
- Depending on the system, numbering may or may not skip an empty slot and continue with the ports that are associated with the next occupied slot. (See the *Implementation Guide* for your system for specific information about port numbering.)
- Numbering includes unused ports.
- Only one port number is assigned to a Gigabit Ethernet module in switches that use Gigabit Ethernet modules.
- The system no longer assigns port number 1 to the out-of-band management port, which does not receive a port number.
- The `rxFrames` value that the Ethernet summary command reports for a bridge port may differ from the value that the bridge port summary command reports. The Ethernet summary command counts *all* frames that are delivered to the port while the bridge port summary command reports only *valid* frames that are passed to the port. Therefore, the Ethernet summary value should exceed the bridge port summary value by the number of receive errors (`rxErrors`).
- At some prompts, you can specify the `?` option to list Ethernet ports and port numbers. The `?` option displays Selection, Port, and Port Label columns. The Selection column and Port column contain the same port numbers because they represent your physical ports.

Fields in the Ethernet Summary Display

Field	Description
actualFlowControl	Actual flow control setting. When autonegotiation is completed, the value is the autonegotiated setting. When autonegotiation is disabled, the value is the user-selected flow control value.
actualPortMode	Actual operating port mode. When autonegotiation is completed, the values shown are the autonegotiated settings. When autonegotiation is disabled, the value is the user-selected port mode.
autoNegMode	Autonegotiation mode configured for port. Possible values are <code>enable</code> or <code>disable</code> .
autoNegState	Current negotiation state. Possible values are <code>disabled</code> , <code>configuring</code> , <code>completed</code> , and <code>failed</code> .
linkStatus	Boolean value that indicates the current state of the physical link for this port (either <code>enabled</code> or <code>disabled</code>).
macAddress	MAC address of this port.
noRxBuffers	Number of frames that were discarded because no buffer space was available.
portLabel	User-defined label name. The maximum length of the string is 32 characters, including the null terminator.
portState	Current software operational state of this port. Possible values are <code>on-line</code> , <code>off-line</code> , <code>partitioned</code> , <code>tx-fault</code> , and <code>config-error</code> . The value <code>on-line</code> appears when the port is both enabled and connected to a cable. The value <code>partitioned</code> appears when the port has been disabled by the ethernet port monitoring feature.
portType	Specific description of this port's type. Values for each port type: <code>10/100BASE-T (RJ45)</code> , <code>100BASE-FX (SC)</code> , <code>1000BASE-SX (SC)</code> , <code>1000BASE-LX (GBIC)</code> , <code>1000BASE-SX (GBIC)</code> , <code>Backplane (9000)</code> .
reqFlowControl	Configurable parameter that sets the flow control option (when autonegotiation is disabled). When autonegotiation is enabled, flow control values are ignored.
reqPortMode	Configurable parameter that sets the port mode on Ethernet ports that have port mode options (when autonegotiation is disabled). When autonegotiation is enabled, port mode values are ignored.
rxBytes	Number of bytes received by this port, including framing characters.
rxErrs	Total of all receive errors that are associated with this port.

Field	Description
rxFrames	Number of frames that were copied into receive buffers by this port.
slot:channel (9000 switch fabric module)	Maps a CoreBuilder® 9000 switch fabric module port to an interface module backplane link. The "channel" designation is just a backplane trace number. For example, to troubleshoot a problem with switch fabric module port 5 (slot:channel 3:1), look at the first backplane link for slot 3.
slot:port (9000)	Module slot and port number in the CoreBuilder 9000 system.
txBytes	Number of bytes that were transmitted by this port, including framing characters.
txErrs	Sum of all transmit errors that are associated with this port (summary report only).
txFrames	Number of frames that were transmitted by this port.
txQOverflows	Number of frames that were lost because transmit queue was full.
vendorName (3500)	Vendor name for a GBIC module. Other modules display n/a.

To display Ethernet port statistics relative to a baseline, see the *Implementation Guide* for your system.

Procedure

- To display summary information about Ethernet ports, enter:
`ethernet summary`
- At the prompt (for example, (1-24|a11|?)), select the ports whose information you want to display, or to display a port summary, specify ?
Indicate a range of ports with a hyphen (-). Separate nonconsecutive ports with a comma.

The system displays port information based on the ports that you specified.

ethernet detail

Displays detailed Ethernet port information including the information in the summary and additional Ethernet port statistics, such as collision counters.

✓ 3500
 ✓ 9000
 ✓ 9400

Valid Minimum Abbreviation

e d

✓ 3900
 ✓ 9300

Important Considerations

- Port numbering is consecutive, regardless of module type (if you are using a system that has modules).
- Depending on the system, numbering may or may not skip an empty slot and continue with the ports that are associated with the next occupied slot. (See the *Implementation Guide* for your system for specific information about port numbering.)
- Numbering includes unused ports.
- Only one port number is assigned to a Gigabit Ethernet module in switches that use Gigabit Ethernet modules.
- The system no longer assigns port number 1 to the out-of-band management port, which does not receive a port number.
- The `rxFrames` value that the Ethernet detail command reports for a bridge port may differ from the value that the bridge port detail command reports. The Ethernet detail command counts *all* frames that are delivered to the port while the bridge port detail command reports only *valid* frames that are passed to the port. Therefore, the Ethernet detail value should exceed the bridge port detail value by the number of receive errors (`rxErrors`).
- At some prompts, you can specify the `?` option to list Ethernet ports and port numbers. The `?` option displays Selection, Port, and Port Label columns. The Selection column and Port column contain the same port numbers because they represent your physical ports.

Fields in the Ethernet Detail Display

Field	Description
actualFlowControl	Actual flow control setting. When autonegotiation is completed, the value is the autonegotiated setting. When autonegotiation is disabled, the value is the user-selected flow control value.
actualPortMode	Actual operating port mode. When autonegotiation is completed, the value shown is the autonegotiated setting. When autonegotiation is disabled, the value is the port mode.
alignmentErrs (3500, 3900 and 9000)	Number of frames received by this port that are not an integral number of octets in length and do not pass the FCS check.
autoNegMode	Autonegotiation mode configured for port. Possible values are <code>enable</code> or <code>disable</code> .
autoNegState	Current negotiation state. Possible values are <code>disabled</code> , <code>configuring</code> , <code>completed</code> , and <code>failed</code> .
carrierSenseErr (3500, 3900 and 9000)	Number of frames that were discarded because the carrier sense condition was lost while transmitting a frame from this port.
excessCollision (3500, 3900 and 9000)	Number of frames that have been dropped because they experienced 15 consecutive collisions when sent from this port. This value is incremented by 1 each time that a frame experiences 15 consecutive collisions.
excessDeferrals (3500 and 9000 Layer 3)	Number of frames that were not transmitted on this port because the maximum allowed deferral time was exceeded.
fcsErrs	Number of frames received by this port that are an integral number of octets in length but do not pass the frame check sequence (FCS) test.
fragments (3900, 9000 Layer 2, 9300 and 9400)	Number of frames received by this port that were shorter than 64 bytes and had CRC or alignment errors.
jabbers (3900, 9000 Layer 2, 9300 and 9400)	Number of frames received by this port that were longer than 1518 bytes and had CRC or alignment errors.
lateCollisions (3500, 3900 and 9000)	Number of times that a collision was detected on this port later than 512 bit-times into the transmission of a frame.
lengthErrs (3500 and 9000 Layer 3)	Number of frames received by this port that are longer than 1518 bytes or shorter than 64 bytes.

Field	Description
linkStatus	Boolean value that indicates the current state of the physical link for this port (either <i>enabled</i> or <i>disabled</i>).
macAddress	MAC address of this port.
multiCollisions (3500, 3900 and 9000 Layer 3)	Number of frames that have experienced from 2 to 15 consecutive collisions <i>before successful transmission</i> from this port. If a frame also experiences a collision on the 15th attempt, it is dropped and the <i>excessCollision</i> count is increased by 1.
noRxBuffers	Number of frames that were discarded because no buffer space was available.
oversized (3900, 9000 Layer 2, 9300 and 9400)	Number of frames received by this port that were longer than 1518 bytes.
paceAccess (3900 and 9000 Layer 2)	Whether PACE® Interactive Access is <i>enabled</i> or <i>disabled</i> for this port.
portLabel	User-defined label name. The maximum length of the string is 32 characters, including the null terminator.
portState	Current software operational state of this port. Possible values are <i>on-line</i> , <i>off-line</i> , <i>partitioned</i> , <i>tx-fault</i> , and <i>config-error</i> . The value <i>on-line</i> appears when the port is both enabled and connected to a cable. The value <i>partitioned</i> appears when the port has been disabled by the ethernet port monitoring feature.
portType	Specific description of this port's type. Values for each port type: <i>10/100BASE-T (RJ45)</i> , <i>100BASE-FX (SC)</i> , <i>1000BASE-SX (SC)</i> , <i>1000BASE-LX (GBIC)</i> , <i>1000BASE-SX (GBIC)</i> , <i>Backplane (9000)</i> .
reqFlowControl	Configurable parameter that sets the flow control option (when autonegotiation is disabled). When autonegotiation is enabled, flow control values are ignored.
reqPortMode	Port mode on Ethernet ports that have port mode options (when autonegotiation is disabled). When autonegotiation is enabled, port mode values are ignored.
requestedState	Configurable parameter that is used to enable and disable this port. The default is <i>enabled</i> .
runts (3900, 9000 Layer 2, 9300 and 9400)	Number of frames received by this port that were shorter than 64 bytes.
rxBroadcast (3900, 9000 Layer 2, 9300 and 9400)	Number of broadcasts received by this port.

Field	Description
rxByteRate	Average number of bytes received per second by this port during the most recent sampling period.
rxBytes	Number of bytes received by this port, including framing characters.
rxDiscards (3500 and 9000 Layer 3)	Number of received frames that were discarded because there was no higher layer to receive them or because the port was disabled.
rxFrameRate	Average number of frames that were received per second by this port during the most recent sampling period. Sampling periods are 1 second long and not configurable.
rxFrames	Number of frames that were copied into receive buffers by this port.
rxInternalErrs	Number of frames that were discarded because of an internal error during reception.
rxMcastsOnly (3900, 9000 Layer 2, 9300 and 9400)	Number of multicast frames received by this port.
rxMulticasts	Number of multicast frames that were delivered to a higher-level protocol or application by this port.
rxPeakByteRate	Peak value of ethernetPortByteReceiveRate for this port since the station was last initialized.
rxPeakFrameRate	Peak value of ethernetPortFrameReceiveRate for this port since the station was last initialized.
rxUnicasts	Number of unicast (nonmulticast) frames that were delivered by this port to a higher-level protocol or application.
singleCollision (3500, 3900 and 9000)	Number of frames that have experienced only one collision before successful transmission from this port on the second attempt.
slot:port (9000)	Module slot and port number.
txBroadcasts (3900, 9000 Layer 2, 9300 and 9400)	Number of frames that were queued for transmission from this port by a higher-level protocol or application, including frames not transmitted successfully.
txByteRate	Average number of bytes that were transmitted per second by this port during the most recent sampling period.
txBytes	Number of bytes that were transmitted by this port, including framing characters.
txDiscards	Number of transmitted frames that were discarded because the port was disabled.

Field	Description
txFrameRate	Average number of frames that were transmitted per second by this port during the most recent sampling period. Sampling periods are 1 second long and not configurable.
txFrames	Number of frames that were transmitted by this port.
txInternalErrs	Number of frames that were discarded because of an internal error during transmission.
txMcastsOnly (3900, 9000 Layer 2, 9300 and 9400)	Number of multicast frames transmitted by this port.
txMulticasts	Number of multicast frames that were queued for transmission from this port by a higher-level protocol or application, including frames not transmitted successfully.
txPeakByteRate	Peak value of ethernetPortByteTransmitRate for this port since the station was last initialized.
txPeakFrameRate	Peak value of ethernetPortFrameTransmitRate for this port since the station was last initialized.
txQOverflows	Number of frames lost because transmit queue was full.
txUnicasts	Number of unicast (nonmulticast) frames that are queued for transmission by a higher-level protocol or application, including frames not transmitted successfully.
vendorName (3500)	Vendor name for a GBIC module. Other modules display n/a.

**ethernet
autoNegotiation**

Enables or disables autonegotiation of port attributes such as duplex mode and port speed on ports that support autonegotiation.

✓ 3500
✓ 9000
✓ 9400

Valid Minimum Abbreviation

e a

✓ 3900
✓ 9300

Important Considerations

- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.
- When you `enable` autonegotiation, the system ignores your requested `portMode` information for 10/100BASE-TX ports and your requested `flowControl` information for 1000BASE-SX ports. When you `disable` autonegotiation, the system recognizes the requested `portMode` values for ports that have `portMode` options and the requested `flowControl` values for 1000BASE-SX ports. (100BASE-FX ports and backplane ports do not support autonegotiation.)

Therefore, it is extremely important that you understand how to implement flowcontrol and `portMode` in your network. See the *Implementation Guide* for your system for more information.

Options

Prompt	Description	Possible Values	[Default]
Port	Port numbers for which you want to enable or disable autonegotiation	<ul style="list-style-type: none"> ■ A single port ■ A range of ports ■ all ■ ? (to display a port summary) 	–
Autonegotiation setting	Whether to enable or disable autonegotiation on each of the ports that you selected	<ul style="list-style-type: none"> ■ enable ■ disable 	enable

ethernet portMode Sets the port speed (10 Mbps or 100 Mbps) and the duplex mode (full-duplex or half-duplex) on individual ports.

✓ 3500
✓ 9000
9400

Valid Minimum Abbreviation

e portm

✓ 3900
9300

Important Considerations

- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.
- The device that is connected to each port must be configured for the same port mode. If the port speeds differ, the link does not come up. If the duplex modes differ, link errors occur.
- Gigabit Ethernet ports do not support mode options. The value `a11` refers only to ports that support port mode options.
- If you change to full-duplex mode on the port, a message indicates that collision detection will be disabled unless you configure the connected device to the same duplex mode.
- Disable autonegotiation on any port on which you are setting a specific port mode.
- 10/100BASE-TX supports the following modes and speeds:
 - 10 Mbps, full-duplex mode
 - 10 Mbps, half-duplex mode
 - 100 Mbps, full-duplex mode
 - 100 Mbps, half-duplex mode
- 100BASE-FX supports the following modes and speeds:
 - 100 Mbps, full-duplex mode
 - 100 Mbps, half-duplex mode

Options

Prompt	Description	Possible Values	[Default]
Port	Ports for which you want to change the portMode values	<ul style="list-style-type: none"> ■ A single port ■ A range of ports ■ all ■ ? (to display a port summary) 	–
Port mode setting	Speed and duplex mode for each of the ports that you selected	See “Important Considerations,” earlier in this section	10half (10/100BASE-TX) 100half (100BASE-FX)

Procedure

- 1 To change the port speed or duplex mode for 10/100BASE-TX ports or the duplex mode for 100BASE-FX ports, enter:
`ethernet portMode`
- 2 At the prompt (for example, (1-24|all|?)), enter the ports whose portMode values you want to change, or to display a port summary, specify ?

After you have selected the ports, the system prompts you to enter the port mode for the ports that you selected.

ethernet flowControl

Controls whether a Fast Ethernet or Gigabit Ethernet port can respond to or generate flow control packets.

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

e f

- ✓ 3900
- ✓ 9300

Important Considerations

- Flow control allows a port to:
 - Decrease the frequency with which it sends packets to a receiving device, if packets are being sent too rapidly.
 - Send flow control packets to a sending device, to request that the device slow its speed of transmission to the port.
- The system does not count flow control packets in either receive or transmit statistics.

Options

Prompt	Description	Possible Values	[Default]
Port selection	Ports for which you want to set flow control characteristics	<ul style="list-style-type: none"> ■ A single port ■ A range of ports ■ all ■ ? (to display a port summary) 	–
Flow control setting	Flow control characteristics for each of the ports that you selected	<ul style="list-style-type: none"> ■ on ■ off ■ rxOn ■ txOn 	off

Flow Control Settings

Setting	Description	Available on Port Type
on	Port recognizes flow control packets and responds by pausing transmission. The port can generate flow control packets as necessary to slow incoming traffic.	Gigabit Ethernet Fast Ethernet
off	Port ignores flow control packets and does not generate them.	Gigabit Ethernet Fast Ethernet
rxOn	Port recognizes flow control packets and responds by halting transmission. The port does not generate flow control packets.	Gigabit Ethernet
txOn	Port ignores flow control packets, but it can generate them, if necessary.	Gigabit Ethernet

ethernet paceAccess *For CoreBuilder 9000: Applies to Layer 2 switching modules only.*

- 3500
- ✓ 9000
- 9400

Configures the Ethernet ports on your system to support the PACE® Interactive Access feature, which ensures reliable timing by preventing excessive Ethernet network jitter (the variation in the timing of packet delivery that can cause garbled sound, jerky images, and delays).

- ✓ 3900
- 9300

Valid Minimum Abbreviation

e pa

Important Considerations

- PACE technology is 3Com’s method to provide reliable timing, optimal LAN bandwidth utilization, and data prioritization for time-sensitive multimedia and real-time applications, and data-only applications.
- PACE Interactive Access employs a “back-off” algorithm that enables your system to control traffic flow on a point-to-point link with an end station. When the network experiences congestion, the switch holds packets. PACE Interactive Access prevents an end station from “monopolizing” the link.

Options

Prompt	Description	Possible Values	[Default]
Port	Ports for which you want to set the PACE® feature	<ul style="list-style-type: none"> ■ A range of port numbers ■ all ■ ? (to display a port summary) 	–
PACE setting	Whether the PACE feature is on or off for each of the ports that you selected	<ul style="list-style-type: none"> ■ enable ■ disable 	disable

ethernet
paceInteractiveAccess

✓ 3500
✓ 9000
9400

3900
9300

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Configures the Ethernet ports on your system to support the PACE Interactive Access feature, which ensures reliable timing by preventing excessive Ethernet network jitter (the variation in the timing of packet delivery that can cause garbled sound, jerky images, and delays).

Valid Minimum Abbreviation

e pa

Important Considerations

- PACE technology is 3Com's method to provide reliable timing, optimal LAN bandwidth utilization, and data prioritization for time-sensitive multimedia and real-time applications, and data-only applications.
- PACE Interactive Access employs a "back-off" algorithm that enables your system to control traffic flow on a point-to-point link with an end station. When the network experiences congestion, the switch holds packets. PACE Interactive Access prevents an end station from "monopolizing" the link.

Options

Prompt	Description	Possible Values	[Default]
Port	Ports for which you want to set the PACE® feature	<ul style="list-style-type: none"> ■ A range of port numbers ■ all ■ ? (to display a port summary) 	–
PACE setting	Whether the PACE feature is on or off for each of the ports that you selected	<ul style="list-style-type: none"> ■ enable ■ disable 	disable

ethernet label Labels the Ethernet ports to help identify the kind of device that is attached to each port (for example, LAN, workstation, or server).

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

e 1

Important Considerations

- Label Ethernet ports so that you can easily identify the devices that are attached to them (such as LANs, workstations, or servers). For example: `engineeringserver`
- A new port label appears in system displays the next time that you display information for that port.

- ✓ 3900
- ✓ 9300

Options

Prompt	Description	Possible Values	[Default]
Port selection	Ports for which you want to define a port label	<ul style="list-style-type: none"> ■ A range of port numbers ■ all ■ ? (to display a port summary) 	–
Port label	Labels that appear the next time that you display information for the ports that you selected	String of up to 32 ASCII characters, including the null terminator	–

ethernet portState Enables or disables Ethernet ports, controlling whether the ports send or receive frames.

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

e ports

- ✓ 3900
- ✓ 9300

Important Consideration

- When an Ethernet port is `enabled`, frames are transmitted normally over that port. When an Ethernet port is `disabled`, the port neither sends nor receives frames.

Options

Prompt	Description	Possible Values	[Default]
Port	Ports that you want to enable or disable	<ul style="list-style-type: none"> ■ Individual ports ■ A range of port numbers ■ all ■ ? (to display a port summary) 	–
Port state	Value shown in the summary and detail displays reports: <code>on-line</code> for all enabled ports displayed and <code>off-line</code> for all disabled ports displayed	<ul style="list-style-type: none"> ■ enabled ■ disabled 	enabled

Procedure

- 1 To enable or disable an Ethernet port, from the top level of the Administration Console, enter:
`ethernet portState`
- 2 At the prompt (for example, `(1-24|all|?)`), enter the ports whose port state values you want to set, or to display a port summary, specify `?`
- 3 Enter `enabled` or `disabled` for each Ethernet port.

The `portState` value shown in the summary and detail displays reports `on-line` for all enabled ports that are displayed and `off-line` for all disabled ports. The Port Status LED for each disabled port on the module indicates the disabled status.

**ethernet monitoring
summary**

Displays the status of 10/100 Mbps Ethernet ports that are being monitored. The display shows the status of port statistics that are being monitored, including:

3500
✓ 9000
9400

- error count
- excessive collisions
- multiple collisions
- late collisions
- runts
- fcsErrs

✓ 3900
9300

Valid Minimum Abbreviation

e m s

Important Consideration

- The Ethernet monitoring feature is enabled by default, and performs these functions:
 - 1 Monitors 10/100Mbps Ethernet ports for excessive collisions, multiple collisions, late collisions, runts, and FCS errors
 - 2 Compares these error counters against user-defined thresholds
 - 3 Disables a port that reaches an error threshold
 - 4 Reports the reason that a port is disabled to the Administration Console, MIB databases, and SNMP traps
 - 5 Reenables the port after an initial backoff time interval
 - 6 Continues monitoring

ethernet monitoring mode

Enables or disables port monitoring on 10/100 Mbps Ethernet ports on the switch.

3500

✓ 9000

9400

✓ 3900

9300

Valid Minimum Abbreviation

e m m

Important Considerations

- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.
- You can determine when a monitored port is in error and has been disabled by these port statistics:
 - The `status` value shown in the ethernet monitoring summary display reports `partitioned`.
 - The `portState` value shown in the ethernet summary and ethernet detail displays reports `partitioned`.
 - The `linkStatus` value shown in the ethernet summary and ethernet detail displays reports `disabled`.

When the monitoring feature reenables the port, port statistics resume normal values.

- The Ethernet monitoring feature is enabled by default, and performs these functions:
 - 1 Monitors 10/100Mbps Ethernet ports for excessive collisions, multiple collisions, late collisions, runts, and FCS errors
 - 2 Compares these error counters against user-defined thresholds
 - 3 Disables a port that reaches an error threshold
 - 4 Reports the reason that a port is disabled to the Administration Console, MIB databases, and SNMP traps
 - 5 Reenables the port after an initial backoff time interval
 - 6 Continues monitoring

8

FIBER DISTRIBUTED DATA INTERFACE (FDDI)

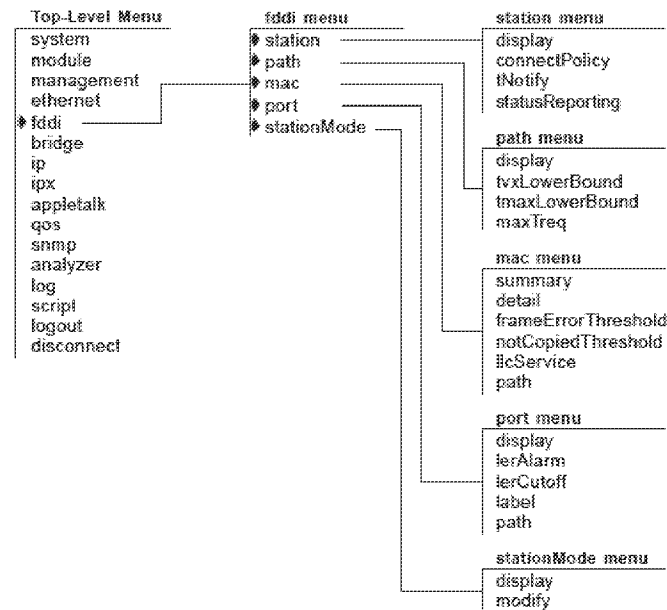
Fiber Distributed Data Interface (FDDI) is a standards-based solution that provides fast and reliable data transfer on a local area network. This chapter provides guidelines and other key information about how to configure FDDI parameters in your system.



For more information about implementing FDDI in your network, see the Implementation Guide for your system.

Menu Structure

The commands that you can use depend on the system that you have, your level of access, and the types of modules and other hardware options that are configured for your system. The following diagram shows the complete list of commands for all systems. See the checklist at the beginning of each command description in this chapter for whether your system supports the command.



fddi station display

Displays FDDI station information. The system display shows the station configuration, status reporting, and the most pertinent statistics about general station activity and errors.

✓ 3500

✓ 9000

9400

3900

9300

Valid Minimum Abbreviation

```
fd station d
```

Fields in the FDDI Station Display

Field	Description
configuration	Attachment configuration for the station or concentrator. Values can be <code>Thru</code> , <code>Isolated</code> , <code>Wrap_A</code> , and <code>Wrap_B</code> .
connectPolicy	Bit string that represents the connection policies in effect on a station. How connection policies translate into bits is described in "fddi station connectPolicy" in this chapter. This value is user-defined.
ecmState	Current state of the ECM state machine.
ports	Ports numbers assigned to the FDDI module. The FDDI port numbers change depending on the configuration of your system.
remoteDisconnect	Flag indicating that the station was remotely disconnected from the network as a result of receiving an <code>fddiSMTAction</code> with the value of <code>disconnect</code> in a Parameter Management Frame (PMF). A station requires a Connect Action to rejoin the network and clear the flag.
stationID	Unique identifier for the FDDI station.
statusReporting	Whether a station generates Status Report Frames (SRFs) to report events and conditions to network management stations. This value is user-defined.
tnotify	Timer used in the Neighbor Notification protocol to indicate the interval of time between generation of Neighbor Information Frames (NIF). This value is user-defined.
traceMaxExp	Maximum propagation time for a trace on an FDDI topology. Places a lower bound on the detection time for an unrecovering ring.

fddi station connectPolicy

Sets the connectPolicy attribute string that represents the connection policies in effect on a station. A connection's type is defined by the types of the two ports involved in the connection.

- ✓ 3500
- ✓ 9000
- 9400

- 3900
- 9300

Valid Minimum Abbreviation

fd station c

Important Considerations

- Port types can be A, B, M, or S.
- The system FDDI ports are type A or type B for Dual Attachment Station (DAS) ports and type M for Single Attachment Station (SAS) ports.
- By default, all connections to the system ports are valid. M-M connections are accepted so that one CoreBuilder® 3500 port can be connected to another system port.

Options

Prompt	Description	Possible Values	[Default]
Ports	One or more FDDI station ports for which you want to set the connection policies	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
connectPolicy	Bit string that represents the connection policies in effect on that station	See next table	–

Bit to Set for Rejecting a Station Connection

This Connection Is Rejected	If This Bit Is Set	Connection Rules
A-A	0	Undesirable peer connection that creates twisted primary and secondary rings; notify station management (SMT).
A-B	1	Normal trunk ring peer connection.
A-S	2	Undesirable peer connection that creates a wrapped ring; notify SMT.

This Connection Is Rejected	If This Bit Is Set	Connection Rules
A-M	3	Tree connection with possible redundancy. The node may not go to Thru state in Configuration Management (CFM). In a single MAC node, Port B has precedence (with defaults) for connecting to a Port M.
B-A	4	Normal trunk ring peer connection.
B-B	5	Undesirable peer connection that creates twisted primary and secondary rings; notify SMT.
B-S	6	Undesirable peer connection that creates a wrapped ring; notify SMT.
B-M	7	Tree connection with possible redundancy. The node may not go to Thru state in CFM. In a single MAC node, Port B has precedence (with defaults) for connecting to a Port M.
M-A	12	Tree connection with possible redundancy.
M-B	13	Tree connection with possible redundancy.
M-S	14	Normal tree connection.
M-M	15	Connection that allows one system port to be connected to another system port.

fddi station tNotify

Sets the timer used in the Neighbor Notification protocol to indicate the interval of time between generation of Neighbor Information Frames (NIF).

- ✓ 3500
- ✓ 9000
- 9400

- 3900
- 9300

Valid Minimum Abbreviation

fd station t

Important Considerations

- If you set the T-notify value low, your network reacts quickly to station changes, but uses more bandwidth.
- If you set the T-notify value high, less bandwidth is used, but your network does not react to station changes as quickly.

Options

Prompt	Description	Possible Values	[Default]
Ports	One or more FDDI station ports for which you want to set the neighbor notification timer	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
tnotify	Timer (in seconds) used in the Neighbor Notification protocol to indicate the interval of time between generation of Neighbor Information Frames (NIF)	2 – 30 seconds	30

**fdi station
statusReporting**

Controls whether a station generates Status Report Frames (SRFs) to report events and conditions to network management stations.

✓ 3500
✓ 9000
9400

Valid Minimum Abbreviation

`fd station s`

Important Consideration

- If you do not have an SMT management station listening to these event reports or if you use SNMP to monitor FDDI events on all FDDI end stations, set this attribute to `disabled` so that the station does not generate SRFs.

3900
9300

Options

Prompt	Description	Possible Values	[Default]
Ports	One or more FDDI station ports for which you want to set <code>statusReporting</code>	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
<code>statusReporting</code>	Parameter that controls whether a station generates Status Report Frames (SRFs) to report events and conditions to network management stations	<ul style="list-style-type: none"> ■ enabled ■ disabled 	enabled

fddi path display Displays FDDI path information.

- ✓ 3500
- ✓ 9000
- 9400

Valid Minimum Abbreviation

fd pa d

Important Consideration

- The path display changes slightly when ports are configured as DAS ports.

- 3900
- 9300

Fields in the FDDI Path Display

Field	Description
maxTReq	Maximum time value of fddiMACT-Req that any MAC that is configured in this path uses. This value can be user-defined.
path	Current selected path.
ports	Ports numbers that are assigned to the FDDI module. The FDDI port numbers change depending on the configuration of your system.
ringLatency	Total accumulated latency of the ring that is associated with this path.
tmaxLowBound	Minimum time value of fddiMACT-Max that any MAC that is configured in this path uses. This value can be user-defined.
traceStatus	Current trace status of the path.
tvxLowBound	Minimum time value of fddiMACTvxValue that any MAC that is configured in this path uses. This value can be user-defined.

Options

Prompt	Description	Possible Values	[Default]
Ports	One or more FDDI station ports for which you want to set the path display	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
Path	Path that you want to set. <ul style="list-style-type: none"> ■ A DAS port has primary and secondary paths. ■ A SAS port has only a primary path. 	<ul style="list-style-type: none"> ■ p (primary) ■ s (secondary) ■ all 	–

**fddi path
txvLowerBound**

Specifies the minimum time value (in microseconds) of fddiMAC txvValue that any MAC that is configured in this path uses.

✓ 3500
✓ 9000
9400

3900
9300

Valid Minimum Abbreviation

fd pa tv

Important Considerations

- A MAC uses its valid transmission timer (TVX) to detect and recover from certain ring errors. If a valid frame has not passed through a MAC during the time indicated by fddiMACTvxValue, the MAC reinitializes the ring.
- By adjusting the txvLowerBound value, you specify how quickly the ring recovers from an error. The lower you set this value, the faster the network reacts to problems, but the ring might be reinitialized when there is no problem.
- The higher you set this value, the less chance of frequent reinitializations, but the network takes longer to recover from errors.
- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.

Options

Prompt	Description	Possible Values	[Default]
Ports	One or more FDDI station ports for which you want to set the txvLowerBound	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
Path	Path that you want to set: <ul style="list-style-type: none"> ■ A DAS port has primary and secondary paths. ■ A SAS port has only a primary path. 	<ul style="list-style-type: none"> ■ p (primary) ■ s (secondary) ■ all 	–
txvLowerBound	Minimum time value of fddiMAC txvValue that any MAC that is configured onto this path uses	0 – 4294967295 microseconds	2500

**fddi path
tmaxLowerBound**

- ✓ 3500
- ✓ 9000
- 9400

- 3900
- 9300

Specifies the minimum time value (in microseconds) of fddiMAC T-Max that any MAC that is configured in this path uses. This value specifies the boundary for how high T-Req (the requested token rotation time) can be set.

Valid Minimum Abbreviation

fd pa tm

Important Consideration

- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.

Options

Prompt	Description	Possible Values	[Default]
Ports	One or more FDDI station ports for which you want to set the tmaxLowerBound	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
Path	Path that you want to set. <ul style="list-style-type: none"> ■ A DAS port has primary and secondary paths. ■ A SAS port has only a primary path. 	<ul style="list-style-type: none"> ■ p (primary) ■ s (secondary) ■ all 	–
tmaxLowerBound	Minimum time value of fddiMAC T-Max that any MAC that is configured onto this path uses	0 – 4294967295 microseconds	16500

fdi path maxTreq Specifies the maximum time value (in microseconds) of fdiMACT-Req that is used by any MAC that is configured in this path. T-Req is the value that a MAC bids during the claim process to determine a ring's operational token rotation time, T_Opr. The lowest T-Req bid on the ring becomes T_Opr.

✓ 3500
✓ 9000
9400

3900
9300

Valid Minimum Abbreviation

fd pa m

Important Considerations

- When you set T_Opr low, the token rotates more quickly, so token latency is reduced. However, more of the ring's available bandwidth is used to circulate the token.
- Higher values of T_Opr use less bandwidth to circulate the token, but they increase token latency when the ring is saturated.
- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.

Options

Prompt	Description	Possible Values	[Default]
Ports	One or more FDDI station ports for which you want to set the path maxTreq	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
Path	Path that you want to set. <ul style="list-style-type: none"> ■ A DAS port has primary and secondary paths. ■ A SAS port has only a primary path. 	<ul style="list-style-type: none"> ■ p (primary) ■ s (secondary) ■ all 	–
maxTreq	Value that a MAC bids during the claim process to determine a ring's operational token rotation time, T_Opr	0 – 4294967295 microseconds	16500

fdi mac summary

✓ 3500
 ✓ 9000
 9400

3900
 9300

Displays a summary of FDDI MAC information. A summary report displays various FDDI MAC statistics, including information about the MAC, received and transmitted frames, and received and transmitted bytes.

Valid Minimum Abbreviation

fd m s

Important Consideration

- The MAC summary display changes slightly when ports are configured as DAS ports.

Fields in the FDDI MAC Summary Display

Field	Description
currentPath	Path on which this MAC is currently located (primary, secondary, or isolated)
downstream	MAC address of this MAC's downstream neighbor
Errors	Sum of errorCount, lateCount, lostCount, and txExpiredCount
noRxBuffers	Number of frames discarded because no buffer space was available
port	Port numbers assigned to the FDDI module. The FDDI port numbers change depending on the configuration of your system.
rxBytes	Number of bytes that this MAC received
rxErrors	Number of errors that this MAC received
rxFrames	Number of frames that this MAC received
station	Unique identifier for the FDDI station.
smtAddress	Address of the MAC that was used for SMT frames
txBytes	Number of bytes that this MAC transmitted
txFrames	Number of frames that this MAC transmitted. This number does not include MAC frames.
txQOverflows	Number of frames that were discarded because the transmit queue was full
upstream	MAC address of this MAC's upstream neighbor

fddi mac detail

Displays detailed FDDI MAC information. A detail report displays various FDDI MAC statistics, including information about the MAC, received and transmitted frames, and received and transmitted bytes, as well as additional FDDI MAC statistics.

✓ 3500

✓ 9000

9400

3900

9300

Valid Minimum Abbreviation

fd m d

Important Consideration

- The MAC summary display changes slightly when ports are configured as DAS ports.

Fields in the FDDI MAC Detail Display

Field	Description
currentPath	Path on which this MAC is currently located <i>primary or secondary, isolated, concatenated, or thru</i>
downstream	MAC address of this MAC's downstream neighbor
downstreamType	PC type of this MAC's downstream neighbor
dupAddrTest	Pass or fail test for a duplicate address
duplicateAddr	Whether this address is duplicated on the FDDI ring
errorCount	Number of SMT MAC errors
frameCount	Number of frames that this MAC received
frameErrCond	Active when the frameErrorRatio is greater than or equal to frameErrorThresh.
frameErrorRatio	Ratio of the number lostCount plus the frameErrorCount divided by the frameCount plus lostCount
frameErrThresh	Threshold for determining when a MAC condition report is generated
lateCount	Number of token rotation timer expirations since this MAC last received a token
llcAvailable	Whether this MAC can send or receive LLC frames
llcService	Setting of the Logical Link Control service
lostCount	Number of frames and tokens that this MAC lost during reception
noRxBuffers	Number of frames discarded because no buffer space was available
notCopiedCond	Active when the notCopiedRatio is greater than or equal to notCopiedThresh.

Field	Description
notCopiedCount	Number of frames that were addressed to this MAC but were not copied into its receive buffers
notCopiedRatio	Ratio of notCopiedCount divided by the quantity copiedCount plus notCopiedCount
notCopiedThresh	Threshold for determining when a MAC condition report is generated
oldDownstream	Previous value of the MAC address of this MAC's downstream neighbor
oldUpstream	Previous value of the MAC address of this MAC's upstream neighbor
ringOpCount	Number of times that this MAC has entered the operational state from the nonoperational state
rmtState	State of the ring management as defined in SMT
rxByteRate	Average number of bytes per second that this MAC received during the most recent sampling period
rxBytes	Number of bytes that this MAC received
rxDiscards	Number of good frames that this MAC received and discarded before being delivered to a higher-level protocol or application. Does not include frames that were not received into receive buffers, such as missed frames.
rxFrameRate	Average number of frames per second that this MAC received during the most recent sampling period
rxFrames	Number of frames that this MAC received
rxInternalErrs	Number of frames discarded because of an internal hardware error during reception
rxMulticasts	Number of multicast frames that this MAC delivered to a higher-level protocol or application
rxPeakByteRate	Peak value of fddiMACByteReceiveRate for this MAC since the station was last initialized
rxPeakFrameRate	Peak value of fddiMACFrameReceiveRate for this MAC since the station was last initialized
rxUnicasts	Number of unicast (nonmulticast) frames that this MAC delivered to a higher-level protocol or application
smtAddress	Address of the MAC used for SMT frames
tMax	Maximum value of the target token rotation time
tMaxCapab	Maximum supported target token rotation time that this MAC can support
tNeg	Target token rotation time negotiated during the claim process
tokenCount	Number of tokens that this MAC received

Field	Description
tReq	Target token rotation time that this MAC requested
txCapab	Maximum time value of the valid transmission timer that this MAC can support
txExpiredCount	Number of times that this MAC's valid transmission timer has expired
txValue	Value of the valid transmission timer that this MAC uses
txByteRate	Average number of bytes that this MAC transmitted per second during the most recent sampling period
txBytes	Number of bytes that this MAC transmitted
txDiscards	Number of frames discarded because LLC service was not enabled or the FDDI ring was not operational
txFrameRate	Average number of frames that this MAC transmitted per second during the most recent sampling period
txFrames	Number of frames that this MAC transmitted. This number does not include MAC frames.
txInternalErrs	Number of frames discarded because of an internal hardware error during transmission
txMulticasts	Number of multicast frames queued for transmission by a higher-level protocol or application, including frames not transmitted successfully
txPeakByteRate	Peak value of fddiMACByteTransmitRate for this MAC since the station was last initialized
txPeakFrameRate	Peak value of fddiMACFrameTransmitRate for this MAC since the station was last initialized
txQOverflows	Number of frames discarded because the transmit queue was full
txUnicasts	Number of unicast frames queued for transmission by a higher-level protocol or application, including frames not transmitted successfully
upstream	MAC address of this MAC's upstream neighbor
upstreamDupAddr	Whether the address upstream of this address is duplicated on the ring

**fddi mac
frameErrorThreshold**

Determines when the system generates a MAC condition report because too many frame errors have occurred.

- ✓ 3500
- ✓ 9000
- 9400

Valid Minimum Abbreviation

fd m f

Important Considerations

- 3900
- 9300

- A frame error occurs when a frame becomes corrupted.
- A high frame error rate often indicates a faulty station on the FDDI ring or a dirty FDDI connector.
- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.

Options

Prompt	Description	Possible Values	[Default]
Ports	One or more FDDI station ports for which you want to set the mac frameErrorThreshold	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
frameErrorThreshold value	Time value set to determine when the system generates a MAC condition report because too many frame errors have occurred	0 – 4294967295 microseconds	655

fdi mac notCopiedThreshold Sets the timing when the system generates a MAC condition report because too many frames could not be copied.

✓ 3500
✓ 9000
9400

Valid Minimum Abbreviation

f d m n

Important Considerations

- Not-copied frames occur when there is no buffer space available in the station (which in turn indicates congestion in the station).
- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.

Options

Prompt	Description	Possible Values	[Default]
Ports	One or more FDDI station ports for which you want to set the mac notCopiedThreshold	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
notCopiedThreshold	Time value set to determines when the system generates a MAC condition report because too many frames could not be copied	0 – 4294967295 microseconds	6550

fdi mac llcService

Sets the Logical Link Control (LLC) service so that LLC frames are sent and received on the MAC. LLC frames are all data frames that are transmitted on the network.

- ✓ 3500
- ✓ 9000
- 9400

- 3900
- 9300

Valid Minimum Abbreviation

fd m 1

Important Considerations

- If there is something wrong on your network, you may want to turn off data (user) traffic for a MAC by disabling LLC service. Although you have disabled data traffic from the MAC, the MAC still participates in neighbor notification and is visible to network management.
- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.

Options

Prompt	Description	Possible Values	[Default]
Ports	One or more FDDI station ports for which you want to set the mac llcService	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
llcService	Whether LLC frames are sent and received on the MAC	<ul style="list-style-type: none"> ■ enabled ■ disabled 	enabled

fddi mac path Sets the path assignment for MACs.

✓ 3500

✓ 9000

9400

3900

9300

Valid Minimum Abbreviation

f d m p

Important Considerations

- The fddiMAC path selections depend on the stationMode configuration (DAS or SAS).
- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.

Options

Prompt	Description	Possible Values	[Default]
Ports	One or more FDDI station ports for which you want to set the MAC path	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
MAC path	Path assignments for MACs	For DAS ports: <ul style="list-style-type: none"> ■ primary ■ secondary ■ isolated For SAS ports: <ul style="list-style-type: none"> ■ primary ■ isolated 	primary

fdi port display

Displays information about FDDI ports, including the type, path, and port label, as well as other FDDI port statistics, such as error counters.

- ✓ 3500
- ✓ 9000
- 9400

Valid Minimum Abbreviation

fd po d

- 3900
- 9300

Fields in the FDDI Port Display

Field	Description
connectState	Connect state of this port (disabled, connecting, standby, or active)
currentPath	Path on which this port is currently located
ebErrorCond	Whether an elasticity buffer error has been detected during the past 2 seconds
ebErrorCount	Number of elasticity buffer errors that have been detected
lctFailCount	Number of consecutive times that the link confidence test (LCT) has failed during connection management
lernCount	Number of link errors that this port detected
lernRejectCount	Number of times that the link error monitor rejected the link
lerAlarm	Link error rate estimate at which a link connection generates an alarm
lerCondition	Whether the lerEstimate is less than or equal to lerAlarm
lerCutoff	Link error rate estimate at which a link connection is broken
lerEstimate	Average link error rate. It ranges from 10 ⁻⁴ to 10 ⁻¹⁵ and is reported as the absolute value of the exponent of the link error estimate
lineState	Line state of this port
myType	Type of port connector on the port (A, B, S, M)
neighborType	Type of port connector at the other end of the physical connection (A, B, S, M)
pcmState	Current Physical Connection Management (PCM) state defined in SMT
pcWithhold	Reason for withholding the connection
pmdClass	Type of PMD entity that is associated with this port
port	Ports numbers that are assigned to the FDDI module. The FDDI port numbers change depending on the configuration of your system.
portLabel	32-character string of a user-defined name for the port

fdi port lerAlarm Sets the link error rate (LER) value at which a link connection generates an alarm.

✓ 3500

✓ 9000

9400

3900

9300

Valid Minimum Abbreviation

fd po lerA

Important Considerations

- The lerAlarm value is expressed as the absolute value of the exponent (such as 1×10^{-10}). A healthy network has an LER exponent between 1×10^{-10} and 1×10^{-15} .
- If the LER value is greater than the alarm setting, then SMT sends a Status Report Frame (SRF) to the network manager software indicating a problem with a port.
- Set the lerAlarm value below these values so that you receive alarms only if your network is in poor health. The SMT Standard recommended value is 8.
- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.

Options

Prompt	Description	Possible Values	[Default]
Ports	One or more FDDI station ports for which you want to set the port lerAlarm	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
lerAlarm value	Link error rate (LER) value at which a link connection generates an alarm	4 – 15	7

fddi port lerCutoff

Sets the link error rate estimate at which a link connection is disabled. When the lerCutoff value is reached, the PHY that detected a problem is disabled.

- ✓ 3500
- ✓ 9000
- 9400

- 3900
- 9300

Valid Minimum Abbreviation

fd po lerC

Important Considerations

- The lerCutoff value must be lower than the lerAlarm value so that the network management software is alerted to a problem before the PHY (port) is actually removed from the network.
- Set the lerCutoff below these values so that a port is removed only as a last resort. The SMT Standard recommended value is 7.
- The lerCutoff value is expressed as an exponent (such as 1×10^{-10}). A healthy network has an LER exponent between 1×10^{-10} and 1×10^{-15} .
- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.

Options

Prompt	Description	Possible Values	[Default]
Ports	One or more FDDI station ports for which you want to set the port lerCutoff	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
lerCutoff	Link error rate estimate at which a link connection is disabled	4 – 15	4

fddi port label

Assigns a unique name to your FDDI ports for easy identification of the devices that are attached to them (for example, workstation, server, FDDI backbone). Port labels serve as useful reference points and as an accurate means of identifying your ports for management.

✓ 3500

✓ 9000

9400

3900

9300

Valid Minimum Abbreviation

```
fd po label
```

Important Consideration

- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.

Options

Prompt	Description	Possible Values	[Default]
Ports	One or more FDDI station ports for which you want to set the port label	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
Label	Name of the FDDI port used for identification	–	–

fddi port path Sets the one or more FDDI ports to be either part of the primary path or isolated from the ring.

- ✓ 3500
- ✓ 9000
- 9400

Valid Minimum Abbreviation

fd po p

- 3900
- 9300

Options

Prompt	Description	Possible Values	[Default]
Ports	One or more FDDI station ports for which you want to set the path	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
Path	Sets the type of path used by the port: <ul style="list-style-type: none"> ■ isol — isolates the port from the ring ■ pri — sets the port to be part of the primary ring 	<ul style="list-style-type: none"> ■ isol ■ pri 	pri

**fddi stationMode
display**

Generates a display of FDDI stationMode information. The display shows the station mode, DAS (Dual Attachment Station) or SAS (Single Attachment Station), for each FDDI port.

✓ 3500
✓ 9000
9400

Valid Minimum Abbreviation

```
fd stationM d
```

3900
9300

Important Consideration

- Before the new stationMode takes effect, you must reboot your system.

Fields in the FDDI Station Mode Display

Field	Description
Ports	Ports numbers that are assigned to the FDDI module. The FDDI port numbers change, depending on the configuration of your system.
stationMode	Current FDDI stationMode, DAS or SAS, that is assigned to a specific port.

fdi stationMode modify Modifies the stationMode, DAS or SAS, that is assigned to a specific port number.

- ✓ 3500
- ✓ 9000
- 9400

Valid Minimum Abbreviation

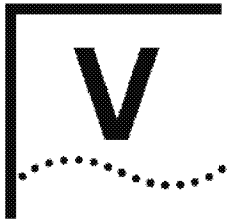
fd stationM m

Important Considerations

- 3900
- 9300
- You cannot modify the stationMode when any of the ports in the pair are part of a trunk.
- Before the new stationMode takes effect, you must reboot your system.
- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.

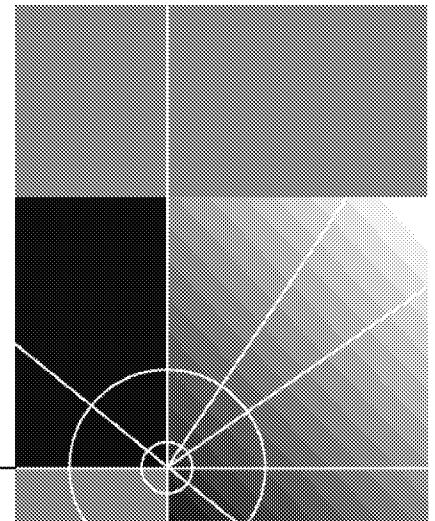
Options

Prompt	Description	Possible Values	[Default]
Ports	FDDI station port for which you want to set the stationMode	<ul style="list-style-type: none"> ■ Any of the available ports on the installed FDDI modules ■ all 	–
stationMode	Mode of the FDDI port pair selected to change	<ul style="list-style-type: none"> ■ DAS ■ SAS 	SAS
reboot	Prompt to reboot the system if you want the stationMode changes to take effect	<ul style="list-style-type: none"> ■ y (yes) ■ n (no) 	–



BRIDGING PARAMETERS

- Chapter 9** **Bridge-Wide Parameters**
- Chapter 10** **Bridge Port Parameters**
- Chapter 11** **Trunks**
- Chapter 12** **MultiPort Link Aggregation (MPLA)**
- Chapter 13** **Resilient Links**
- Chapter 14** **Virtual LANs (VLANs)**
- Chapter 15** **Packet Filters**



9

BRIDGE-WIDE PARAMETERS

This chapter provides guidelines and other key information about how use the Administration Console to configure bridge-wide parameters.



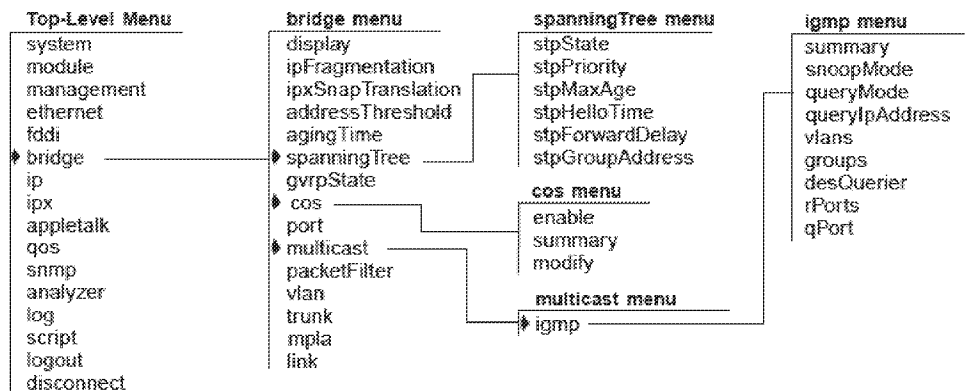
This chapter addresses the commands in the bridge menu, except port, packetFilter, vlan, trunk, mpla, and link, which other chapters in this Command Reference Guide address.



For more information about configuring bridging and related features, see the Implementation Guide for your system.

Menu Structure

The commands that you can use depend on the system that you have, your level of access, and the types of modules and other hardware options that are configured for your system. The following diagram shows the complete list of commands for all systems. See the checklist at the beginning of each command description in this chapter for whether your system supports the command.



bridge display Displays bridge statistics and configuration information including Spanning Tree Protocol (STP) parameter values.

✓ 3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

b d

Fields in the Bridge Display

Field	Description
addressCount	Number of addresses in the bridge address table at the point in time in which you are viewing it. This value fluctuates but the highest value reached is recorded in the <code>PeakAddrCount</code> field.
addrTableSize	Maximum number of addresses that can be stored in the bridge address table. For CoreBuilder® switches, the value is 32K. For SuperStack® II Switches, the value is 16K.
addrThreshold	Configurable reporting threshold for the total number of addresses known on this bridge. When this threshold is reached, the system generates the SNMP trap <code>addressThresholdEvent</code> . The range of valid values for setting this object is between 1 and 1 plus the maximum table size. To configure this value for the 3500 and 9000 L3 modules, see "bridge addressThreshold" later in this chapter. This option is not available for the 3900, 9300, 9400 and 9000 L2 modules at this release.
agingTime	Configurable time period in seconds that the bridge uses to age out dynamic addresses except when a topology change has occurred. (After a topology change, the bridge uses the value shown in the <code>forwardDelay</code> field instead until it receives configuration messages without the topology change flag set). The default value for <code>agingTime</code> is 300 seconds. The acceptable range is 10 – 1,000,000. You can also enter 0 to disable aging. To configure this value, see "bridge agingTime" later in this chapter.
bridgeFwdDelay	Configurable time period in seconds that the bridge spends in <i>each of</i> two states — listening and learning — before it transitions to the forwarding state, provided that the bridge is the root bridge. (If the bridge is not the root bridge, the bridge uses the value shown in the <code>fwdDelay</code> field that is assigned to it by the root bridge.) The default value is 15 seconds. The acceptable range is 4 – 30 seconds. To configure the bridge forward delay, see "bridge spanningTree stpForwardDelay" later in this chapter.

Field	Description
bridgeHelloTime	Configurable time period in seconds that elapses between configuration messages when the bridge is the root bridge. (If the bridge is not the root bridge, the bridge uses the value shown in the <code>helloTime</code> field which is assigned to it by the root bridge.) The default value is 2 seconds. The acceptable range is 1 – 10 seconds. To configure the bridge hello time, see “bridge spanningTree stpHelloTime” later in this chapter.
bridgeIdentifier	Unique bridge identification that includes the bridge priority value and the MAC address of port 1.
bridgeMaxAge	Configurable time period in seconds that the bridge uses to discard the stored configuration message when it is operating as the root bridge. (If the bridge is not the root bridge, it uses the value shown in the <code>maxAge</code> field instead which is assigned to it by the root bridge.) The default value is 20 seconds. The acceptable range is 6 – 40 seconds. To configure the bridge maximum age, see “bridge spanningTree stpMaxAge” later in this chapter.
designatedRoot	Identity of the root bridge. It includes the root bridge’s priority value and the MAC address of port 1 on that bridge.
forwardDelay	Time period in seconds that the bridge spends in <i>each of</i> two states — listening and learning — as assigned by the root bridge. Compare with the <code>bridgeFwdDelay</code> field.
gvrpState (3500 and 9000 L3)	Status of GARP VLAN Registration Protocol (GVRP) for the entire bridge. You configure GVRP as a bridge state as well as individual port states. To configure GVRP for the bridge, see “bridge gvrpState” later in this chapter. To configure GVRP on ports, see “bridge port gvrpState” in Chapter 10.
helloTime	Time period in seconds that elapses between the configuration messages that the bridge receives from the root bridge. Compare with the <code>bridgeHelloTime</code> field.
holdTime	Minimum delay time the bridge uses between topology change BPDUs that it sends.
ipFragmentation (3500 and 9000 L3)	Shows configuration state of the IP fragmentation option. The default setting is enabled. To configure this option, see “bridge ipFragmentation” later in this chapter.
ipxTranslation (3500 and 9000 L3)	Shows configuration state of IPX SNAP translation. The default setting is disabled. To configure this option, see “bridge ipxSnapTranslation” later in this chapter.
lowLatency	(Not available at this release)

Field	Description
maxAge	Time period in seconds that the bridge uses to discard stored configuration messages. The value is determined by the root bridge. Compare with the <code>bridgeMaxAge</code> field.
mode	Reflects that the bridge operates as a transparent bridge.
peakAddrCount	Reflects the highest number of addresses that have been counted since the last address table flush. For the current size of the address table, see the <code>addressCount</code> field.
priority	Configurable STP priority value for the bridge. The default value is 0x8000. (0x signifies that 8000 is a hexadecimal number.) The acceptable range is 0x0 – 0xffff (0 – ffff). To configure a value, see “bridge spanningTree stpPriority” later in this chapter. The bridge priority is included in the bridge identifier and is considered the most significant portion because it influences root bridge selection. A lower priority increases the odds that the bridge will become the root bridge.
rootCost	Value that reflects the total cost of the best path (lowest value) from the bridge root port to the root bridge. The value sums individual port path costs. To configure path costs for ports on the bridge, see “bridge port stpCost” in Chapter 10.
rootPort	Logical port with the best path from the bridge to the root bridge.
stpGroupAddress	Address to which the bridge listens to receive configuration messages and other STP information. To modify the STP group address, see “bridge spanningTree stpGroupAddress” later in this chapter.
stpState	Whether the Spanning Tree Protocol is enabled or disabled for the bridge. The default value is disabled for all switches except CoreBuilder 9000 modules. To configure the bridge STP state, see “bridge spanningTree stpState” later in this chapter. (STP is also configured on a port-by-port basis. See “bridge port stpState” in Chapter 10.)
timeSinceLastTopologyChange	Time elapsed (in hours, minutes, and seconds) since STP last reconfigured the network topology.
topologyChangeCount	Number of times that STP has reconfigured the network topology since you enabled STP or rebooted the system (whichever is less).
topologyChangeFlag	Whether the bridge topology is currently changing (<code>true</code>) or not changing (<code>false</code>)

**bridge
ipFragmentation**

✓ 3500
✓ 9000
9400

3900
9300

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Determines whether the Fiber Distributed Data Interface (FDDI) and Ethernet stations that are connected to your system can communicate using IP when FDDI stations transmit packets that are too large for Ethernet. IP fragmentation divides such large FDDI packets into smaller packets that can be bridged to Ethernet LANs.

Valid Minimum Abbreviation

b ipf

Options

Prompt	Description	Possible Values	[Default]
ipFragmentation value	Whether large FDDI packets can be divided into smaller packets so that they can be bridged to Ethernet	<ul style="list-style-type: none"> ■ enabled ■ disabled 	enabled

bridge
ipxSnapTranslation

✓ **3500**
 ✓ **9000**
9400

3900
9300

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Translates 802.3_RAW IPX packets to FDDI_SNAP packets when they are forwarded from Ethernet to FDDI links, and vice versa when packets are forwarded from FDDI to Ethernet.

Valid Minimum Abbreviation

b ipx

Important Consideration

- When IPX SNAP Translation is disabled, the system uses standard IEEE 802.1H bridging to translate 802.3_RAW packets to FDDI_RAW packets when they are forwarded from Ethernet to FDDI, and vice versa from FDDI to Ethernet.

Options

Prompt	Description	Possible Values	[Default]
ipx SnapTranslation	Whether the system uses IPX SNAP Translation when forwarding packets between Ethernet and FDDI links	<ul style="list-style-type: none"> ■ enabled ■ disabled 	disabled

bridge addressThreshold

✓ 3500
✓ 9000
9400

3900
9300

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Sets the reporting threshold for the number of Ethernet addresses that are known. When this threshold is reached, the system generates the SNMP trap called *addressThresholdEvent*.

Valid Minimum Abbreviation

b ad

Important Considerations

- The bridge address table size on CoreBuilder switches is 32K; that is, the bridge can store a maximum of 32768 addresses.
- The range of valid values for this parameter is between 1 and 1 plus the address table size. Setting the address threshold to the highest possible value prevents the system from generating the trap, because the value can never be reached.

Options

Prompt	Description	Possible Values	[Default]
address threshold	Threshold for the total number of addresses that are known on this bridge	1 – 32769	29491 (factory default), or current value

bridge agingTime Sets the maximum period (in seconds) for aging out (deleting) dynamic addresses from the address table.

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

b ag

- ✓ 3900
- ✓ 9300

Important Considerations

- Use this parameter to configure the system to age addresses in a timely manner, without increasing packet flooding.
- To disable the bridge aging function, set the value to 0.
- This parameter does not affect statically configured addresses.

Options

Prompt	Description	Possible Values	[Default]
aging time	Maximum period (in seconds) for aging out dynamically learned forwarding information	<ul style="list-style-type: none"> ■ 0 to disable ■ 10 – 1,000,000 seconds 	300

**bridge spanningTree
stpState**

Enables or disables the Spanning Tree Protocol (STP) on your system.

✓ 3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

b sp stps

Important Considerations

- The state of STP is configured in two places: the entire bridge (this command) and individual bridge ports. (See Chapter 10.) The combination of the states determines the forwarding behavior of each port, as shown in the following table:

Bridge STP State	Port STP State	Port Participates in STP?	Port Forwards Frames?
Disabled	Disabled	No	Yes, if link state is up.
	Enabled	No	Yes, if link state is up.
	Removed	No	Yes, if link state is up.
Enabled	Disabled	No	No
	Enabled	Yes	Determined by STP, provided that the link state is up.
	Removed	No	Yes, if link state is up.

- After you enable STP, the system takes several seconds to process the command before the Administration Console menu reappears.
- Although bridge-wide STP is initially disabled, default values exist for the following STP bridge parameters: priority, max age, hello time, forward delay, and group address. These values do not function until STP is enabled.
- CoreBuilder® 3500 and CoreBuilder 9000 Layer 3 modules include an `ignore STP mode` option. See Chapter 14 in this guide or see your system *Implementation Guide* for more information.
- Bridge-wide STP must be disabled on a CoreBuilder 9400 switch if you configure it as a MultiPoint Link Aggregation (MPLA) core switch. For more information about MPLA, see the *CoreBuilder 9400 Implementation Guide*.

Options

Prompt	Description	Possible Values	[Default]
stpState (3500, 3900, 9300, 9400)	Whether the Spanning Tree Protocol is enabled or disabled for the system	■ enabled ■ disabled	disabled (factory default), or current value
stpState (9000 L2 and L3)	Whether the Spanning Tree Protocol is enabled or disabled for the module	■ enabled ■ disabled	enabled (factory default), or current value

**bridge spanningTree
stpPriority**

Modifies the bridge priority, which influences the choice of the root and designated bridges.

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

b sp stpp

- ✓ 3900
- ✓ 9300

Important Considerations

- The bridge priority is expressed as a hexadecimal value. The characters Ox signify this.
- The lower the bridge's priority value, the more likely it is that the bridge is chosen as the root bridge or a designated bridge.
- You can change the value while STP is disabled or enabled. If you change the value while STP is disabled, the value is retained when you enable STP.

Options

Prompt	Description	Possible Values	[Default]
STP priority	Bridge-wide STP parameter	0x0 – 0xffff	0x8000 (factory default), or current value

**bridge spanningTree
stpMaxAge**

Determines when the stored CPDU configuration message is discarded from the bridge's memory if the bridge is the root bridge. The current value is shown in the bridgeMaxAge field of the `bridge display`.

- ✓ 3500
- ✓ 9000
- ✓ 9400

- ✓ 3900
- ✓ 9300

Valid Minimum Abbreviation

`b sp stpm`

Important Considerations

- If the value is too small, the STP may reconfigure the topology too often, causing temporary loss of connectivity in the network.
- If the value is too large, the network may take longer than necessary to adjust to a new STP configuration after a topology change such as the restarting of a bridge.
- A conservative value assumes a delay variance of 2 seconds per hop. The recommended and default value is 20 seconds.
- Although the possible range for stpMaxAge is 6 – 40, the available range is constrained by the following inequalities:
 - $2 \times (\text{stpForwardDelay} - 1 \text{ second}) \geq \text{stpMaxAge}$
 - $\text{stpMaxAge} \geq 2 \times (\text{stpHelloTime} + 1 \text{ second})$

Options

Prompt	Description	Possible Values	[Default]
STPmax age	Value (in seconds) when the stored configuration message information is deemed too old and is discarded	6 – 40 seconds	20 (factory default), or current value

**bridge spanningTree
stpHelloTime**

Sets the time between configuration messages that the bridge generates if it is operating as the root bridge. The current value is shown in the bridgeHelloTime field of the `bridge display`.

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

`b sp stph`

- ✓ 3900
- ✓ 9300

Important Considerations

- If the probability of losing configuration messages is high, shorten the time to make the protocol more robust.
- If the probability of losing configuration messages is low, lengthen the time to lower the overhead of the algorithm.
- The recommended Hello time is 2 seconds.
- Although the possible range for stpHelloTime is 1 – 10, the available range is constrained by the following inequality:

$$\text{stpMaxAge} \geq 2 \times (\text{stpHelloTime} + 1 \text{ second})$$

Options

Prompt	Description	Possible Values	[Default]
STP hello time	Time (in seconds) between configuration messages from the root bridge	1 – 10 seconds	2 (factory default), or current value

bridge spanningTree stpForwardDelay

- ✓ 3500
- ✓ 9000
- ✓ 9400

- ✓ 3900
- ✓ 9300

Sets the amount of time that the bridge spends in each of the listening and learning states if it is the root bridge. The current value is shown in the bridgeFwdDelay field of the `bridge display`.

Valid Minimum Abbreviation

`b sp stpf`

Important Considerations

- This value temporarily prevents a bridge from starting to forward data packets to and from a link until news of a topology change has spread to all parts of a bridged network.
- The recommended and default value is 15 seconds.
- Setting the value too low can result in temporary loops while STP reconfigures the topology.
- Setting the value too high can lead to a longer wait while STP reconfigures the topology.
- If the configuration was not successful, the system notifies you that your changes failed, and you can try to reenter the changes.
- Although the possible range for stpForwardDelay is 4 – 30, the available range is constrained by the following inequality:

$$2 \times (\text{stpForwardDelay} - 1 \text{ second}) \geq \text{stpMaxAge}$$

Options

Prompt	Description	Possible Values	[Default]
STP forward delay	Time (in seconds) that a bridge spends in the listening state and the learning state	4 – 30 seconds	15 (factory default), or current value

**bridge spanningTree
stpGroupAddress**

- ✓ 3500
- ✓ 9000
- ✓ 9400

Sets the single address to which a bridge listens to receive Spanning Tree Protocol (STP) information. Each STP bridge on the network sends STP packets to the group address. Every STP bridge on the network receives STP packets that were sent to the group address, regardless of which bridge sent the packets. The current value is shown in the stpGroupAddress field of the `bridge display`.

- ✓ 3900
- ✓ 9300

Valid Minimum Abbreviation

`b sp stpg`

Important Considerations

- Because there is no industry standard for a group address, products from different vendors may respond to different group addresses. If STP does not seem to be working in a mixed-vendor environment, other vendors' products may use different group addresses as their defaults. If that is true, set the STP group address to be the same across all bridges in the network.
- Before you can modify the STP group address, you must disable STP (if it is not already disabled) on the bridge. (See "bridge spanningTree stpState" earlier in this chapter.)

Options

Prompt	Description	Possible Values	[Default]
STP group address	Single address to which a bridge listens for STP information	A valid STP group address	01-80-C2-00-00-00 (factory default), or current value

bridge gvrpState *For CoreBuilder 9000: Applies to Layer 3 switching modules only.*

✓ 3500
✓ 9000
9400

Enables or disables the GARP VLAN Registration Protocol (GVRP), which can help simplify management of VLAN configurations in larger networks, and determines whether the virtual LAN (VLAN) origin for a port-based VLAN is dynamic (with GVRP) or static (without GVRP).

3900
9300

Valid Minimum Abbreviation

b g

Important Considerations

- To activate GVRP in your system, you first enable it for the entire bridge (this command) and then enable it on appropriate individual bridge ports (see Chapter 10).
- To maximize the effectiveness of GVRP, it should be enabled in as many end stations and network devices as possible.
- VLANs that are created dynamically with GVRP exist only as long as a GVRP-enabled device is sending updates. If the devices no longer send updates, or if GVRP is disabled, or if the system is rebooted, all dynamic VLANs are removed.
- If you disable GVRP after it has been enabled for a period of time, the system deletes all VLAN interfaces that were learned through GVRP and leaves unchanged all VLANs that were statically configured through the Administration Console or through the Web management software.

Options

Prompt	Description	Possible Values	[Default]
GVRP state	Whether the system uses GVRP for the entire bridge	<ul style="list-style-type: none"> ■ enable ■ disable 	disabled

bridge cos enable *For CoreBuilder 9000: Applies to Layer 2 switching modules only.*

3500
 ✓ 9000
 ✓ 9400

Enables or disables IEEE 802.1p Class of Service (CoS) on the bridge. Use this feature to help prioritize business-critical or time-sensitive traffic in your network.

Valid Minimum Abbreviation

b c e

✓ 3900
 ✓ 9300

Important Considerations

- The opportunity to be processed in the high priority queue exists only for IEEE 802.1Q tagged packets (provided that CoS is enabled) with priority values that match the high priority queue configuration. Non-tagged packets are always processed in the low priority queue, along with tagged packets with priority values that match the low priority queue configuration.
- CoS is enabled by default and initial queue assignments conform with IEEE 802.1p recommendations — that is, priorities 0 – 3 are assigned to the low priority queue and priorities 4 – 7 are assigned to the high priority queue. To modify queue assignments, see “bridge cos modify” later in this chapter.
- If you disable CoS, all tagged and non-tagged traffic is processed through the low priority queue and its buffers. (The high priority queue and buffers are shut off.)

Options

Prompt	Description	Possible Values	[Default]
CoS setting	Whether all bridge ports in the system implement Class of Service	<ul style="list-style-type: none"> ■ enabled ■ disabled 	enabled (factory default), or current value

bridge cos summary *For CoreBuilder 9000: Applies to Layer 2 switching modules only.*

3500
 ✓ 9000
 ✓ 9400

✓ 3900
 ✓ 9300

Displays whether Class of Service (CoS) is enabled or disabled; shows how the eight possible priority values are assigned (or, if CoS is disabled, how they were last assigned) to the two queues; and shows the rate limit that exists on the high priority queue (queue 1).

Valid Minimum Abbreviation

b c s

Important Considerations

- By default, CoS is enabled and the eight priority values (traffic classes 0 – 7) are divided between the two queues in accordance with IEEE 802.1p recommendations — that is, queue 1 (high priority) has classes 4, 5, 6, and 7 and queue 2 (low priority) has classes 0, 1, 2, and 3.
- If CoS is disabled (indicated at the top of the display), the display reflects the most recent configuration even though it is no longer active.

Options

Prompt	Description	Possible Values	[Default]
Queue index number	Number of the queue for which you want to see information	<ul style="list-style-type: none"> ■ 1 ■ 2 ■ all 	—

Fields in the Bridge CoS Summary Display

Field	Description
Queue	Number of the queue. Queue 1 is always the high priority queue. Queue 2 is always the low priority queue.
Rate limit	Percentage of traffic allowed on the high priority queue. See the <i>Implementation Guide</i> for your system for more information about the rate limit option.
Traffic classes	Priority values assigned to each queue. The IEEE 802.1p standard specifies eight possible values (0 – 7), each of which is intended to signify a certain kind of traffic.

bridge cos modify *For CoreBuilder 9000: Applies to Layer 2 switching modules only.*

3500
 ✓ 9000
 ✓ 9400

Changes how the eight priority values (0 – 7) are assigned to each of the two hardware queues and changes the optional rate limit on queue 1 (the high priority queue).

Valid Minimum Abbreviation

b c m

✓ 3900
 ✓ 9300

Important Considerations

- Because you cannot configure a rate limit for queue 2, the Administration Console prompts you to enter a rate limit only if you select queue 1.
- When you assign priority values to a given queue, the system automatically assigns the remaining priority values to the other queue.
- If CoS is disabled, you can still modify the queue settings; however, they do not affect traffic until CoS is enabled.

Options

Prompt	Description	Possible Values	[Default]
Queue index	Number of the device queue whose settings you want to modify	<ul style="list-style-type: none"> ■ 1 ■ 2 ■ ? (for a list of selectable indexes) 	–
Rate limit	Throughput limit that applies only to queue 1 and is expressed as a percentage	Whole numbers from 1 – 100	100 (factory default), or current value
Class of service tags	IEEE 802.1p priority values that you want to assign to the selected queue. Use commas to separate multiple values.	<ul style="list-style-type: none"> ■ 0 – 7 ■ all ■ ? (for a list of possible values) 	For queue 1, values 4, 5, 6, 7 (factory default), or current values For queue 2, values 0, 1, 2, 3 (factory default), or current values

**bridge multicast igmp
summary**

3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

For CoreBuilder 9000: Applies to Layer 2 switching modules only.

Displays a summary of parameters related to the Internet Group Management Protocol (IGMP) which conserves network bandwidth by directing IP multicast application traffic only to the ports that require it.

Valid Minimum Abbreviation

b mu i su

Important Consideration

- For the CoreBuilder 3500 system and CoreBuilder 9000 Layer 3 modules, IGMP commands exist under the `ip multicast igmp` menu.

Fields in the Bridge Multicast IGMP Summary Display

Field	Description
igmp snooping	Whether the IGMP snooping function is enabled or disabled for the entire system.
igmp querying	Whether the system is enabled to operate as an IGMP querier. IGMP snooping must be enabled for the querying function to operate.
igmp query source IP address	Source IP address used by the system or module in query messages if it is elected as the IGMP querier.

**bridge multicast igmp
snoopMode****For CoreBuilder 9000: Applies to Layer 2 switching modules only.**

Enables or disables the snooping (listening) function of the Internet Group Management Protocol (IGMP).

3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

b mu i sn

Important Considerations

- The value that you select applies to the entire system or module.
- IGMP snooping must be disabled on a CoreBuilder 9400 switch if you configure it as a MultiPoint Link Aggregation (MPLA) core switch. For more information about MPLA, see the *CoreBuilder 9400 Implementation Guide*.
- For the CoreBuilder 3500 system and CoreBuilder 9000 Layer 3 modules, IGMP commands exist under the `ip multicast igmp` menu.

Options

Prompt	Description	Possible Values	[Default]
IGMP snooping	Whether your system implements IGMP snooping	<ul style="list-style-type: none"> ■ enabled ■ disabled 	enabled (factory default), or current value

**bridge multicast igmp
queryMode**

3500
 ✓ 9000
 ✓ 9400

✓ 3900
 ✓ 9300

For CoreBuilder 9000: Applies to Layer 2 switching modules only.

Enables or disables the querying function of the Internet Group Management Protocol (IGMP). From all IGMP-capable devices on a given subnetwork, the one with the lowest IP address is elected as the querier.

Valid Minimum Abbreviation

b mu i querym

Important Considerations

- The value that you select applies to the entire system.
- If you enable `igmp querymode`, but disable `igmp snoopmode`, the system or module cannot operate as an IGMP querier.
- To prevent IP multicast traffic from occupying unnecessary bandwidth, the best device to operate as the querier is the one closest to the source of IP multicast traffic. You can disable querying on select devices or manipulate IP addresses with the `bridge multicast igmp queryIpAddress` command to force this configuration.
- IGMP querying must be disabled on a CoreBuilder 9400 switch if you configure it as a MultiPoint Link Aggregation (MPLA) core switch. For more information about MPLA, see the *CoreBuilder 9400 Implementation Guide*.
- For the CoreBuilder 3500 system and CoreBuilder 9000 Layer 3 modules, IGMP commands exist under the `ip multicast igmp` menu.

Options

Prompt	Description	Possible Values	[Default]
IGMP querying	Whether the system can operate as the IGMP querier if so elected	<ul style="list-style-type: none"> ■ enabled ■ disabled 	enabled (factory default), or current value

**bridge multicast igmp
queryIpAddress****For CoreBuilder 9000: Applies to Layer 2 switching modules only.**

Configures the source address that is inserted in IGMP query packets.

3500
 ✓ 9000
 ✓ 9400

Valid Minimum Abbreviation

b mu i queryi

✓ 3900
 ✓ 9300

Important Considerations

- For the CoreBuilder 9400 and SuperStack II Switch 9300 and 3900 systems, you do not need to use this command as long as you have one in-band IP interface configured; the system uses its IP address as the source IP address of query packets. Use this command only if you want the system to use a different source IP address for query packets. If there are no in-band IP interfaces configured and you want to enable querying, you must enter an IP address with this command.
- For a CoreBuilder 9000 Layer 2 switching module to offer itself as a querier, you must enter an IP address with this command.
- For the CoreBuilder 3500 system and CoreBuilder 9000 Layer 3 modules, IGMP commands exist under the `ip multicast igmp` menu.

Options

Prompt	Description	Possible Values	[Default]
IGMP Query Source IP Address	Source address that the system uses in its IGMP queries	Any unique IP address in dotted decimal format	0.0.0.0, first in-band IP interface index, or current value (3900, 9300, 9400) 0.0.0.0, or current value (9000 L2)

**bridge multicast igmp
vlans**

3500

✓ **9000**

✓ **9400**

✓ **3900**

✓ **9300**

For CoreBuilder 9000: Applies to Layer 2 switching modules only.

If IGMP snooping is enabled, lists the VLAN IDs of VLANs that are carrying IP multicast traffic.

Valid Minimum Abbreviation

`b mu i v`

Important Consideration

- For the CoreBuilder 3500 system and CoreBuilder 9000 Layer 3 modules, IGMP commands exist under the `ip multicast igmp` menu.

bridge multicast igmp groups

3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

For CoreBuilder 9000: Applies to Layer 2 switching modules only.

Displays IP multicast group and associated port information for a selected VLAN.

Valid Minimum Abbreviation

b m u i g

Important Considerations

- For the CoreBuilder 3500 system and CoreBuilder 9000 Layer 3 modules, IGMP commands exist under the `ip multicast igmp` menu.
- If no IP multicast group traffic is present on the selected VLAN, you see this message: `No groups exist for this VLAN`

Options

Prompt	Description	Possible Values	[Default]
VLAN ID	ID number of the VLAN for which you want to display group and port information	<ul style="list-style-type: none"> ■ A valid VLAN ID (VID) number ■ ? (for a list of selectable VIDs) 	1 (Default VLAN)

Fields in the Bridge Multicast IGMP Groups Display

Field	Description
VLAN ID	ID number of the selected VLAN.
Group	Hexidecimal equivalent of the IP multicast group address shown in the <code>IpAddress</code> column.
IpAddress	IP multicast group address of the traffic that the system or module has observed on the selected VLAN.
Ports	Ports that lead to group members.

**bridge multicast igmp
desQuerier**

For CoreBuilder 9000: Applies to Layer 2 switching modules only.

Determines whether the system or module is the designated querier for the selected VLAN.

3500

✓ 9000

✓ 9400

Valid Minimum Abbreviation

`b m u i d`

✓ 3900

✓ 9300

Important Considerations

- For the CoreBuilder 3500 system and CoreBuilder 9000 Layer 3 modules, IGMP commands exist under the `ip multicast igmp` menu.
- If the system or module is not functioning as the querier, you see this message: `Device IS NOT designated querier on VLAN`
- If the system or module is functioning as the querier, you see this message: `Device IS designated querier on VLAN`

Options

Prompt	Description	Possible Values	[Default]
VLAN ID	ID number of the VLAN for which you are requesting information	<ul style="list-style-type: none"> ■ A valid VLAN ID (VID) ■ ? (for a list of selectable VIDs) 	1 (Default VLAN)

**bridge multicast igmp
rPorts*****For CoreBuilder 9000: Applies to Layer 2 switching modules only.***

Lists the ports in the selected VLAN that lead to IP multicast routers.

3500
 ✓ 9000
 ✓ 9400

✓ 3900
 ✓ 9300

Valid Minimum Abbreviation

b m u i r

Important Considerations

- The system determines which ports in a VLAN lead to multicast routers by snooping on advertisements from the following routing protocols: Distance-Vector Multicast Routing Protocol (DVMRP), Multicast Open Shortest Path First (MOSPF), and Protocol Independent Multicast (PIM).
- Router port entries age out after 100 seconds. Routing protocol advertisements are usually sent every few seconds.
- For the CoreBuilder 3500 system and CoreBuilder 9000 Layer 3 modules, IGMP commands exist under the `ip multicast igmp` menu.

Options

Prompt	Description	Possible Values	[Default]
VLAN ID	ID number of the VLAN for which you want to list ports that lead to IP multicast routers	<ul style="list-style-type: none"> ■ A valid VLAN ID (VID) ■ ? (for a list of selectable VIDs) 	1 (Default VLAN)

**bridge multicast igmp
qPort****For CoreBuilder 9000: Applies to Layer 2 switching modules only.**

Displays the number of the port that receives incoming IGMP queries for the selected VLAN.

3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation`b mu i qp`**Important Considerations**

- If no query packets have been received within the last five minutes (approximately) when you enter this command, the system responds:
No queries are heard by the switch
- For the CoreBuilder 3500 system and CoreBuilder 9000 Layer 3 modules, IGMP commands exist under the `ip multicast igmp` menu.

Options

Prompt	Description	Possible Values	[Default]
VLAN ID	ID number of the VLAN for which you want to display the port that last received query packets	<ul style="list-style-type: none"> ■ A valid VLAN ID (VID) ■ ? (for a list of selectable VIDs) 	1 (Default VLAN)

BRIDGE PORT PARAMETERS

This chapter provides guidelines and other key information about how to manage bridge ports in your system.



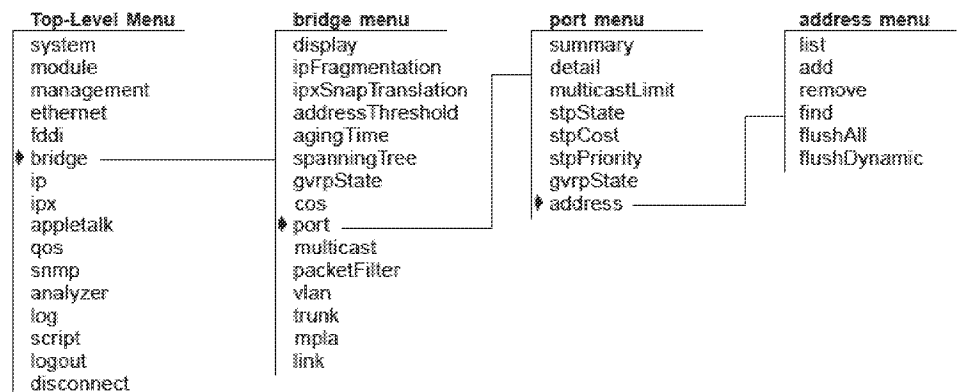
This chapter covers bridge port options only. For information about other bridge menu options, use the Table of Contents to find the appropriate chapter in this Command Reference Guide.



For more information about configuring bridge ports in your network, see the Implementation Guide for your system.

Menu Structure

The commands that you can use depend on the system that you have, your level of access, and the types of modules and other hardware options that are configured for your system. The following diagram shows the complete list of commands for all systems. See the checklist at the beginning of each command description in this chapter for whether your system supports the command.



bridge port summary

Displays a summary of bridge port information, including the Spanning Tree Protocol (STP) configurations for selected bridge ports.

✓ 3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

b po su

Important Considerations

- The port numbering that is displayed is always sequential, although it depends on the placement of the modules that you have configured into your system. See the *Implementation Guide* for your system for more information about port numbering.
- For resilient links, the main and standby ports are shown in ascending order.
- When you are prompted to select ports, you can enter ? to see a matrix of information about the bridge ports. This matrix is useful, for example, if you have trunks configured but forget which port is the anchor port. You must use the anchor port number to display a port summary for a trunk.

Fields in the Bridge Port Summary Display

Field	Description
fwdTransitions	Number of times that the port has entered the forwarding state since you enabled STP or rebooted the system. This value is useful for determining the relative stability of the topology.
gvrpState (3500, 9000 L3)	Whether GARP VLAN Registration Protocol (GARP) is enabled or disabled on the port. For GVRP to function on the port, you must enable it on the port as well as the entire bridge. To configure GVRP on a port, see "bridge port gvrpState" later in this chapter. To configure GVRP on the bridge, see "bridge gvrpState" in Chapter 9.
linkState	State of the link (up or down), that is, whether it is available for communication.
portId	Port identification, which includes the port priority value (first 2 digits after "0x") and the logical port number (last 2 digits). Both are shown as hexadecimal values.

Field	Description
portNumber	Logical index number that the system assigns to the bridge port, which may not correspond with the physical port number depending on your system configuration. (For example, when you define a trunk, only the anchor port receives a portNumber.) As you add and remove logical ports, portNumbers are reassigned so that they remain consecutive.
rxDiscards	Total number of frames received on the bridge port that have been discarded. This value reflects a summary of all statistics that end with <code>Discs</code> , <code>Discards</code> , or <code>Filters</code> .
rxFrames	Total number of frames that this bridge port received from its segment. However, unlike the <code>rxFrames</code> field in the Ethernet display which counts all frames, this field does not count frames in error. Thus, this value may be lower than the value shown in the <code>rxFrames</code> field in the Ethernet display.
state	Current operating state of the port: <ul style="list-style-type: none">■ Blocking — The bridge continues to run STP on the port, but the bridge does not receive packets from the port, learn locations of station addresses from it, or forward packets onto it.■ Listening — The bridge continues to run STP and to transmit configuration messages on the port, but it discards packets that are received on the port and does not transmit packets that are forwarded to the port.■ Learning — STP operating state in which the bridge receives packets on the port to learn the location of some of the stations that are located on the port.■ Forwarding — The bridge receives packets on the port and forwards or does not forward them, depending on address comparisons with the bridge's source address list. Provided that the link state is up, this <code>state</code> field indicates <code>forwarding</code> even if STP is disabled for the bridge.■ Disabled — Management has disabled the port or the link state is down.

Field	Description
stp	<p>Configurable status of STP on a port. If bridge-wide STP is enabled, the port STP configuration options are:</p> <ul style="list-style-type: none">■ <code>enabled</code> — STP sets the operating state of the port (blocking, listening, etc.) according to network topology characteristics. This is the default configuration for all ports.■ <code>disabled</code> — STP is disabled and the port is disabled. The port does not participate in STP decisions, frame reception, or frame transmission.■ <code>removed</code> — STP is disabled on the port but the port can still receive or transmit frames if its link state is up. <p>If bridge-wide STP is disabled, the port STP setting has no effect; as long as its link state is up, the port forwards all valid frames. To see a matrix of port and bridge STP settings, see "bridge port stpState" in this chapter.</p>
txFrames	<p>Number of frames that this port has transmitted. This object counts a frame transmitted on the interface that corresponds to this port only if the frame is for a protocol that the local bridging function is processing (includes bridge management frames).</p>

bridge port detail Displays detailed information about bridge ports, including the Spanning Tree Protocol (STP) configurations for the bridge port.

✓ 3500
✓ 9000
✓ 9400

Valid Minimum Abbreviation

b po d

✓ 3900
✓ 9300

Important Considerations

- The port numbering that is displayed for your ports is always sequential, although it depends on the placement of the modules that you have configured into your system. See the *Implementation Guide* for your system for more information about port numbering.
- For resilient links, the main and standby ports are shown in ascending order.
- When you are prompted to select ports, specify the ? option to see a list of information about your bridge ports. This matrix is useful, for example, if you have trunks configured but forget which port is the anchor port. You must use the anchor port number to display a port summary for a trunk.

Fields in the Bridge Port Detail Display

Field	Description
designatedBridge	Identity of the designated bridge of the LAN to which the port is attached. It is an STP port parameter.
designatedCost	Cost through this port to get to the root bridge. The designated cost of the root port is the same as the cost that is received in incoming BPDUs from the designated bridge for that LAN. It is an STP port parameter.
designatedPort	Identity of the designated port on the designated bridge.
designatedRoot	Identity of the root bridge in the LAN, which includes the root bridge's priority value and the MAC address of port 1 on that bridge.
fwdTransitions	Number of times that the port has entered the forwarding state since you enabled STP or rebooted the system. This value is useful for determining the relative stability of the topology.
gvrpState (3500, 9000 L3)	Whether the GARP VLAN Registration Protocol (GVRP) is enabled or disabled on the port. For GVRP to function on the port, you must enable it on the port as well as the entire bridge. To configure GVRP on a port, see "bridge port gvrpState" in this chapter. To configure GVRP on the bridge, see "bridge gvrpState" in Chapter 9.

Field	Description
linkState	State of the link (up or down), that is, whether it is available for communication.
pathCost	Cost to add to the total path cost when this port is the root port. To configure a port's STP cost, see "bridge port stpCost" in this chapter.
portNumber	Logical index number that the system assigns to the bridge port, which may not correspond with the physical port number depending on your system configuration. (For example, when you define a trunk, only the anchor port receives a portNumber.) As you add and remove logical ports, portNumbers are reassigned so that they remain consecutive.
portId	Port identification, which includes the port priority value (first 2 digits after "0x") and the logical port number (last 2 digits). Both are shown as hexadecimal values.
priority	Configurable STP port priority value. The default value is 0x80. (0x signifies that the value to follow is a hexadecimal number.) The acceptable range is 0x0 – 0xff. To configure port priority values, see "bridge port stpPriority" in this chapter. The port priority is included in the port ID and is considered the most significant portion because it is the first factor that determines if a port is to be the designated port when more than one bridge port is attached to the same LAN. The lowest priority is chosen. If all ports in a bridge have the same priority, then the port number is used as the determining factor.
rxAllFilters (3500 and 9000 L3)	Number of frames that the bridge port discarded due to a user-defined packet filter on its "receive all" path.
rxBlockedDiscs (3500 and 9000 L3)	Number of frames that the bridge port discarded because the receiving bridge port was not in the forwarding state.
rxErrorDiscs	Number of frames that the bridge port discarded because of internal bridge system errors (such as hardware and software address table discrepancies).
rxForwards (3500 and 9000 L3)	Total number of frames (all types) that the bridge port received and forwarded to another bridge port.
rxForwardMcasts (3900, 9300, 9400, and 9000 L2)	Number of multicast frames that the bridge port received and forwarded to another bridge port.
rxForwardUcasts (3900, 9300, 9400, and 9000 L2)	Number of unicast frames the bridge port received and forwarded to another bridge port.
rxFloodUcasts	Number of unicast frames that the port received and flooded to one or more ports.

Field	Description
rxFrames	Total number of frames that this bridge port received from its segment. However, unlike the rxFrames field in the Ethernet display which counts all frames, this field does not count frames in error. Thus, this value may be lower than the value shown in the rxFrames field in the Ethernet display.
rxInternalFilters (3500 and 9000 L3)	Number of frames discarded due to customer filters on the rxInternal path.
rxMcastExcDiscs	Number of multicast frames that were discarded when rxMcastLimit was exceeded.
rxMcastExceeds	Amount of time that rxMcastLimit has been exceeded.
rxMcastFilters (3500 and 9000 L3)	Number of frames that were discarded due to a user-defined packet filter on the "receive multicast" path of this port.
rxMcastLimit	Configurable parameter that limits the rate of multicast frames that are forwarded from a bridge port. The default value is 0, which means there is no limit. To configure this option, see "bridge port multicastLimit" in this chapter.
rxMcastLimitType (3900, 9300, 9400, and 9000 L2)	Configurable parameter that selects the type of frames on which the multicast limit operates (both multicast and broadcast frames, or broadcast frames only). The default value is McastBcast. To configure this option, see "bridge port multicastLimit" in this chapter.
rxNoDestDiscs (3900, 9300, 9400, and 9000 L2)	Number of frames that this port discarded because of an unknown VLAN ID or because the port was in a non-forwarding Spanning Tree state.
rxNoRescrDiscs (3500 and 9000 L3)	Number of frames that this port discarded due to insufficient resource availability (buffer space).
rxOtherDiscs (3900, 9300, 9400, 9000 L2, 9000 L3)	Number of frames that this port discarded because they contained either invalid (group) source addresses or source addresses that belong to this bridge (indicates network loops).
rxOtherDiscards (3500)	Number of frames that this port discarded because they contained either invalid MAC source addresses or source addresses that belong to this bridge.
rxSameSegDiscs	Number of frames that this port discarded because the destination address is known on the same network segment as the source address and, thus, the frame does not need to be bridged.
rxSecurityDiscs	Number of frames that this port discarded because they contained source addresses that were statically configured on another bridge port.
SRRingNumber (3500 and 9000 L3)	(Not available at this release)

Field	Description
SRHopLimit (3500 and 9000 L3)	(Not available at this release)
state	<p>Current operating state of the port:</p> <ul style="list-style-type: none"> ■ Blocking — The bridge continues to run STP on the port, but the bridge does not receive packets from the port, learn locations of station addresses from it, or forward packets onto it. ■ Listening — The bridge continues to run STP and to transmit configuration messages on the port, but it discards packets that are received on the port and does not transmit packets that are forwarded to the port. ■ Learning — Similar to listening, but the bridge receives packets on the port to learn the location of some of the stations that are located on the port. ■ Forwarding — The bridge receives packets on the port and forwards or does not forward them, depending on address comparisons with the bridge's source address list. Provided that the link state is up, this <code>state</code> field indicates <code>forwarding</code> even if STP is disabled for the bridge. ■ Disabled — Management has disabled the port or the link state is <code>down</code>.
stp	<p>Configurable status of STP on a port. Provided that bridge-wide STP is enabled, the port STP configuration states function as follows:</p> <ul style="list-style-type: none"> ■ enabled — STP sets the operating state of the port (<code>blocking</code>, <code>listening</code>, etc.) according to network topology characteristics. This is the default configuration for all ports. ■ disabled — STP is disabled and the port is disabled. The port does not participate in STP decisions, frame reception, or frame transmission. ■ removed — STP is disabled on the port but the port can still receive or transmit frames if its link state is up. <p>If bridge-wide STP is disabled, this port STP setting is meaningless; as long as its link state is up, the port forwards all frames. To configure STP on a port, see "bridge port stpState" in this chapter.</p>
txAllFilters (3500 and 9000 L3)	Number of frames that the bridge port discarded because of a user-defined packet filter on its "transmit all" path.
txBlockedDiscs (3500 and 9000 L3)	Number of frames that this bridge port discarded because the transmitting bridge port was not in the forwarding state.

Field	Description
txFrames	Number of frames that this port transmitted to its segment. This object counts a frame transmitted on the interface that corresponds to this port only if the frame is for a protocol that the local bridging function is processing (includes bridge management frames).
txMcastFilters (3500 and 9000 L3)	Number of frames that this port discarded because of a user-defined packet filter on its "transmit multicast" path.
txMtuExcDiscs (3500 and 9000 L3)	Number of frames that this port discarded because of excessive size.

**bridge port
multicastLimit**

Sets a threshold value on a bridge port that affects the per-second forwarding rate of multicast or broadcast traffic that originates on the segment connected to that port.

- ✓ 3500
- ✓ 9000
- ✓ 9400

- ✓ 3900
- ✓ 9300

Valid Minimum Abbreviation

b p o m

Important Considerations

- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.
- A value of zero indicates that no limit is configured.
- If you want to configure a limit for a trunk, be sure to apply it to the trunk's anchor port (lowest-numbered port) only. However, be aware that the limit that you specify applies separately to *each link* in the trunk, even though you only enter it once — that is, it is not an aggregate.
- For a larger array of similar options in the CoreBuilder 3500 and 9000 Layer 3 modules, see the Quality of Service (QoS) chapter in this guide (Chapter 22) and in the appropriate *Implementation Guide*.

Options

Prompt	Description	Possible Values	[Default]
Bridge ports	Bridge ports for which you want to set the multicastLimit	One or more valid bridge port numbers	—
Frame type (3900, 9300, 9400, 9000 L2)	Frame type to which the limit shall apply	<ul style="list-style-type: none"> ■ BcastOnly (broadcasts only) ■ McastBcast (multicasts and broadcasts) 	McastBcast
Multicast threshold value	Configurable parameter that limits the per-second receive rate of specified traffic.	<ul style="list-style-type: none"> ■ 0 – 200 (K frames/sec) (3500 and 9000 L3) ■ 0 – 200000 (frames/sec) (3900, 9300, 9400, and 9000 L2) 	0

bridge port stpState

Sets the Spanning Tree Protocol (STP) state for one or more bridge ports. The selection is effective only if STP is enabled for the system or module.

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

b po stps

- ✓ 3900
- ✓ 9300

Important Considerations

- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.
- The following table explains the forwarding behavior of a port based on its bridge and port STP states:

Bridge STP State	Port STP State	Port Participates in STP?	Port Forwards Frames?
Disabled	Disabled	No	Yes, if link state is up.
	Enabled	No	Yes, if link state is up.
	Removed	No	Yes, if link state is up.
Enabled	Disabled	No	No
	Enabled	Yes	Determined by STP, provided that the port link state is up.
	Removed	No	Yes, if link state is up.

Options

Prompt	Description	Possible Values	[Default]
Ports	Ports for which you want to control the STP setting	<ul style="list-style-type: none"> ■ One or more valid port numbers ■ ? (to display a port summary) 	–
STP state	Spanning Tree Protocol state that you assign to specified ports	<ul style="list-style-type: none"> ■ enabled ■ disabled ■ removed 	enabled (factory default), or current value

bridge port stpCost

- ✓ 3500
- ✓ 9000
- ✓ 9400

Sets the path cost that the Spanning Tree Protocol (STP) adds to the root cost field in a configuration message that the port receives. The system uses this value to determine the path cost to the root through the port. The current value is shown in the `pathCost` field of the `bridge port detail` display.

- ✓ 3900
- ✓ 9300

Valid Minimum Abbreviation

```
b po stpc
```

Important Considerations

- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.
- A larger path cost value makes the LAN that is reached through the port more likely to be low in the Spanning Tree topology. The lower the LAN is in the topology, the less through traffic it carries. For this reason, you may want to assign a large path cost to a LAN that has a lower bandwidth or to one on which you want to minimize traffic.
- If your configuration is successful, the previous menu appears. If the configuration is not successful, the system notifies you that your changes failed, and you can try to reenter your changes.
- See the *IEEE 802.1D MAC Bridges* standard for recommended path cost settings.

Options

Prompt	Description	Possible Values	[Default]
Bridge ports	Bridge ports for which you want to set the path cost	One or more valid bridge port numbers	–
STP cost	Configurable bridge port STP parameter that specifies the cost to add to the total path cost when this port is the root port	1 – 65535	<ul style="list-style-type: none"> ■ 100 (Ethernet) ■ 10 (Fast Ethernet) ■ 1 (Gigabit Ethernet)

**bridge port
stpPriority**

- ✓ 3500
- ✓ 9000
- ✓ 9400

- ✓ 3900
- ✓ 9300

Sets the Spanning Tree Protocol (STP) bridge port priority. This value influences the choice of port when the bridge has two or more ports that have the same path cost and that are connected to the same LAN, which creates a loop. STP selects the bridge port with the lowest priority and places the remaining ports in the blocking state. The current value is shown in the priority field of the `bridge port detail` display.

Valid Minimum Abbreviation

`b po stpp`

Important Considerations

- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.
- Port priority is a 1-octet value written in hexadecimal format.
- If all ports in a bridge have the same priority value, then the port number is used as the determining factor.
- If your configuration is successful, the previous menu appears. If the configuration is not successful, the system notifies you that your changes failed, and you can try to reenter your changes.

Options

Prompt	Description	Possible Values	[Default]
Bridge ports	Bridge ports for which you want to set the STP port priority	A valid bridge port number	—
STP priority	One-octet value that determines which port is the designated port when there is more than one port attached to the same LAN	0x0 – 0xff, where 0x precedes a hexadecimal value	0x80

bridge port gvrpState *For CoreBuilder 9000: Applies to Layer 3 switching modules only.*

✓ 3500
✓ 9000
9400

Allows the port to participate in sending and receiving GARP VLAN Registration Protocol (GVRP) updates, which can help you simplify the management of IEEE 802.1Q VLAN configurations.

Valid Minimum Abbreviation

b p o g

3900
9300

Important Considerations

- You can use this command to configure the same setting on multiple ports simultaneously. When you specify multiple port numbers, the system prompts you to choose the setting and then applies it to all of the ports.
- To activate GVRP in your system, you must enable it for the entire bridge (see “bridge gvrpState” in Chapter 9) as well as on individual bridge ports (this command). If you enable GVRP on a port but you have not enabled it for the bridge, GVRP does not function.
- To maximize the effectiveness of GVRP, it should be enabled in as many end stations and network devices as possible.
- GVRP updates are not sent to any blocked Spanning Tree Protocol (STP) ports. GVRP operates only on ports that are in the forwarding state.
- If GVRP is enabled on the bridge and on a given port which changes to the STP forwarding state, the port automatically begins to participate in GVRP.
- VLANs that are created dynamically with GVRP exist only as long as a GVRP-enabled device is sending updates — if the devices no longer send updates, GVRP is disabled, or the system is rebooted, all dynamic VLANs are removed, but the system leaves unchanged all VLANs that were statically configured through a management interface.

Options

Prompt	Description	Possible Values	[Default]
Bridge ports	Bridge ports for which you wish to enable or disable the GVRP state	<ul style="list-style-type: none"> ■ enable ■ disable 	disable

bridge port address list

Displays the MAC addresses (canonical addresses) that are currently associated with selected bridge ports, as well as the address type (static or dynamic).

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

b p o a l

- ✓ 3900
- ✓ 9300

Important Consideration

- If you have multiple ports that are associated with a trunk, the display groups ports that are associated with a trunk on one line (for example, 3, 4, 6) and lists the addresses that are associated with the trunk.

Options

Prompt	Description	Possible Values	[Default]
VLAN interface indexes (only if in allClosed mode)	Index numbers of the VLANs to which the desired bridge ports belong	<ul style="list-style-type: none"> ■ One or more valid VLAN indexes ■ all ■ ? (for a list of selectable VLANs) 	—
Bridge ports	Bridge ports for which you want to display MAC addresses	<ul style="list-style-type: none"> ■ One or more valid bridge port numbers ■ all ■ ? (to display a port summary) 	—

bridge port address add Adds new MAC addresses to the selected bridge ports as statically configured addresses.

✓ 3500
✓ 9000
✓ 9400

Valid Minimum Abbreviation

b p o a a

Important Considerations

- If you have multiple ports that are associated with a trunk, the display groups ports that are associated with a trunk on one line (for example, 3, 4, 6) and lists the addresses that are associated with the trunk.
- A statically configured address is never aged out of the address table and cannot be learned on a different port. You must first remove it from its former port.

Options

Prompt	Description	Possible Values	[Default]
VLAN interface indexes (only if in allClosed mode)	Index numbers of the VLANs to which the desired bridge ports belong	<ul style="list-style-type: none"> ■ One or more valid VLAN indexes ■ all ■ ? (for a list of selectable VLANs) 	–
Bridge ports	Bridge ports to which you want to add certain MAC addresses	<ul style="list-style-type: none"> ■ One or more valid bridge port numbers ■ ? (to display a port summary) 	–
MAC address	MAC address that you want to add to the selected port	A valid MAC address	–

**bridge port address
remove**

Removes individual MAC addresses from the address table.

✓ 3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

b po a r

Important Consideration

- This command is typically used to remove only static MAC addresses, because the bridge could relearn a dynamic MAC address shortly after you remove it.

Options

Prompt	Description	Possible Values	[Default]
VLAN interface indexes (only if in allClosed mode)	Index numbers of the VLANs to which the desired bridge ports belong	<ul style="list-style-type: none"> ■ One or more valid VLAN indexes ■ all ■ ? (for a list of selectable VLANs) 	–
MAC address	MAC address that you want to remove	A valid MAC address	–

bridge port address find Displays the bridge port (as well as the vlan index number if the system is in allClosed mode) that is associated with a specified MAC address.

✓ 3500

✓ 9000

✓ 9400

Valid Minimum Abbreviation

b po a fi

Options

✓ 3900

✓ 9300

Prompt	Description	Possible Values	[Default]
MAC address	MAC address (canonical address) that you want to find on the system	A valid MAC address	–

**bridge port address
flushAll**

Removes all static and dynamic MAC addresses from the bridge ports that you select. Static MAC addresses are those that you specified using the `bridge port address add` option. Dynamic MAC addresses are those that the bridge learned automatically.

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

b po a flushA

- ✓ 3900
- ✓ 9300

Important Consideration

- If the bridge is power cycled, reset, or rebooted, the address table is automatically flushed.

Options

Prompt	Description	Possible Values	[Default]
VLAN interface indexes (only if in allClosed mode)	Index numbers of the VLANs to which the desired bridge ports belong	<ul style="list-style-type: none"> ■ One or more valid VLAN indexes ■ all ■ ? (for a list of selectable VLANs) 	—
Bridge ports	Bridge ports for which you want to remove all addresses	<ul style="list-style-type: none"> ■ One or more valid bridge port numbers ■ ? (to display a port summary) 	—

bridge port address flushDynamic

Removes all dynamic MAC addresses from the bridge ports that you select. Dynamic MAC addresses are those that the bridge learned by receiving and processing packets.

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

b po a flushd

- ✓ 3900
- ✓ 9300

Important Consideration

- If the bridge is power cycled, reset, or rebooted, the address table is automatically flushed.

Options

Prompt	Description	Possible Values	[Default]
VLAN interface indexes (only if in allClosed mode)	Index numbers of the VLANs to which the desired bridge ports belong	<ul style="list-style-type: none"> ■ One or more valid VLAN indexes ■ all ■ ? (for a list of selectable VLANs) 	–
Bridge ports	Bridge ports for which you want to remove all addresses	<ul style="list-style-type: none"> ■ One or more valid bridge port numbers ■ ? (to display a port summary) 	–

11

TRUNKS

You can configure a system to aggregate multiple network links into a single *trunk*. With trunking you can create high-speed point-to-point or multipoint connections without changing or replacing existing cabling. In addition, trunking provides automatic point-to-point redundancy between two devices. Redundant links normally have one link disabled by Spanning Tree (to prevent looping); trunking utilizes both links.

This chapter provides guidelines and other key information about how to configure trunking in your system.

The system treats trunked bridge ports in the same way that it treats normal individual bridge ports. Also, all higher-level network functions — including Spanning Tree algorithms, virtual LANs (VLANs), and Simple Network Management Protocol (SNMP) management — do not distinguish a trunk from any other network port. Unlike for any other network port, the system automatically distributes traffic across the ports that are associated with a trunk. If any of the trunk's ports go down or up, the system automatically redistributes traffic across the new arrangement of operational ports.



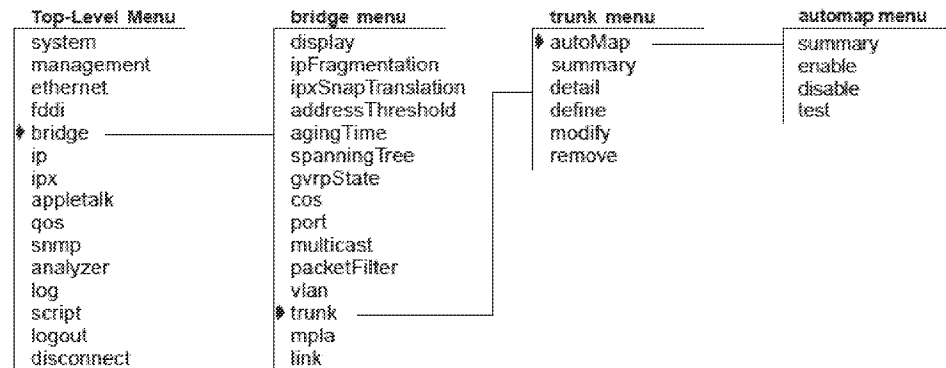
For more trunking information, see the Implementation Guide for your system.



Trunks can work with MultiPoint Link Aggregation (MPLA). MPLA is a feature for the CoreBuilder® 9400 that increases the capacity and availability of campus LAN cores without using complex, meshed router networks. Functioning at Layer 2, MPLA provides both dual-homed link resiliency and automatic load sharing over point-to-multipoint backbone connections. MPLA increases network availability using scalable Gigabit Ethernet connections among multiple campus switches. For more information about MPLA and trunking, see the CoreBuilder 9400 Implementation Guide.

Menu Structure

The commands that you can use depend on the system that you have, your level of access, and the types of modules and other hardware options that are configured for your system. The following diagram shows the complete list of commands for all systems. See the checklist at the beginning of each command description in this chapter for whether your system supports the command.



**bridge trunk
autoMap summary**

Displays a list of slot numbers that have been selected to support automatic backplane trunking.

3500

✓ 9000

9400

3900

9300

Valid Minimum Abbreviation

b t a

Important Considerations

- Automatic backplane trunking is supported only through the switch fabric modules and managed interface modules.
- The Gigabit Ethernet (GEN) Switch Fabric Module (Model Number 3CB9FG24T) has 24 non-blocking Gigabit Ethernet ports that connect to the chassis backplane to provide high-speed, low-latency connectivity between CoreBuilder 9000 interface modules.
- The GEN Switch Fabric Module supports port trunking for 12 groups, with up to six ports in a group.

Fields in the Bridge Trunk autoMap Summary Display

Field	Description
Slot number	Port numbers selected to be in the trunk.
AutoMap status	Whether the autoMap on the slot is enabled or disabled

**bridge trunk
autoMap
enable/disable**

3500

✓ 9000

9400

3900

9300

Dynamic backplane trunking provides automatic backplane trunking on the switch fabric modules and managed interface modules.

Valid Minimum Abbreviation

b t a e

Important Considerations

- You can enable or disable the autoMap function on slots.
- All trunking is performed through the switch fabric module.
- Do not perform backplane trunking through the interface modules.
- When you enable autoMap on a module in a specific slot, the switch fabric module verifies that the switch fabric module and the interface module's backplane configuration support dynamic backplane mapping.
- When you disable autoMap on a module in a specific slot, the switch fabric module verifies that the interface module's backplane configuration is compatible with that of the switch fabric module's backplane.

Options

Prompt	Description	Possible Values	[Default]
Slot number	Slot number to choose to enable or disable autoMap function	One slot number	–

**bridge trunk
autoMap test**

Indicates what happens when you do a reset on the switch fabric module when autoMap is enabled.

3500

✓ 9000

9400

3900

9300

Valid Minimum Abbreviation

b t a t

Important Consideration

- After you enable or disable a module for automatic backplane trunking, the switch fabric module verifies that the interface module's backplane configuration is compatible or not compatible to the switch fabric's configuration.

- If autoMap is enabled on the desired interface module, then the switch fabric module verifies that the switch fabric and interface module's backplane configuration satisfies the requirements of automatic backplane trunking. If the switch fabric module and interface module satisfy requirements, then no reset is required. If not, then the switch fabric module determines if the interface module must reconfigure to support backplane configuration requirements. If the switch fabric module or interface module must reconfigure, then a message is sent to the user that a reset is required:

```
Fabric reset required for trunk configuration to be
effective for the module in slot x.
```

- If autoMap is disabled, the switch fabric module verifies that the interface module's backplane configuration is compatible to the switch fabric's configuration. If the interface module is compatible to the switch fabric module's backplane configuration, then no reset is required. If not, then the switch fabric module determines if the interface module can support the defined switch fabric module's backplane configuration.

If the interface module can, then a message is sent to the interface module with the desired backplane port configuration. Otherwise, the switch fabric module will modify its configuration and a message is sent to the user that a reset is required:

```
Fabric reset required for trunk configuration to be
effective for the module in slot x.
```

**bridge trunk
summary**

- ✓ 3500
- ✓ 9000
- ✓ 9400

- ✓ 3900
- ✓ 9300

Displays summary information about configured trunks on your system. In a summary report, the system displays the trunk name and index number, the ports defined in that trunk, whether the Trunk Control Message Protocol (TCMP) is enabled or disabled, and whether the port link is up or down.

Valid Minimum Abbreviation

b t s

Fields in the Bridge Trunk Summary Display

Field	Description
Index	Identifying number that the system assigned to the trunk. You can select all or one trunk.
Name	Trunk name that you defined.
Ports	Port numbers in the trunk.
State	Whether the trunk is up or down
TCMP	Whether the Trunk Control Message Protocol (TCMP) is enabled or disabled.

bridge trunk detail Displays detailed trunk information in addition to the summary information.

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

b t det

- ✓ 3900
- ✓ 9300

Fields in the Bridge Trunk Detail Display

Field	Description
FlowC	For Gigabit Ethernet trunks, the flow control setting (on, off, rxOn, txOn). For other media types, the field contains n/a to indicate that flow control does not apply.
Index	Identifying number for the system or module that the system assigned to the trunk.
Missing	Number of ports that are configured for the trunk, but are missing because an interface module is inaccessible.
Mode	Operating mode: 100half or 100full for Fast Ethernet and 1000full for Gigabit Ethernet.
Name	Trunk name that you defined.
Node trunk id	TCMP identifier that the system assigned to the trunk.
Node trunk id list	Node trunk identifications that each port has detected on the trunk.
Ports	Ports in the trunk. The second half of the display lists each individual port in each trunk.
Present	Number of ports that participate in the trunk.
rxBadType	Number of TCMP messages received that contain a bad TCMP Type field.
rxBadVersion	Number of TCMP messages received that contain a bad TCMP version number.
rxFrames	Number of TCMP messages that were received on each port.
rxHellos	Number of TCMP helloMessages that were received on each port.
rxOverflow	Number of times that TCMP has detected a TCMP trunk configuration that exceeds the eight-node maximum.
rxSameTrunkid	Number of times that TCMP has received a helloMessage that contains the TCMP agent's own Node trunk id (an illegal configuration).
Selected node trunk id list	Node trunk identifications that are selected for use on the trunk.
State	Whether the trunk is up or down.

Field	Description
TCMP	Whether TCMP is <i>enabled</i> or <i>disabled</i> for the trunk.
Tcmpstate	TCMP state for each port in the trunk: <ul style="list-style-type: none">■ <i>not InUse</i> — Not selected for use in the trunk■ <i>selected</i> — Selected for use in the trunk, but not yet active in the trunk■ <i>inUse</i> — Active in the trunk
Trunk state	State (<i>up</i> or <i>down</i>) of each port link in the trunk.
txFrames	Number of TCMP messages that were transmitted on each port.
txHellos	Number of TCMP helloMessages that were transmitted on each port.
Type	The network type that you assigned to the ports in the trunk (for example, <i>FDDI</i> , <i>Fast_Ethernet</i> , or <i>Gigabit_Ethernet</i>).

bridge trunk define

Defines one or more trunks on the system. When you define a trunk, you specify ports and characteristics for the trunk.

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

b t def

- ✓ 3900
- ✓ 9300

Important Considerations

- If you have more than one media type on your system (for example, Fiber Distributed Data Interface (FDDI), Fast Ethernet, and Gigabit Ethernet), you are prompted for a media type before you are prompted for the trunk information.
- All links to be trunked must be homogeneous. For example, you cannot mix Fast Ethernet and Gigabit Ethernet links in a trunk.
- If you have already defined other trunks on your system, you cannot select ports that are part of an existing trunk.
- In general, create trunks before you define your virtual LANs (VLANs). If you create a trunk whose ports are part of existing VLANs, the VLAN bridge port configuration changes. For example, if you have the default VLAN as well as IP VLANs and you then define a trunk with ports in one of the IP VLANs, the system removes those ports from that VLAN and places them in the default VLAN. You must modify the VLAN and add the new bridge ports to the appropriate VLAN. This situation does not apply if you have only the default VLAN (all ports are part of the default VLAN).
- When you define a VLAN to include trunk ports, specify the anchor port (lowest-numbered port) that is associated with the trunk.
- Do not use Gigabit Ethernet (GEN) Interface modules (such as the 2-port 1000BASE-SX Gigabit Ethernet (GEN) Interface Module) when defining trunks.
- Enter ? to see the port summary (for example, to indicate whether there are ports associated with FDDI Dual Attach Station (DAS) pairs), and then enter the appropriate port numbers. To specify an FDDI DAS pair, specify the lowest-numbered port in the DAS pair.
- The number of trunk groups and the number of ports within a trunk group depend on your system. See the Options table.

The 3CB9FG24T switch fabric module supports up to 12 trunk groups on the CoreBuilder 9000.

- If you are working with Gigabit Ethernet modules in a SuperStack II Switch, keep in mind that each Gigabit Ethernet module uses an internal trunk resource towards the limit of four. You can trunk Gigabit Ethernet modules together (each with one port) to consolidate the Gigabit trunk resources. If you have four trunks defined and you add a Gigabit Ethernet module to the system, after a boot, the system reports that the configuration is incompatible. You must delete one of the existing trunks.
- You must reboot the module at the end of the trunk definition process. (You can define multiple trunks in one `bridge trunk define` operation.) On the CoreBuilder® 9000, rebooting a module returns you to the EME prompt, which requires you to reconnect to the module.
- The following considerations apply to the trunk clustering function, MultiPoint Link Aggregation (MPLA), in the CoreBuilder 9400 system:
 - When you configure a new switch, define multipoint aggregated links and reboot the system before you define other trunks and VLANs on the switch.
 - On a reboot, existing trunks and VLANs are deleted, and the default VLAN is restored. Trunked ports that were part of a VLAN before reboot are moved to the default VLAN. You must then redefine trunks or VLANs that you want to continue to use. See Chapter 11.

Options

Prompt	Description	Possible Values	[Default]
Mac type (if you have more than one)	Media type for the trunk.	Depends on your configuration: <ul style="list-style-type: none"> ■ FDDI ■ Fast_Ethernet ■ Gigabit_Ethernet ■ 10/100BASE-TX ■ 100BASE-FX ■ 1000BASE-SX ■ ? (for a list of selectable media types) 	–

Prompt	Description	Possible Values	[Default]
Ports	Total number of the bridge ports that you want to be part of the trunk.	<p>9000:</p> <ul style="list-style-type: none"> ■ Layer 2 modules support up to 4 trunk groups with up to 6 ports per trunk ■ Layer 3 modules support up to 3 trunk groups with up to 6 ports per trunk <p><i>The 6-port SAS (3-port DAS) FDDI Layer 3 supports 3 trunk groups. In SAS mode the trunks can contain up to 6 ports. In DAS mode, the trunks can contain up to 3 ports.</i></p> <ul style="list-style-type: none"> ■ The FGA24 switch fabric module supports up to 4 trunk groups with up to 6 ports per trunk and the FGA24T and GA9 switch fabric modules support up to 12 trunk groups with up to 6 ports per trunk <p><i>(The GA9 cannot support 12 trunk groups because there are not enough ports on this module.)</i></p> <p>3500:</p> <ul style="list-style-type: none"> ■ Supports up to 4 trunk groups with up to 8 ports per trunk <p>3900:</p> <ul style="list-style-type: none"> ■ Supports up to 4 trunk groups with up to 6 ports per trunk <p>9300 and 9400:</p> <ul style="list-style-type: none"> ■ Supports up to 12 trunk groups with up to 6 ports per trunk ■ all ■ ? (for a list of selectable ports) 	–

Prompt	Description	Possible Values	[Default]
Mode	Operating mode for the trunk.	<ul style="list-style-type: none"> ■ 100half, 100full (for Fast Ethernet) ■ 10half, 10full, 100half, 100full (for platforms that support 10 Mbps Ethernet) 	--
Flow control	Flow control setting (Ethernet only)	<ul style="list-style-type: none"> ■ on ■ off ■ rxOn (Gigabit Ethernet) ■ txOn (Gigabit Ethernet) 	off
Trunk name	Name of the trunk. Use quotation marks (") around any string with embedded spaces.	<ul style="list-style-type: none"> ■ Maximum 32 alphanumeric characters ■ ? (for a list of selectable names) 	--
TCMP	Trunk Control Message Protocol (TCMP). Performs the following functions: <ul style="list-style-type: none"> ■ Detects and corrects trunks that violate trunk configuration rules ■ Ensures orderly activation and deactivation of trunk ports 	<ul style="list-style-type: none"> ■ enabled ■ disabled 	enabled

Procedure

You can define all trunks in one `bridge trunk define` operation and then reboot. At the end of each trunk definition, the system prompts you to define another trunk.

1 If you have more than one media type on your system, enter the media type (for example, `Fast_Ethernet` or `Gigabit_Ethernet`).

2 Enter the ports that you want to be part of the trunk.

To get information about the selectable ports, enter `?`

3 Enter the correct operating mode for 10/100 Ethernet ports.

If you are configuring a Fast Ethernet trunk, select the Fast Ethernet port mode (`100half`, `100full`).

4 For an Ethernet trunk, enter the flow control setting (`on`, `off`, `rxOn`, or `txOn`).

- 5 Enter the trunk name, or to get information about specifying the trunk name, enter ?
- 6 Specify whether TCMP is enabled or disabled.
The system indicates that the trunk definition is complete and allows you to define additional trunks until you reach the system trunk limit.
- 7 At the system prompt, to define another trunk enter **y** (yes) or to end the trunk sequence, enter **n** (no).

You must then reboot to enable the trunks to take effect.

Bridge Trunk Define Example (9000)

The example shows a define operation that creates two trunks.

```
Select menu option: bridge trunk define
Select mac type {Fast_Ethernet,Gigabit_Ethernet|?}: Fast_Ethernet
Select ports (14-19|all|?): 14-18
Enter mode {100half,100full|?}: 100full
Enter trunk name {? []}: "Trunk 1"
Enter TCMP state (disabled,enabled) [enabled]: enabled
Trunk definition complete
```

```
Define another trunk? (y,n) [n]: y
Select mac type {Fast_Ethernet,Gigabit_Ethernet|?}: Fast_Ethernet
Select up to 8 ports (1-12|?): 1-6
Enter trunk name {? []}: Trunk2
Enter TCMP state (disabled,enabled) [enabled]: enabled
Trunk definition complete
```

The configuration of the ports will be modified.

The system must be rebooted to complete trunk configuration.
This may take a few minutes.

```
Are you sure you want to reboot the system? (n,y) [y]: y
```

bridge trunk modify

Changes a trunk in either of two ways:

- ✓ 3500
- ✓ 9000
- ✓ 9400

- Modifies a trunk's characteristics (for example, a Fast Ethernet operating mode or the Trunk Control Message Protocol (TCMP) state).
- Adds or removes a port from the trunk, as long as you maintain at least one of the original ports in the trunk.

- ✓ 3900
- ✓ 9300

Valid Minimum Abbreviation

b t m

Important Considerations

- Keep at least one port that you defined in the original trunk. To completely redefine a trunk configuration, remove the trunk and define a new one.
- You cannot modify, add, or remove ports that are part of different trunks from the trunk that you are modifying.
- To avoid configuration errors, do not modify Fiber Distributed Data Interface (FDDI) station mode port pairs when any of the ports in the pair are members of a trunk.
- If you have more than one media type on your system (for example, Fast Ethernet and Gigabit Ethernet), you are prompted for a media type before you are prompted for the trunk information.
- Any changes that you make to the trunk's characteristics take effect immediately and do not interrupt trunk operations. If you add or remove a port, however, you must reboot the system to implement the change.

- In an FDDI trunk:
 - You cannot modify FDDI station mode port pairs when any of the ports in the pair are in a trunk.
 - When you modify the station mode, any FDDI ports that are associated with virtual LANs (VLANs) or a trunk are removed from the VLAN or trunk.
- Within a trunk, you cannot change certain port characteristics, such as FDDI station mode. For example, in an FDDI trunk, you cannot change a trunked DAS (dual attach station) port to an SAS (single attach station) port or an SAS port to a DAS port.
- If you change an FDDI port pair from SAS to DAS, you select the pair using just the lower of the two port numbers, just as with a trunk anchor port.

Options

Prompt	Description	Possible Values	[Default]
Trunk index	Index number of the trunk that you want to modify	<ul style="list-style-type: none"> ■ One or more trunks ■ ? (for a list of selectable trunk indexes) 	–

Prompt	Description	Possible Values	[Default]
Ports	Total number of the bridge ports that you want to be part of the trunk	<p>9000:</p> <ul style="list-style-type: none"> ■ Layer 2 modules support up to 4 trunk groups with up to 6 ports per trunk ■ Layer 3 modules support up to 3 trunk groups with up to 6 ports per trunk <p><i>The 6-port SAS (3-port DAS) FDDI Layer 3 supports 3 trunk groups. In SAS mode the trunks can contain up to 6 ports. In DAS mode, the trunks can contain up to 3 ports.</i></p> <ul style="list-style-type: none"> ■ The FGA24 switch fabric module supports up to 4 trunk groups with up to 6 ports per trunk and the FGA24T switch fabric module supports up to 12 trunk groups with up to 6 ports per trunk <p><i>(The GA9 cannot support 12 trunk groups because there are not enough ports on this module.)</i></p> <p>3500:</p> <ul style="list-style-type: none"> ■ Supports up to 4 trunk groups with up to 8 ports per trunk <p>3900:</p> <ul style="list-style-type: none"> ■ Supports up to 4 trunk groups with up to 6 ports per trunk <p>9300 and 9400:</p> <ul style="list-style-type: none"> ■ Supports up to 12 trunk groups with up to 6 ports per trunk ■ all 	Currently configured ports

Prompt	Description	Possible Values	[Default]
Mode	Operating mode for a 10/100 Ethernet trunk	<ul style="list-style-type: none"> ■ 100half, 100full (for Fast Ethernet) ■ 10half, 10full, 100half, 100full (for platforms that support 10 Mbps Ethernet) 	Current mode
Flow control (Gigabit Ethernet only)	Flow control setting for a Gigabit Ethernet trunk	<ul style="list-style-type: none"> ■ on ■ off ■ rxOn ■ txOn 	Current value
Trunk name	Name of the trunk. Use quotation marks (") around any string with embedded spaces.	<ul style="list-style-type: none"> ■ Maximum 32 alphanumeric characters ■ ? (for a list of selectable trunk names) 	Current trunk name
TCMP	Trunk Control Message Protocol (TCMP). Performs the following functions: <ul style="list-style-type: none"> ■ Detects and corrects trunks that violate trunk configuration rules ■ Ensures orderly activation and deactivation of trunk ports 	<ul style="list-style-type: none"> ■ enabled ■ disabled 	enabled (factory default), or current TCMP state

Procedure

To modify trunk information for a bridge, follow these steps:

- 1** Enter the trunk index number, or to display the selectable trunks, enter `?`
The system shows the media type for the trunk (for example, `Fast Ethernet`, `Gigabit Ethernet`, or `FDDI`).
- 2** At the prompt, enter the ports that you want to be part of the trunk, or to display a port summary, enter `?`
The maximum number of ports per trunk is 8 (for the CoreBuilder 3500 and the CoreBuilder 9000 Layer 3 modules).
- 3** To change the 10/100 operating mode, enter the new operating mode, or to display information about the selectable values, enter `?`
For Fast Ethernet, you can select 100 Mbps, running in half-duplex or full-duplex mode. All ports in the trunk are set to the specified operating mode.
- 4** To change the flow control setting for a Gigabit Ethernet trunk only, enter a new flow control setting
- 5** To change the name of the trunk, enter the new name, or to view information on how to specify a trunk name, enter `?`
The name can have up to 32 characters. Use quotation marks around any character string that has embedded spaces.
- 6** Enter the TCMP state. The system default is `enabled`.
If you modified the port information, the system displays a message to inform you that the port configuration will change and then displays a reboot prompt.
- 7** At the system prompt, to reboot the system, enter `y` (yes) and implement the new trunk information, or to return to the previous menu, enter `n` (no).
Entering `n` (no) cancels the trunk changes. The system reports that it is unable to continue with the trunk configuration.

Bridge Trunk Modify Example (9000)

```
Select menu option: bridge trunk modify
Select trunk index {1-3|?}: ?
```

```
Selectable trunks
```

selection	ports	name
1	7,8,12	trunk1
2	1,2,4,19	trunk2
3	3,14,17,18	trunk3

```
Select trunk index {1-3|?}: 2
```

```
Fast Ethernet
```

```
Select ports (1,2,5,6,15,16,19|all|?) [1,2,19]: 1,2
```

```
Enter trunk name {?} [trunk2]:
```

```
Enter TCMP state (disabled,enabled) [enabled]:
```

```
The configuration of the ports will be modified.
```

```
Are you sure you want to reboot the system? (n,y) [y]:
```

bridge trunk remove

Removes a previously defined trunk. You can remove one or more trunks with this command.

✓ 3500
 ✓ 9000
 ✓ 9400

Valid Minimum Abbreviation

b t r

✓ 3900
 ✓ 9300

Important Considerations

- The number of trunk groups and the number of ports within a trunk group depend on your system. See the Options table. However, because each Gigabit Ethernet module uses an internal trunk resource towards the limit of four (Gigabit Ethernet only), keep in mind how many trunk resources you have when you remove trunks. For example, if you have a trunk with two Gigabit Ethernet ports (which consolidates two Gigabit trunk resources into one) as well as three other trunks, and you then try to remove the Gigabit Ethernet trunk, you will exceed the trunk resource limit. (The Gigabit Ethernet ports use two trunk resources.) The system reports that it is unable to remove the trunk because the trunk resource limit would be exceeded.
- Removing a trunk requires a module reboot. For CoreBuilder 9000 modules, rebooting a module returns you to the EME prompt, which requires you to reconnect to the module.

Options

Prompt	Description	Possible Values	[Default]
Trunk index	Index number of the trunk that you want to remove	<ul style="list-style-type: none"> ■ One or more valid trunk index number ■ all ■ ? (for a list of selectable trunk indexes) 	–

Bridge Trunk Remove Example (9000)

```
Select menu option: bridge trunk remove
CB9000@slot10.1 [12-E/FEN-TX-L3] (bridge/trunk) remove
Select trunk index(s) {1-2|all|?}: 2
```

The configuration of the ports will be modified.

The module must be rebooted to complete trunk configuration.
This may take a few minutes.

Are you sure you want to reboot the system? (n,y) [y]:y

12

MULTIPOINT LINK AGGREGATION (MPLA)

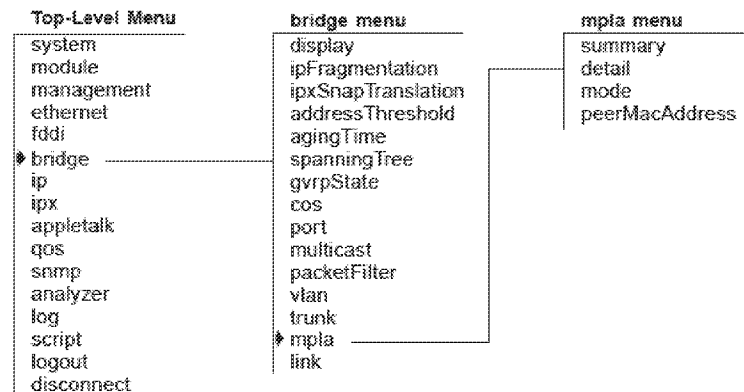
MultiPoint Link Aggregation (MPLA) increases the capacity and availability of campus LAN cores without using complex, meshed router networks. Functioning at Layer 2, MPLA provides both dual-homed link resiliency and automatic load sharing over point-to-multipoint backbone connections. MPLA increases network availability using scalable Gigabit Ethernet connections among multiple campus switches.



For more information about MPLA and trunking, see the CoreBuilder 9400 Implementation Guide.

Menu Structure

The commands that you can use depend on the system that you have, your level of access, and the types of modules and other hardware options that are configured for your system. The following diagram shows the complete list of commands for all systems. See the checklist at the beginning of each command description in this chapter for whether your system supports the command.



bridge mpla summary Describes the state of the multipoint aggregated link.

3500

9000

✓ 9400

3900

9300

Valid Minimum Abbreviation

b mp s

Fields in the Bridge MPLA Summary Display

Field	Description
Mode	Whether MPLA is enabled on the switch. Possible values are <code>enabled</code> and <code>disabled</code> . The default is <code>disabled</code> .
Peer Switch Interface State	The state (<code>up</code> or <code>down</code>) of the out-of-band management port on the other (peer) switch in the MPLA core.

bridge mpla detail Displays the trunk state and node trunk IDs for the switch ports.

3500

9000

✓ 9400

3900

9300

Valid Minimum Abbreviation

b mp d

Fields in the Bridge MPLA Detail Display

Field	Description
Mode	Whether MPLA is enabled on the switch. Possible values are <i>enabled</i> and <i>disabled</i> . The default is <i>disabled</i> .

bridge mpla mode

Enables or disables the MultiPoint Link Aggregation feature on the switch.

3500

9000

✓ 9400

3900

9300

Valid Minimum Abbreviation

b mp m

Important Considerations

- Use only CoreBuilder 9400 systems as MPLA core switches.
The core of a multipoint aggregated link must contain two 9400 switches, whose out-of-band management ports also must be directly connected.
- Use only Switch 3900 devices as edge switches.
Each MPLA edge switch must have at least one physical link to each core switch. Multiple trunked links may connect an edge and core switch, for added bandwidth
- Use only Gigabit Ethernet links between MPLA core switches and edge switches.
- All links from an edge switch to the MPLA core switches must be aggregated (trunked) at the edge switch.
- While the Trunk Control Message Protocol (TCMP) is optional in point-to-point trunks, you must configure it to run on all of the point-to-multipoint links between MPLA edge switches and core switches.
- You can enable these features in MPLA *edge* switches, but not in MPLA *core* switches:
 - Spanning Tree
 - IGMP snooping
 - Resilient links
 - Roving analysis port
- When you configure a new MPLA core switch, define MPLA configurations and reboot the switch before you define other trunks and VLANs on the switch.

Procedure

- 1** To enable MultiPoint Link Aggregation on the switch, use the `bridge mpla mode enable` command.
To disable MultiPoint Link Aggregation on the switch, use the `bridge mpla mode disable` command.
- 2** Select the ports that you want to be part of the multipoint aggregated link using the `bridge trunk define` command, as described in Chapter 11.
- 3** Reboot the switch to implement the multipoint aggregated link selection.
On reboot, existing trunks and VLANs are deleted, and the default VLAN is restored.

**bridge mpla
peerMacAddress**

Specifies the MAC address of the out-of-band management port of the *attached* CoreBuilder 9400 switch in the MPLA core (the *peer* core switch).

3500

9000

✓ 9400

3900

9300

Valid Minimum Abbreviation

b mp p

Important Considerations

- You execute this command on each of the two CoreBuilder 9400 switches in the MPLA core.
- In each core switch, you use this command to specify the MAC address for the out-of-band management port of the *attached* peer switch.



You must use this management port to connect a crossover Ethernet cable to the out-of-band management port on the switch you are presently configuring.

- The input format for this MAC address is 00-00-00-00-00-00

13

RESILIENT LINKS

Resilient links protect your network against the failure of an individual link or device by providing a secondary backup link that is inactive until it is needed.

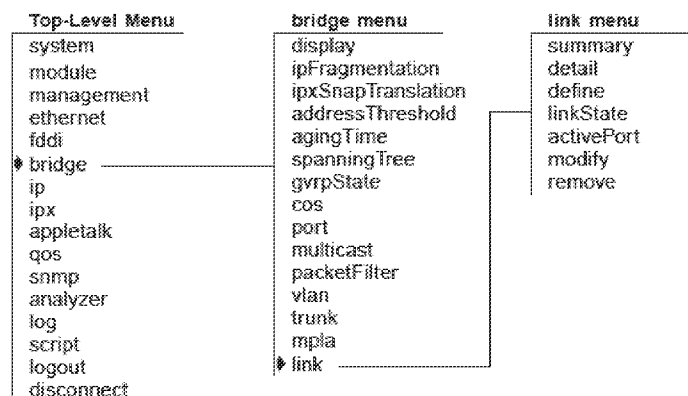
This chapter provides guidelines and other key information about how to configure resilient links in your system.



For more information about resilient links, see the Implementation Guide for your system.

Menu Structure

The commands that you can use depend on the system that you have, your level of access, and the types of modules and other hardware options that are configured for your system. The following diagram shows the complete list of commands for all systems. See the checklist at the beginning of each command description in this chapter for whether your system supports the command.



bridge link summary *For CoreBuilder 9000: Applies to Layer 2 switching modules only.*

3500
 ✓ 9000
 ✓ 9400

Displays summary information about configured resilient links on your system. In a summary report, the system displays the index number, link name, and whether the link is up or down.

✓ 3900
 ✓ 9300

Valid Minimum Abbreviation

b l s

Fields in the Bridge Link Summary Display

Field	Description
Index	Number that the system assigned to the resilient link pair. You can select all resilient link pairs or one resilient link pair.
Name	Name of the defined resilient link pair.
State	Whether the resilient link pair is up or down.

bridge link detail *For CoreBuilder 9000: Applies to Layer 2 switching modules only.*

Displays detailed link information in addition to the summary information.

3500
 ✓ 9000
 ✓ 9400

Valid Minimum Abbreviation

b 1 det

✓ 3900
 ✓ 9300

Fields in the Bridge Link Detail Display

Field	Description
Active Port	Port that carries network traffic
Enable State	Whether the resilient pair is enabled or disabled
Index	Number that the system assigned to the resilient link pair. You can select all resilient link pairs or one resilient link pair.
Main Link	Link state (up or down) of the main link
Main Port	Main resilient link port
Name	Name of the defined link
Standby Link	Link state (up or down) of the standby link
Standby Port	Standby resilient link port to which traffic shifts if the main resilient link port fails
State	Whether the resilient link pair is up or down

bridge link define *For CoreBuilder 9000: Applies to Layer 2 switching modules only.*

Defines one or more links on the system. When you define a link, you specify ports and characteristics for the link.

3500
 ✓ 9000
 ✓ 9400

✓ 3900
 ✓ 9300

Valid Minimum Abbreviation

`b l def`

Important Considerations

- Connect the network cable to the resilient link ports after you reboot the system; failure to do so may create a bridge loop in your network.
- In general, create resilient links before you define your virtual LANs (VLANs). If you plan to create resilient links for part of a VLAN, create the resilient links before you create the VLAN.
- When you create a resilient link that includes ports that are part of a VLAN, those ports are removed from the VLAN. You must modify the VLAN and add the new bridge port to the appropriate VLAN. This situation does not apply to the default VLAN (all ports are part of the default VLAN).
- If you have already defined other resilient links or trunks on your system, you cannot select ports that are part of an existing resilient link pair or a trunk.
- You must reboot the system at the end of the link definition process. (You can define multiple links in one `define` operation.)
- The resilient link port pair uses a single MAC address for frames sourced by this pair.
- The resilient link name can be up to 32 alphanumeric characters.

Options

Prompt	Description	Possible Values	[Default]
Resilient link name	Name of the link. Use quotation marks around any character string that contains spaces	Maximum 32 alphanumeric characters	–
Main Port	Main port that you want to be part of the link.	Any of the available ports on the system	–
Standby Port	Standby port that you want to be part of the link.	Any of the available ports on the system	–
Define another link?	Whether you want to define another link.	<ul style="list-style-type: none"> ■ y (yes) ■ n (no) 	n
Reboot the system?	Resilient links that you define do not take effect until you reboot the system.	<ul style="list-style-type: none"> ■ y (yes) ■ n (no) 	y

Procedure

You can define all links in one `bridge link define` operation and then reboot. At the end of each link definition, the system prompts you to define another link.

- 1 Enter the link name, or to get information about specifying the link name, enter `?`
- 2 Select the port that you want to be the main port.
To get information about the selectable ports, enter `?`
- 3 Select the port that you want to be the standby port.
To get information about the selectable ports, enter `?`
- 4 At the system prompt, to define another link enter `y` (yes), or to end the link define sequence, enter `n` (no).

You must reboot for the links to take effect.

bridge link linkState *For CoreBuilder 9000: Applies to Layer 2 switching modules only.*

Sets the linkState value (enabled or disabled) for a specific resilient link.

3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

b l l

Important Considerations

- When the `bridge link linkState` option is enabled, the resilient link transmits or receives frames.
- When the `bridge link linkState` option is disabled, the resilient link no longer transmits or receives frames.

Options

Prompt	Description	Possible Values	[Default]
Resilient link index	Index number of the resilient link that you want to modify	<ul style="list-style-type: none"> ■ Depends on configured links ■ ? (for a list of selectable link indexes) ■ A valid link number ■ all 	–
linkState value	Whether you want the resilient link for the selected link index to transmit and receive frames	<ul style="list-style-type: none"> ■ enable ■ disable 	–

bridge link activePort *For CoreBuilder 9000: Applies to Layer 2 switching modules only.*

Sets either the main port or the standby port as the active port. The active port carries the network traffic.

3500
 ✓ 9000
 ✓ 9400

Valid Minimum Abbreviation

b 1 a

✓ 3900
 ✓ 9300

Options

Prompt	Description	Possible Values	[Default]
Resilient link index	Index number of the link whose active port you want to set	<ul style="list-style-type: none"> ■ Depends on configured links ■ ? (for a list of selectable link indexes) ■ A valid link number ■ all 	—
Active port state	Port that you want to carry network traffic	<ul style="list-style-type: none"> ■ main ■ standby 	—

bridge link modify *For CoreBuilder 9000: Applies to Layer 2 switching modules only.*

Modifies the link name, as well as the main port and standby port, of a defined resilient link.

3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

b l m

Important Considerations

- Connect the network cable to the resilient link port after you reboot the system.
- In general, create links before you define your Virtual LANs (VLANs). If you plan to create resilient links for part of a VLAN, create the resilient links before you create the VLAN.
- When you create a resilient link that includes ports that are part of a VLAN, those ports are removed from the VLAN. You must modify the VLAN and add the new bridge port to the appropriate VLAN. This situation does not apply to the default VLAN (all ports are part of the default VLAN).
- If you have already defined other links or trunks on your system, you cannot select ports that are part of an existing link or a trunk.
- You must reboot the system at the end of the link definition process. (You can define multiple links in one `define` operation.)
- The resilient link port pair uses a single MAC address for frames sourced by this pair.
- The resilient link name can be up to 32 alphanumeric characters.

Options

Prompt	Description	Possible Values	[Default]
Resilient link name	New resilient link name. Use quotation marks around any character string that has embedded spaces.	Maximum 32 alphanumeric characters	–
Main port	New port to be the main port of the defined resilient link.	Any of the available ports on the system	–
Standby port	New port to be the standby port of the defined resilient link.	Any of the available ports on the system	–
Define another link?	Whether you want to define another link.	<ul style="list-style-type: none"> ■ y (yes) ■ n (no) 	n
Reboot the system?	Resilient links that you define do not take effect until you reboot the system.	<ul style="list-style-type: none"> ■ y (yes) ■ n (no) 	y

bridge link remove *For CoreBuilder 9000: Applies to Layer 2 switching modules only.*

Removes a previously defined resilient link pair. You can remove one or more resilient link pairs with this command.

3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviation

b l r

Important Consideration

- Removing a link requires that you reboot the system.

Options

Prompt	Description	Possible Values	[Default]
Resilient link index	Index number of the resilient link pair that you want to remove	<ul style="list-style-type: none"> ■ Depends on configured links ■ ? (for a list of selectable link indexes) 	–

Bridge Link Remove Example

Select menu option: `bridge link remove`

Select link index(s) (1-2|all|?): `2`

The configuration of the ports will be modified.

The system must be rebooted to complete resilient link configuration.

This may take a few minutes.

Are you sure you want to reboot the system? (n,y) [y]: `y`

14

VIRTUAL LANs (VLANs)

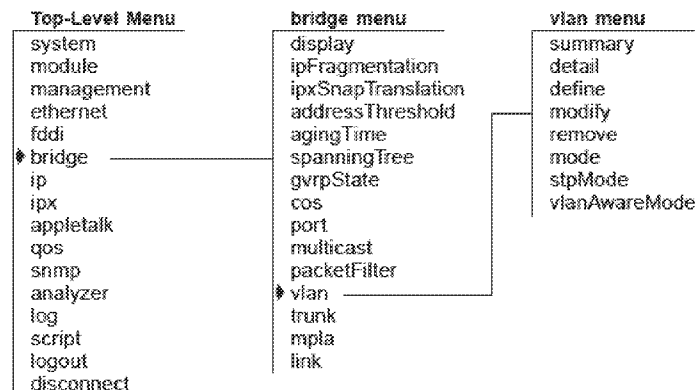
A virtual LAN (VLAN) is a logical definition of a network work group. It is roughly equivalent to a broadcast domain. A *VLAN interface* is your system's point of attachment to a given VLAN. A VLAN and a VLAN interface are analogous to an IP subnetwork and an IP interface.



For more information about VLANs, see the Implementation Guide for your system.

Menu Structure

The commands that you can use depend on the system that you have, your level of access, and the types of modules and other hardware options that are configured for your system. The following diagram shows the complete list of commands for all systems. See the checklist at the beginning of each command description in this chapter for whether your system supports the command.



The `bridge vlan stpMode` command is available only when you enable *allClosed* mode on the CoreBuilder® 3500 system or the CoreBuilder 9000 Layer 3 switching modules. The command does not appear when you are using the default VLAN mode (*allOpen*) or when you use *allClosed* mode on a Layer 2 system or module.

bridge vlan summary

Displays a summary of VLAN information. In a summary report, the system displays the ports and protocols that are assigned to each VLAN.

✓ 3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

Valid Minimum Abbreviations

b v s (in allOpen mode on Layer 2 or Layer 3 switches and modules)

b v su (in allClosed mode on Layer 3 switches and modules)

Important Considerations

- The summary display lists the physical ports that are associated with each VLAN interface. It does not indicate bridge port characteristics (for example, trunked ports). See “bridge vlan detail” next for this information.
- The VLAN mode (shown in the Type field) affects VLANs as follows:
 - For the CoreBuilder 3500, CoreBuilder 9400, SuperStack® II Switch 3900, and SuperStack II Switch 9300, the VLAN mode affects all configured VLANs on the system. For the entire system, the default VLAN mode is `allOpen`.
 - For the CoreBuilder 9000, the VLAN mode affects all VLANs that are associated with a particular module (the switch fabric module, or all VLANs on a switching module). For each module, the default VLAN mode is `allOpen`.
- As of Release 3.0.0, the CoreBuilder 3500 system and CoreBuilder 9000 Layer 3 modules support one of three origins for a VLAN:
 - If you explicitly create the VLAN with a `bridge vlan define` operation, the origin of the VLAN is `static`.
 - If you create a router port IP interface (for which the system automatically creates a router port VLAN), the origin of the router port VLAN is `router`.
 - If you enable dynamic port-based VLAN configuration via the GARP VLAN Registration Protocol (GVRP), the origin is `GVRP`.

- GVRP is based on IEEE 802.1Q and allows for dynamic configuration of port-based VLANs. GVRP can help you simplify the management of VLAN configurations in larger networks. Use the command `bridge port gvrpState` to explicitly enable GVRP on the participating bridge ports *and* use the command `bridge gvrpState` to enable the bridge GVRP state for the entire system. The bridge GVRP state enables you to control GVRP on the system without losing the per-port GVRP state. By default, the GVRP state for the entire system is `disabled` and the GVRP state for each bridge port is `disabled`.
- The system prompts you for a VLAN interface index number before it displays the summary information.

Options

Prompt	Description	Possible Values	[Default]
VLAN interface index	Index numbers of the VLAN interfaces for which you want summary information	<ul style="list-style-type: none"> ■ One or more selectable VLAN interface index numbers ■ all ■ ? (for a list of selectable indexes) 	1 (if you have only one VLAN)

Fields in the Bridge VLAN Summary Display

Field	Description
Index	System-assigned index number that identifies a VLAN of the identified origin. Statistics appear in the display for the VLAN that you specify.
Name	Character string of from 0 through 32 bytes that identifies the VLAN. The default VLAN always uses the name <code>Default</code> .

Field	Description
Origin	<p>For all Layer 2 systems or switching modules, the VLAN origin is always <code>static</code>, which indicates that the user created the VLAN. For the CoreBuilder® 3500 or CoreBuilder 9000, the origin indicates one of the following:</p> <ul style="list-style-type: none"> ■ <code>static</code> — The VLAN was created statically (user-configured by using the <code>bridge vlan define</code> command). ■ <code>router</code> — The VLAN was created automatically by a router port IP interface (of router origin). You create a router port IP interface using the <code>ip interface define</code> command with the interface type <code>port</code>. You cannot modify or remove a router port VLAN. ■ <code>GVRP</code> — The VLAN was created dynamically from a GVRP update (GVRP). You must enable the GVRP state for the entire system as a bridge-wide parameter <i>and</i> for the participating bridge ports as a bridge-port parameter.
Ports	<p>Index numbers of the bridge ports that belong to the VLAN, or the bridge port that belongs to the router port IP interface.</p> <p>On the CoreBuilder 9000, the list of ports includes the front-panel ports and the appropriate backplane ports. Example: On a 12-port Layer 3 module, the list of ports includes ports 1 – 12 and port 13, which is the module's backplane port.</p>
Type (VLAN mode)	<p>Either <code>allOpen</code> or <code>allClosed</code>. VLANs in <code>allOpen</code> mode share a single address table for all configured VLANs; in <code>allClosed</code> mode, each VLAN has its own unique address table. Standard bridging rules apply based on the table addresses that are assigned to the specific VLAN. A router port IP interface requires that you put the system in <code>allClosed</code> mode.</p>
VID	<p>Unique, user-defined integer (VLAN ID) that identifies this VLAN. It is used by management operations. You can assign or modify a VID that is associated with a static VLAN; you cannot modify the VID selected automatically after you define a router port IP interface, nor can you change the VID of the default VLAN. The default VLAN requires a VID of 1.</p>
VLAN Aware Mode (3500 and 9000 Layer 3)	<p>Whether the VLAN aware mode (tagging mode) is <code>allPorts</code> or <code>taggedVlanPorts</code>. The default for CoreBuilder 3500 Release 2.0 or later is <code>allPorts</code>; <code>allPorts</code> is also the default as of CoreBuilder 9000 software Release 3.0. The value <code>taggedVlanPorts</code> is a compatibility mode for VLANs configured prior to CoreBuilder 3500 Release 2.0 and for VLANs configured on CoreBuilder 9000 Layer 3 modules prior to CoreBuilder 9000 Release 3.0.</p>

bridge vlan detail

- ✓ 3500
- ✓ 9000
- ✓ 9400

Displays per-port information such as tagging in addition to the VLAN summary information. For the CoreBuilder 3500 and the CoreBuilder 9000 Layer 3 switching modules, this command also displays VLAN statistics.

Valid Minimum Abbreviation

b v det

- ✓ 3900
- ✓ 9300

Important Considerations

- The default VLAN always uses VLAN ID (VID) 1 and the name `Default`. For Layer 3 systems and modules, it also uses the protocol type `unspecified`.
- The VLAN ID (VID) is used as the 802.1Q tag if tagging is enabled for a port.
- The VLAN statistics for the CoreBuilder 3500 and CoreBuilder 9000 Layer 3 switching modules are valid *only* under one of the following conditions:
 - If the VLANs are defined for the same protocol type (or for the type called `unspecified`) and do not share any ports. Example: IP VLAN1 has ports 1 through 6 and IP VLAN2 has ports 7 through 12.
 - If the VLANs are explicitly defined for different protocol types. In this case, the VLANs may share ports. Example: An IP VLAN and an IPX VLAN both use ports 2 through 4.
- As of Release 3.0.0, the CoreBuilder 3500 system and CoreBuilder 9000 Layer 3 modules support one of three origins for a VLAN:
 - If you explicitly create the VLAN with a `bridge vlan define` operation, the origin of the VLAN is `static`.
 - If you create a router port IP interface (for which the system automatically creates a router port VLAN), the origin of the router port VLAN is `router`.
 - If you enable dynamic port-based VLAN configuration via the GARP VLAN Registration Protocol (GVRP), the origin is `GVRP`.

- GVRP is based on IEEE 802.1Q and allows for dynamic configuration of port-based VLANs. GVRP can help you simplify the management of VLAN configurations in larger networks. Use the command `bridge port gvrpState` to explicitly enable GVRP on the participating bridge ports *and* use the command `bridge gvrpState` to enable the bridge GVRP state for the entire system. The bridge GVRP state enables you to control GVRP on the system without losing the per-port GVRP state. By default, the GVRP state for the entire system is `disabled` and the GVRP state for each bridge port is `disabled`.
- The system prompts you for a VLAN interface index number before it displays the detail information.
- Either you can use network-based IP VLANs (by supplying Layer 3 address information when you configure a VLAN for IP), or you create the IP VLAN and then define multiple IP interfaces per VLAN. See Chapter 16.

Options

Prompt	Description	Possible Values	[Default]
VLAN interface index	Index numbers of the VLAN interfaces for which you want detailed information	<ul style="list-style-type: none"> ■ One or more selectable VLAN interface index numbers ■ all ■ ? (for a list of selectable indexes) 	1 (if you have only one VLAN)

Fields in the Bridge VLAN Detail Display

Field	Description
Ignore STP mode (3500 and 9000 Layer 3)	Whether a VLAN can ignore STP blocked ports and let routing traffic pass through. Possible values: <code>enabled</code> and <code>disabled</code> .
Index	System-assigned index number that identifies a VLAN. Statistics appear for the VLAN that you specify.
Layer 3 addresses (3500 and 9000 Layer 3)	Information that is used to set up flood domains for overlapping IP VLAN subnetworks (network-based VLANs).
Name	Character string 0 through 32 bytes that identifies the VLAN. The default VLAN always uses the name <code>Default</code> .

Field	Description
Origin	<p>For all Layer 2 systems or switching modules, the VLAN origin is always <code>static</code>, which indicates that the VLAN was created by the user. For the CoreBuilder® 3500 or CoreBuilder 9000, the origin indicates one of the following:</p> <ul style="list-style-type: none"> ■ <code>static</code> — The VLAN was created statically (user-configured by using the <code>bridge vlan define</code> command). ■ <code>router</code> — The VLAN was created automatically by the router port IP interface (of router origin). You create a router port IP interface using the <code>ip interface define</code> command with the interface type <code>port</code>. You cannot modify or remove a router port VLAN. ■ <code>GVRP</code> — The VLAN was created dynamically from a GVRP update (<code>GVRP</code>). You must enable the GVRP state for the entire system as a bridge-wide parameter <i>and</i> for the participating bridge ports as a bridge-port parameter.
Ports/Port	<p>Index numbers of the bridge ports that belong to each VLAN. In the second part of the detail display, the Port column lists the ports for the VLAN individually and indicates ports that are trunked or have tagging.</p> <p>On the CoreBuilder 9000, the list of ports includes the front-panel ports and the appropriate backplane ports. Example: On a 12-port Layer 3 module, the list of ports includes ports 1 – 12 and port 13, which is the module's backplane port.</p>
Protocol (3500 and 9000 Layer 3)	<p>Protocol suites for the VLAN. VLANs that are associated with router port IP interfaces always have IP as the protocol type. The default VLAN always uses the protocol type <code>unspecified</code>.</p>
rxBcastBytes (3500 and 9000 Layer 3)	Number of received broadcast bytes
rxBcastFrames (3500 and 9000 Layer 3)	Number of received broadcast frames
rxMcastBytes (3500 and 9000 Layer 3)	Number of received multicast bytes
rxMcastFrames (3500 and 9000 Layer 3)	Number of received multicast frames
rxUcastBytes (3500 and 9000 Layer 3)	Number of received unicast bytes
rxUcastFrames (3500 and 9000 Layer 3)	Number of received unicast frames

Field	Description
Tag type (3500 and 9000 Layer 3)	Whether tagging is set to <code>none</code> or <code>802.1Q</code> (IEEE 802.1Q tagging)
txBcastBytes (3500 and 9000 Layer 3)	Number of transmitted broadcast bytes
txBcastFrames (3500 and 9000 Layer 3)	Number of transmitted broadcast frames
txMcastBytes (3500 and 9000 Layer 3)	Number of transmitted multicast bytes
txMcastFrames (3500 and 9000 Layer 3)	Number of transmitted multicast frames
Type (VLAN Mode)	Either <code>allOpen</code> or <code>allClosed</code> . VLANs in <code>allOpen</code> mode share a single address table for all configured VLANs. In <code>allClosed</code> mode, each VLAN has its own unique address table. Standard bridging rules apply based on the table addresses that are assigned to the specific VLAN. Router port IP interfaces require <code>allClosed</code> mode.
VID	Unique, user-defined integer (VLAN ID) that identifies this VLAN. It is used by management operations. You can assign or modify a VID that is associated with a static VLAN; you cannot modify the VID selected automatically after you define a router port IP interface, nor can you change the VID of the default VLAN. The default VLAN requires a VID of 1.
VLAN Aware Mode (Layer 3 only)	Whether the VLAN aware mode (tagging mode) is <code>allPorts</code> or <code>taggedVlanPorts</code> . The default for CoreBuilder 3500 Release 2.0 or later is <code>allPorts</code> ; <code>allPorts</code> is also the default as of CoreBuilder 9000 software Release 3.0. The value <code>taggedVlanPorts</code> is a compatibility mode for VLANs configured prior to CoreBuilder 3500 Release 2.0 and for VLANs configured on CoreBuilder 9000 Layer 3 modules prior to CoreBuilder 9000 Release 3.0.

**bridge vlan define
(3500/9000 Layer 3)**

✓ 3500
✓ 9000
9400

3900
9300

**For CoreBuilder 9000: Applies to Layer 3 switching modules only.**

Creates a VLAN on the CoreBuilder 3500 system or a CoreBuilder 9000 Layer 3 module. When you explicitly configure a VLAN on the system, you assign information such as a VLAN ID (VID), a set of bridge ports, and, optionally, a protocol type and IEEE 802.1Q tagging.

For details about this command on the SuperStack II Switch 3900, the Switch 9300, the CoreBuilder 9400, and CoreBuilder 9000 Layer 2 modules, see “bridge vlan define (3900/9300/9400/ 9000 Layer 2)” next.

Valid Minimum Abbreviation

`b v def`

Important Considerations

- If you have previously defined your IP VLANs with Layer 3 address information (that is, network-based VLANs), you can redefine your IP VLANs without Layer 3 address information. To define multiple IP interfaces per IP VLAN, use the `ip interface define` command. (See Chapter 16.)
- The VLAN that you create with this command is a static VLAN. To establish routing between static IP VLANs, define your IP VLANs and then use the `ip interface define` command to define an IP routing interface. As of Release 3.0, you can also specify the interface type `vlan` to create one or more IP routing interfaces for a static IP VLAN.
- If you have a router port IP interface on the system, you *cannot* specify the port that belongs to the router port IP interface when you explicitly define an IP VLAN (or a VLAN that includes the IP protocol). A router port IP interface is an alternative to static VLANs and allows routing versus bridging. You create a router port IP interface by entering the `ip interface define` command with the interface type `port` and a single bridge port. A router port IP interface requires `allClosed` mode. See Chapter 16 for more information.

- You must specify a VID in the range from 2 through 4094. You can no longer define a VLAN other than the default VLAN with a VID of 1. VID 1 is reserved for the default VLAN only as of Release 3.0.0. (As of Release 3.0.0, the default VLAN always uses the name `Default` and the protocol type `unspecified`.) If you delete the default VLAN, you can redefine it with VID 1 only.
- You cannot delete a VLAN that has a routing interface associated with it.
- If you plan to use the trunking feature or the MPLA feature, define the appropriate trunks *before* you define your VLANs. See Chapter 11 for more information.
- If you plan for your VLAN to include trunk ports, specify the anchor port (lowest-numbered port) that is associated with the trunk. For example, if ports 1 through 3 are associated with a trunk, specify `1` to define the VLAN to include all of the physical ports in the trunk (ports 1 through 3). If you have not defined trunks, specify one or more port numbers, or `all` to assign all ports to the VLAN interface.
- If a port is shared by another VLAN, verify that if tagging is the only distinguishing characteristic between the VLANs, the specified tag type is not in conflict with the port's tag type in another VLAN (that is, there is only one port that is tagged `none`).
- Do not use this command if you want GVRP to dynamically create IEEE 802.1Q port-based VLANs. Instead, explicitly enable the GVRP state for the participating ports and enable the GVRP state for the entire system. To set the per-port GVRP state, use the `bridge port gvrpState`. (See Chapter 10.) To set the bridge-wide GVRP state, use the `bridge gvrpState` command. (See Chapter 9.)
- Whether you are bridging or routing, you can select more than one protocol suite per VLAN and specify one protocol at each of the prompts. Use the protocol type of `unspecified` to create a port-based VLAN.
- The IPX protocol type `IPX-802.2-SNAP` is available for both the CoreBuilder 3500 system and the CoreBuilder 9000 Layer 3 switching modules.
- For the CoreBuilder 9000, keep the following considerations in mind:
 - When you define a VLAN on a switching module (and other switching modules in the system also define this VLAN), you must define the VLAN on both the switching module *and* on the switch fabric module.

- When you define the VLAN on the Layer 3 switching module, you must specify any front-panel ports in the VLAN as well as the module's backplane port. The specified backplane port must also be tagged if you have more than one VLAN and plan to communicate with VLANs on other modules on the CoreBuilder 9000 through the switch fabric module.
- When you define the VLAN on the switch fabric module, you must specify which switch fabric module backplane port is connected to the module backplane port. The switch fabric module backplane port must also be tagged if you have more than one VLAN.
- When you use a Layer 3 switching module to establish routing between VLANs on other switching modules, you can configure the backplane port of the Layer 3 switching module as part of the VLANs and then define a routing interface for each VLAN. One VLAN equals one network or subnetwork.
- For configurations that include FDDI ports, if you plan for your VLAN to include FDDI DAS ports, you must specify the lowest-numbered port in the DAS pair when defining the ports in the VLAN. See Chapter 8.
- Specify ? to see the port summary (for example, to see whether ports are associated with a trunk), and then enter the appropriate port numbers.
- The VID is used as the IEEE 802.1Q tag if tagging is enabled for a port.

Options

Prompt	Description	Possible Values	[Default]
VID	Unique, user-defined integer used by management operations	<ul style="list-style-type: none"> ■ If the default VLAN exists, 2 – 4094 ■ If the default VLAN does not exist, 1 to redefine the default VLAN, or 2 – 4094 for other VLANs 	Next available VID

Prompt	Description	Possible Values	[Default]
Bridge ports	<p>Index numbers of the bridge ports that belong to the VLAN. If you include trunked ports, specify the anchor port of the trunk. On the CoreBuilder 9000, the list of ports includes the front-panel ports and the module's backplane port.</p> <p>When you define a VLAN that includes the IP protocol type, you cannot specify a port that is owned by a router port IP interface.</p>	<ul style="list-style-type: none"> ■ One or more of the ports that are available to be assigned to the VLAN ■ all ■ ? (for a list of selectable ports) 	–
Protocol suite (for VLANs other than the default)	<p>One or more protocol suites that you want to specify for the VLAN</p> <p>The default VLAN always uses the protocol type unspecified.</p>	<ul style="list-style-type: none"> ■ IP ■ IPX ■ Apple (for AppleTalk) ■ XNS ■ DECnet ■ SNA ■ Vines ■ X.25 ■ NETBEUI ■ unspecified (Default VLAN or a port-based VLAN) ■ IPX-II ■ IPX-802.2 ■ IPX-802.3 ■ IPX-802.2-SNAP 	unspecified (factory default)

Prompt	Description	Possible Values	[Default]
Layer 3 address configuration (IP VLAN only)	Whether you want to define Layer 3 information for the IP VLAN Since this is the last release to support Layer 3 address information in IP VLANs, avoid this mechanism and instead define multiple IP interfaces for the VLAN with <code>ip interface define</code> commands.	<ul style="list-style-type: none"> ■ y (yes) ■ n (no) 	y
Layer 3 address and mask (IP VLAN only)	Fields (IP network address and subnet mask) you can use to set up flood domains for overlapping IP VLAN subnetworks. This is the last release to support Layer 3 address information in IP VLANs.	Any valid IP network address and subnet mask	–
Per-port tagging	Whether you want to configure IEEE 802.1Q VLAN tagging. You are prompted to answer for each port that you selected.	<ul style="list-style-type: none"> ■ y (yes) ■ n (no) 	y
Tag type	Whether you want to configure no tagging or IEEE 802.1Q tagging (the VID) for each port.	<ul style="list-style-type: none"> ■ none ■ 802.1Q 	none
VLAN name (for VLANs other than the default)	Unique, user-defined name that identifies members of the VLAN. If you use spaces, put quotation marks around the VLAN name.	Up to 32 ASCII characters or spaces	–

Procedure

- 1 Enter the VLAN identification (VID) number in the range 2 – 4094.
- 2 Select the bridge ports.
- 3 Select one or more protocol suites.

If you select an IP protocol suite, proceed with step 4. If you did not choose an IP protocol suite for this interface, proceed to step 5.

- 4 Specify whether you want to specify Layer 3 address information (**n** or **y**). The default is **y**. Specify **n** if possible and instead define multiple IP interfaces for this VLAN using `ip interface define` commands. (See Chapter 16.) If you still want to specify Layer 3 address information for an IP VLAN:
 - a Enter **y** for Layer 3 addressing.
 - b Enter the Layer 3 network address.
 - c Enter the Layer 3 subnet mask. To accept the default or current value in brackets [], press Return or Enter.
- 5 Specify whether you want per-port tagging (**n** or **y**). The default is **y**.
- 6 If you specified per-port tagging, enter the tag type for the indicated port (**none** or **802.1Q**).
- 7 If you have defined more than one port, you are prompted again for a tag type for each port.
- 8 Enter the VLAN name.

Bridge VLAN Define Example (9000 Layer 3)

This example shows the steps necessary to define a protocol-based VLAN for IPX 802.3 on a Layer 3 switching module. In this example, only the backplane port (port 13) of the module has IEEE 802.1Q tagging; the front-panel ports in this VLAN are not tagged. Because you have tagged the module's backplane port, you must also tag the corresponding switch fabric module port of the switch fabric module for that VLAN. (Use the EME to connect to the switch fabric module and configure the VLAN.)

```

CB9000@slot2.1 [12-E/FEN-TX-L3] (bridge/vlan): define
Enter VID (2-4094) [5]: 5
Select bridge ports (1-13|all|?): 1-3,13
Enter protocol suite
(IP, IPX, Apple, XNS, DECnet, SNA, Vines, X25, NetBEUI, unspecified,
IPX-II, IPX-802.2, IPX-802.3): IPX-802.3
Enter protocol suite ('q' to quit)
(IP, Apple, XNS, DECnet, SNA, Vines, X25, NetBEUI, IPX-II, IPX-802.2,
IPX-802.3): q
Configure per-port tagging? (n,y) [y]: y
Enter port 1 tag type (none,802.1Q): none
Enter port 2 tag type (none,802.1Q): none
Enter port 3 tag type (none,802.1Q): none
Enter port 13 tag type (none,802.1Q): 802.1Q
Enter VLAN Name {?} [ ]: IPX1

```

Bridge VLAN Define Example (3500)

This example shows the steps necessary to define an IP VLAN with IEEE 802.1Q tagging on some ports. (Instead of supplying Layer 3 address information when you define the VLAN, you can define multiple IP interfaces for this VLAN.) This VLAN has *trunk ports*.

```
Select menu option: bridge vlan define
Enter VID (1-4094) [2]: 2
Select bridge ports (1-4,6,9-13|all|?) [3,6]: ?

Default selection: [3,6]

Selectable bridge ports

selection      ports      label
  1             1
  2             2
  3            3,5      CampusLk1
  4             4
  6            6-8      CampusLk2
  9             9
 10            10
 11            11
 12            12
 13            13

Select bridge ports (1-4,6,9-13|all|?) [3,6]: 3,6,9
Enter protocol suite
(IP,IPX,Apple,XNS,DECnet,SNA,Vines,X25,NetBEUI,unspecified,IPX-II,IPX-802.2
IPX-802.3,IPX-802.2-SNAP): IP
Enter protocol suite ('q' to quit)
(IPX,Apple,XNS,DECnet,SNA,Vines,X25,NetBEUI,IPX-II,IPX-802.2,IPX-802.3,
IPX-802.2-SNAP): q
Configure layer 3 address? (n,y) [y]: n
Configure per-port tagging? (n,y) [y]: y
Enter port 3,5 tag type (none,802.1Q) [none]: none
Enter port 6-8 tag type (none,802.1Q) [none]: 802.1Q
Enter port 9 tag type (none,802.1Q): none
Enter VLAN Name {?} [ ]: IP1
```

bridge vlan define
(3900/9300/9400/
9000 Layer 2)

Creates a port-based VLAN on standalone systems or the CoreBuilder 9000 Layer 2 modules. When you configure a port-based VLAN, you assign a VLAN ID (VID), a set of bridge ports, and, optionally, IEEE 802.1Q tagging.

3500
 ✓ 9000
 ✓ 9400



For details about this command on the CoreBuilder 3500 and CoreBuilder 9000 Layer 3 modules, see “bridge vlan define (3500/9000 Layer 3)” earlier in this chapter.

✓ 3900
 ✓ 9300

Valid Minimum Abbreviation

b v def

Important Considerations

- On the SuperStack II Switch 3900 or 9300, you can define a maximum of 127 port-based VLANs on a single system.
- By default, all ports are defined to be part of the default VLAN, which always uses a VID of 1 and the name Default as of Release 3.0.0. If you delete the default VLAN, you can redefine it with VID 1 only.
- You cannot delete a VLAN that has an IP interface associated with it.
- The VID is used as the IEEE 802.1Q tag for a port if tagging is enabled.
- On the CoreBuilder 9000, the list of ports includes the front-panel ports and both backplane ports (even though only the lower-numbered backplane port is enabled by default). On the SuperStack II Switch 3900, the list of ports includes the 24 or 36 10/100 ports and any Gigabit Ethernet ports in use.
- For the CoreBuilder 9000, keep the following considerations in mind:
 - When you define a VLAN on a switching module and other switching modules in the system also define this VLAN, you must define the VLAN on both the switching module *and* on the switch fabric module.
 - When you define the VLAN on the Layer 2 switching module, you must specify any front-panel ports in the VLAN as well as the module’s lower-numbered backplane port. The specified backplane port must also be tagged if you have more than one VLAN.
 - When you define the VLAN on the switch fabric module, you must specify the switch fabric module backplane port that is connected to the switching module’s backplane port. The switch fabric module port must also be tagged if you have more than one VLAN.

Options

Prompt	Description	Possible Values	[Default]
VID	Unique, user-defined integer used by global management operations	<ul style="list-style-type: none"> ■ If the default VLAN exists, 2–4094 ■ If the default VLAN does not exist, 1 to redefine the default VLAN, or 2–4094 for other VLANs 	Next available VID
Bridge ports	Index numbers of the bridge ports that belong to the VLAN. If you include trunked ports, specify the anchor port of the trunk. See "Important Considerations" for information about the list of ports.	<ul style="list-style-type: none"> ■ One or more of the ports that are available to be assigned to the VLAN ■ all ■ ? (for a list of selectable ports) 	–
Per-port tagging	Whether you want to configure 802.1Q VLAN tagging. You are prompted to answer for each port that you selected.	<ul style="list-style-type: none"> ■ y (yes) ■ n (no) 	y
Tag type	Whether you want no tagging or IEEE 802.1Q tagging (the VID). For a port shared by another VLAN, verify that the specified tag type is not in conflict with the port's tag type in another VLAN.	<ul style="list-style-type: none"> ■ none ■ 802.1Q 	none
VLAN name (for VLANs other than the default)	Unique, user-defined name that identifies members of the VLAN. If you use spaces, put quotation marks around the VLAN name.	Up to 32 ASCII characters or spaces	–

Procedure

Press Return or Enter to accept the default or existing values that appear in brackets [].

- 1 Enter the VLAN identification (VID) number.
- 2 Enter one or more port numbers. To assign all ports to the VLAN, enter **all**.
- 3 Configure the per-port tagging.

- 4 Enter the tag type for each port in the VLAN.
- 5 Enter the VLAN name.

Bridge VLAN Define Example (9000 Layer 2)

This example shows a port-based VLAN that includes tagged front-panel ports and a tagged backplane port (port 21). These ports are tagged because they overlap with ports that belong to other VLANs:

- Because the front-panel ports are tagged, any attached devices must be IEEE 802.1Q enabled.
- Because the backplane port is tagged, the corresponding switch fabric module port must also be tagged in the VLAN definition on the switch fabric module. (You connect to the switch fabric module and define the VLAN to include the appropriate tagged switch fabric module port, based on the slot that contains the switching module.)

```
CB9000@slot 10.1 [20-E/FEN-TX-L2] (bridge/vlan): define
Enter VID (2-4094) [3]: 3
Select bridge ports (1-22|all|?): 1-5,21
Configure per-port tagging? (n,y) [y]: y
Enter port 1 tag type (none,802.1Q): 802.1Q
Enter port 2 tag type (none,802.1Q): 802.1Q
Enter port 3 tag type (none,802.1Q): 802.1Q
Enter port 4 tag type (none,802.1Q): 802.1Q
Enter port 5 tag type (none,802.1Q): 802.1Q
Enter port 21 tag type (none,802.1Q): 802.1Q
Enter VLAN Name {?} [ ]: vlantag3
```

Bridge VLAN Define Example (3900)

This example shows a port-based VLAN that includes tagged ports.

```
Select menu option (bridge/vlan): define
Enter VID (2-4094) [2]: 2
Select bridge ports (1-39|all|?): 3-5
Configure per-port tagging? (n,y) [y]: y
Enter port 3 tag type (none, 802.1Q) [none]: 802.1Q
Enter port 4 tag type (none, 802.1Q) [none]: 802.1Q
Enter port 5 tag type (none, 802.1Q) [none]: 802.1Q
Enter VLAN name {?} [ ]: Sales
```

**bridge vlan modify
(3500/9000 Layer 3)**

✓ 3500
✓ 9000
9400

3900
9300

**For CoreBuilder 9000: Applies to Layer 3 switching modules only.**

Changes an existing port-based, protocol-based, or network-based VLAN definition on the CoreBuilder 3500 system or CoreBuilder 9000 Layer 3 module.

To use this command on the SuperStack II Switch 3900 or Switch 9300, the CoreBuilder 9400, and CoreBuilder 9000 Layer 2 modules, see “bridge vlan modify (3900/9300/9400/ 9000 Layer 2)” next.

Valid Minimum Abbreviation

b v modi

Important Considerations

- Before you modify the port assignments for a VLAN, always enter ? to review the system port summary. If the VLAN includes trunk ports, you must specify the anchor (lowest numbered) port in each trunk. If there are no trunk ports, enter one or more port numbers, or enter all to assign all ports to the VLAN.
- For the CoreBuilder 3500, if you want to modify your VLAN to include FDDI DAS ports, you must specify the lowest-numbered port in the DAS pair.
- If you modify the default VLAN, you can only change the member ports or the tag status. You cannot change the name or the VID or the protocol type of unspecified.
- If you modify the tagging type of a backplane port on a switching module, make sure that you modify the tagging type of the corresponding port on the switch fabric module.
- To modify a VLAN to support more than one protocol suite for the VLAN, specify one protocol at each of the prompts.
- Select the bridge ports that you want to be part of the modified VLAN, or specify ? to display a port summary with the selectable bridge ports.
- If tagging is enabled for a port, the software uses the VID as the 802.1Q tag.

- If you modify the tagging for a port shared by another VLAN, and tagging is the only distinguishing characteristic between the VLANs, verify that the new tag type does not conflict with the port's tag type in another VLAN. (A shared port can use a tag type of `none` for only one of its VLANs; for all other VLANs to which it belongs, the shared port must use IEEE 802.1Q tagging.)

Options

Prompt	Description	Possible Values	[Default]
VLAN interface index	System-assigned index number that identifies a VLAN	<ul style="list-style-type: none"> ■ Selectable VLAN index ■ all ■ ? (for a list of selectable indexes) 	1 (if you have only the default VLAN)
VID (for VLANs other than the default)	Unique, user-defined integer used by global management operations	2 – 4094	Current VID
Bridge ports	Index numbers of the bridge ports that belong to the VLAN. To add trunked ports, specify the anchor port of the trunk. You cannot add a port owned by a router port IP interface.	<ul style="list-style-type: none"> ■ One or more index numbers of the ports that are available to be assigned to the VLAN ■ all ■ ? (for a list of selectable ports) 	Current ports in the VLAN

Prompt	Description	Possible Values	[Default]
Protocol suite (for VLANs other than the default)	One or more protocol suites that you want to specify for the VLAN	<ul style="list-style-type: none"> ■ IP ■ IPX ■ Apple (for AppleTalk) ■ XNS ■ DECnet ■ SNA ■ Vines ■ X.25 ■ NETBEUI ■ unspecified ■ IPX-II ■ IPX-802.2 ■ IPX-802.3 ■ IPX-802.2-SNAP (3500 only) 	Current protocol type
Modify Layer 3 address (IP VLAN)	Whether you want to modify the Layer 3 information for the VLAN Avoid this mechanism and instead define multiple IP interfaces per VLAN with <code>ip interface define</code> commands.	<ul style="list-style-type: none"> ■ y (yes) ■ n (no) 	y
Layer 3 address and mask (IP VLAN)	Optional fields (IP network and mask) used to set up flood domains for overlapping IP VLAN subnetworks	Any valid IP network address and mask	Current address and mask
Per-port tagging	Whether you want to modify the per-port 802.1Q VLAN tagging. You are prompted to answer for each port that you specified.	<ul style="list-style-type: none"> ■ y (yes) ■ n (no) 	y
Tag type	Either no tagging or IEEE 802.1Q tagging (the VID)	<ul style="list-style-type: none"> ■ none ■ 802.1Q 	Current tag type for each port
VLAN name (for VLANs other than the default)	Unique, user-defined name that identifies members of the VLAN. If you use spaces, put quotation marks around the VLAN name.	Up to 32 ASCII characters or spaces	Current name

Procedure

To modify information for a VLAN, follow these steps:

- 1 Select the VLAN interface index.
- 2 For a VLAN other than the default VLAN, enter the VLAN identification (VID) number.
- 3 Specify the index numbers of the bridge ports.
- 4 For a VLAN other than the default VLAN, specify one or more protocol suites.

If you have selected the IP protocol suite, proceed with step 5. If you did not define an IP protocol suite for this VLAN, proceed to step 7.

- 5 Specify whether you want to modify Layer 3 address information (**n** or **y**). Since this is the last release to support Layer 3 address information, specify **n** if possible and instead define multiple IP interfaces for this VLAN using `ip interface define` commands. (See Chapter 16.) If you still want to modify Layer 3 address information for an IP VLAN:
 - a Enter **y** for Layer 3 addressing.
 - b Enter the Layer 3 network address.
 - c Enter the Layer 3 subnet mask. To accept the default or current value in brackets [], press Return or Enter.
- 6 Specify whether you want to modify per-port tagging.
- 7 If you want to modify per-port tagging, enter the new tag type for the port (**none** or **802.1Q**).
- 8 If you have specified that you want to modify more than one port, enter a tag type for each port.
- 9 For a VLAN other than the default VLAN, enter a new VLAN name or keep the current name.

The VLAN name can include up to 32 ASCII characters, including spaces. If you include spaces, put quotation marks around the VLAN name.

Bridge VLAN Modify Example (9000 Layer 3)

This example shows the steps to modify the per-port tagging for a protocol-based VLAN on a Layer 3 module. In this example, front-panel port 5 is changed to have IEEE 802.1Q tagging, and its associated device is IEEE 802.1Q enabled.

```
CB9000@slot2.1 [12-E/FEN-TX-L3] (bridge/vlan): modify
Select VLAN interface index {1-5|?}: 5
```

```
Enter VID (2-4094) [5]: 5
Select bridge ports (1-13|all|?) [1-5,13]: 1-5,13
Enter protocol suite
(IP,IPX,Apple,XNS,DECnet,SNA,Vines,X25,NetBEUI,unspecified,
IPX-II,IPX-802.2,IPX-802.3) [IPX-802.3]: IPX-802.3
Enter protocol suite ('q' to quit) (IP,IPX,Apple,XNS,
DECnet,SNA,Vines,X25,NetBEUI,IPX-II,IPX-802.2): q
Modify per-port tagging? (n,y) [y]: y
Enter port 1 tag type (none,802.1Q) [none]: none
Enter port 2 tag type (none,802.1Q) [none]: none
Enter port 3 tag type (none,802.1Q) [none]: none
Enter port 4 tag type (none,802.1Q) [none]: none
Enter port 5 tag type (none,802.1Q) [none]: 802.1Q
Enter port 13 tag type (none,802.1Q) [802.1Q]: 802.1Q
Enter VLAN Name {?} [IPX]: IPX1
```

Bridge VLAN Modify Example (3500)

This example shows the steps to modify the member ports and per-port tagging for an IP VLAN.

```
Select menu option: bridge vlan modify
Select VLAN interface index {1-2|?}: 2
Enter VID (2-4094) [2]: 2
Select bridge ports (1-4, 6, 9-13|all|?) [3,6,9]: 9,11
Enter protocol suite
(IP,IPX,Apple,XNS,DECnet,SNA,Vines,X25,NetBEUI,unspecified,
IPX-II,IPX-802.2,IPX-802.3, IPX-802.2-SNAP) [IP]: IP
Enter protocol suite ('q' to quit)
(IPX,Apple,XNS,DECnet,SNA,Vines,X25,NetBEUI,IPX-II,
IPX-802.2, IPX-802.3, IPX-802.2-SNAP): q
Modify layer 3 address? (n,y) [y]:n
Modify per-port tagging? (n,y) [y]: y
Enter port 9 tag type (none,802.1Q) [none]: 802.1Q
Enter port 11 tag type (none,802.1Q) [none]: 802.1Q
Enter VLAN Name {?} [IP1]: IP1
```

bridge vlan modify
(3900/9300/9400/
9000 Layer 2)

Changes a port-based VLAN definition on the indicated system Layer 2 module. See “Important Considerations” for information on when changes take effect.

3500
✓ 9000
✓ 9400



To use this command on the CoreBuilder 3500 or CoreBuilder 9000 Layer 3 modules, see the “bridge vlan modify (3500/9000 Layer 3)” earlier in this chapter.

✓ 3900
✓ 9300

Valid Minimum Abbreviation

`b v modi`

Important Considerations

- You need not reboot the system for the changes to take effect. However, depending on the number of VLANs that are affected, the system may take several minutes to return control to you.
- If you modify the tagging type of a backplane port on a switching module, make sure that you modify the tagging type of the corresponding port on the switch fabric module.
- If tagging is enabled for a port, the software uses the VID as the 802.1Q tag.
- If you modify the default VLAN, you can only change the member ports or the tag status. You cannot change the name or the VID.
- If you modify the tagging for a port shared by another VLAN, verify that the new tag type does not conflict with the port’s tag type in another VLAN. (A shared port can use a tag type of `none` for only one of its VLANs; for all other VLANs to which it belongs, the shared port must use IEEE 802.1Q tagging.)

Options

Prompt	Description	Possible Values	[Default]
VLAN interface index	System-assigned index number that identifies a VLAN	<ul style="list-style-type: none"> ■ Selectable VLAN index ■ all ■ ? (for a list of selectable indexes) 	1 (if you have only the default VLAN)

Prompt	Description	Possible Values	[Default]
VID (for VLANs other than the default)	Unique, user-defined integer used by management operations	2 – 4094	Current VID
Bridge ports	Index numbers of the bridge ports that belong to the VLAN. To add trunked ports, specify the anchor port of the trunk.	<ul style="list-style-type: none"> ■ One or more index numbers of the ports that are available to be assigned to the VLAN ■ all ■ ? (for a list of selectable ports) 	Current ports in VLAN
Per-port tagging	Whether you want to configure 802.1Q VLAN tagging. You are prompted to answer for each port that you selected.	<ul style="list-style-type: none"> ■ y (yes) ■ n (no) 	y
Tag type	Either no tagging or IEEE 802.1Q tagging (the VID)	<ul style="list-style-type: none"> ■ none ■ 802.1Q 	Current tag type for each port
VLAN name (for VLANs other than the default)	Unique, user-defined name that identifies members of the VLAN. If you use spaces, put quotation marks around the VLAN name.	Up to 32 ASCII characters or spaces	Current name

Procedure

- 1 Enter the VLAN interface index.
- 2 For a VLAN other than the default VLAN, enter a VLAN identification (VID) number or keep the default in brackets.
- 3 Specify the index numbers of the bridge ports.
- 4 Specify whether you want to modify per-port tagging.
- 5 If you modify per-port tagging, enter the new tag type for the port (**none** or **802.1Q**).
- 6 If you have defined more than one port, enter a tag type for each port.
- 7 For a VLAN other than the default VLAN, enter a new VLAN name or keep the current name.

The VLAN name can include up to 32 ASCII characters, including spaces. If you include spaces, put quotation marks around the VLAN name.

Bridge VLAN Modify Example (9000 Layer 2)

This example shows the removal of two ports from a port-based VLAN that includes tagged front-panel ports and a tagged backplane port (port 21).

```
CB9000@slot 10.1 [20-E/FEN-TX-L2] (bridge/vlan): modify
Select VLAN interface index {1-3|?}: 3
Enter VID (2-4094) [3]: 3
Select bridge ports (1-22|all|?) [1-5,21]: 1-3,21
Configure per-port tagging? (n,y) [y]: y
Enter port 1 tag type (none,802.1Q) [802.1Q]: 802.1Q
Enter port 2 tag type (none,802.1Q) [802.1Q]: 802.1Q
Enter port 3 tag type (none,802.1Q) [802.1Q]: 802.1Q
Enter port 21 tag type (none,802.1Q) [802.1Q]: 802.1Q
Enter VLAN Name {?} [vlan3]: vlantag3
```

Bridge VLAN Modify Example (3900)

This example shows default VLAN changes in the ports and per-port tagging type.

```
Select menu option (bridge/vlan): modify
Select VLAN interface index {1-2|?}: 1
Select bridge ports (1-27|all|?) [1-27]: 2-6
Modify per-port tagging? (n,y) [y]:
Enter port 2 tag type (none,802.1Q) [none]: 802.1Q
Enter port 3 tag type (none,802.1Q) [none]: 802.1Q
Enter port 4 tag type (none,802.1Q) [none]: 802.1Q
Enter port 5 tag type (none,802.1Q) [none]: 802.1Q
Enter port 6 tag type (none,802.1Q) [none]: 802.1Q
```

bridge vlan remove Deletes a VLAN definition.

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

b v r

Important Considerations

- ✓ 3900
 - ✓ 9300
- When you remove a VLAN on a CoreBuilder 9000 Layer 2 or Layer 3 module, the system prompts you to verify that you want to wait the several minutes that it may take for the removal to be complete.
- You cannot remove a VLAN that is associated with any type of routing interface (for example, a router port VLAN created by a router port IP interface or a protocol-based VLAN associated with a particular router interface).

Options

Prompt	Description	Possible Values	[Default]
VLAN interface index	System-assigned index number that is associated with the VLAN	<ul style="list-style-type: none"> ■ A selectable VLAN index ■ all ■ ? (for a list of selectable indexes) 	–
Continue verification (9000 Layer 2 and Layer 3)	Whether you want to continue with the VLAN removal, even though the removal may take a few minutes to complete	<ul style="list-style-type: none"> ■ n (no) ■ y (yes) 	y

Bridge VLAN Remove Example (3500)

```
Select menu option: bridge vlan remove
Select VLAN interface indexes (1-2|all|?): ?

Selectable vlans

selection  VID  ports  name
1          1   1-13  Default
2          2   3,5-9,11  IP1

Select VLAN interface indexes (1-2|all|?):2
```

bridge vlan mode

Determines whether data with a unicast MAC address can be forwarded between VLANs.

- ✓ 3500
- ✓ 9000
- ✓ 9400

Valid Minimum Abbreviation

`b v mode`

- ✓ 3900
- ✓ 9300

Important Considerations

- Select a VLAN mode as follows:
 - **allOpen** — Use this less restrictive mode if you do not have security issues concerning the forwarding of data between VLANs. It is the default VLAN mode for all VLANs that you create. It permits data with a unicast MAC address to be forwarded between VLANs. The allOpen mode implies that the system uses a single bridge address table for all of the VLANs on the system.
 - **allClosed** — Use this restrictive mode if you are concerned about security between VLANs. Data cannot be forwarded between VLANs but can still be routed between VLANs. This mode implies that each VLAN that you create has its own address table.
- For the CoreBuilder 3500 system and CoreBuilder 9000 Layer 3 modules, if you are using allClosed mode and STP (with multiple routes to a destination), you can also use the command “bridge vlan stpMode” to disable STP blocking for a specified VLAN.
- For the CoreBuilder 9000, set a VLAN mode for each switching module and the switch fabric module.
- Changing this mode removes all VLANs and redefines the default VLAN.
- Before you issue this command to change the mode, you must remove all routing interfaces, including router port IP interfaces. If routing interfaces are defined, the system displays this message:

```
could not change configured VLAN mode - interface in
use by client.
```

Options

Prompt	Description	Possible Values	[Default]
VLAN mode	Selected VLAN mode for the entire system	<ul style="list-style-type: none"> ■ allOpen ■ allClosed 	allOpen (factory default), or current value

bridge vlan stpMode *For CoreBuilder 9000: Applies to Layer 3 switching modules only.*

✓ 3500
✓ 9000
9400

3900
9300

If allClosed mode is enabled, allows the system to ignore the Spanning Tree Protocol (STP) state for a specified VLAN interface or all interfaces, for either routing or bridging.

Valid Minimum Abbreviation

b v st

Important Considerations

- This mode is valid only if the VLAN mode is set to allClosed.
- To disable the STP state on a *per-port* basis with either allOpen or allClosed mode, use the `bridge port stpState` command. See Chapter 10.
- If you have configured router port IP interface (and therefore have a router port VLAN), the ignore STP mode is enabled and cannot be changed. You cannot select a router port VLAN with this command.

Options

Prompt	Description	Possible Values	[Default]
VLAN interface index	System-assigned index number that is associated with the VLAN	<ul style="list-style-type: none"> ■ Any selectable VLAN index number ■ all ■ ? (for a list of selectable indexes) 	—
STP state	Whether you want to ignore the STP state for the VLAN index	<ul style="list-style-type: none"> ■ disabled ■ enabled 	disabled

Bridge VLAN STP Mode Example (3500)

```
selection  VID  ports          name
1          1    1-13          Default
2          2    3, 5-9, 11    IP1
```

```
Select VLAN interface index(es) (1-2|all|?):2
```

```
Ignore STP state for VLAN index: 2 (disabled,enabled) [disabled]:enabled
```

**bridge vlan
vlanAwareMode**

✓ 3500
✓ 9000
9400

3900
9300

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

For compatibility purposes, allows the system to observe previous VLAN resource usage and tagged-frame ingress rules for CoreBuilder 3500 serial-port upgrades from Release 1.2.0 to 2.1.0 or 3.0.0 (or CoreBuilder 9000 upgrades from Release 2.0.0 to 3.0.0).

Valid Minimum Abbreviation

b v v

Important Considerations

- Use this command *only* if you upgrade your system and the system reports an error after reaching the VLAN resource limit during a power up with a serial-port console connection. During the upgrade, the difference in resource usage and modes of tagging could cause the later release to use more VLAN resources than did the earlier release, thereby causing a decrease in the total number of allowable VLANs.
- If the system reaches the VLAN resource limit during the upgrade, it displays an error message to identify the index of the VLAN that it was unable to create. The system removes all bridge ports from the VLAN that it could not restore from NV data but does maintain the previously stored NV data.
- The difference in VLAN resource usage is based on the following:
 - In CoreBuilder 3500 Release 1.2.0 (and CoreBuilder 9000 Release 2.0.0), all bridge ports were *not* VLAN aware (tagging aware) unless they were assigned to a VLAN that has one or more tagged ports. This behavior is associated with the VLAN aware mode of `taggedVlanPorts`. If you see the VLAN resource error message, you can restore your VLANs by issuing this command and setting the VLAN aware mode to `taggedVLANPorts`. If VLANs are already defined, the system prompts you to reboot the system to put the new mode into effect.
 - As of CoreBuilder 3500 Release 2.0.0, (and CoreBuilder 9000 Release 3.0.0), all bridge ports become VLAN aware after a software update or after an NV data reset and do not have to be explicitly tagged in order to forward tagged frames. This behavior is associated with the default VLAN aware mode of `allPorts`. If you do not see the VLAN internal resource error message, maintain the VLAN aware mode of `allPorts`.

- The VLAN aware mode reflects the difference in tagged-frame ingress rules between releases. Therefore, even if the system can accommodate the number of VLANs from the earlier release, be aware that it begins using different ingress rules for tagged frames.
 - The CoreBuilder 3500 tagged-frame ingress rules vary for 1.2.0, 2.0.0, and 3.0.0. For more information, see the *CoreBuilder 3500 Implementation Guide*.
 - The CoreBuilder 9000 tagged-frame ingress rules vary for 2.0.0 to 3.0.0. For more information, see the *CoreBuilder 9000 Implementation Guide*.

Options

Prompt	Description	Possible Values	[Default]
VLAN aware mode	Whether all ports are tagging aware or only tagged ports are tagging aware	<ul style="list-style-type: none"> ■ allPorts ■ taggedVlanPorts 	allPorts
Reboot system?	Since changing the mode requires you to reboot, whether you want to reboot the system or cancel the request	<ul style="list-style-type: none"> ■ n (no) ■ y (yes) 	y (yes)

Bridge VLAN Aware Mode Example (3500)

```
Select menu option (bridge/vlan): vlanAwareMode
VLAN-aware mode (taggedVlanPorts,allPorts) [allPorts]:
taggedVLANPorts
Changing the VLAN-aware mode will reboot the system -
continue? (n,y) [y]: y
```


PACKET FILTERS

This chapter provides guidelines and other key information about how to administer bridge packet filters in your system, including the following tasks:

- Listing and displaying packet filters
- Creating, deleting, editing, and loading packet filters
- Assigning and unassigning packet filters
- Managing port groups

Independently configurable packet filtering is provided for the packet processing paths on each bridge port of the system. After you create a packet filter, you can assign the filter to the transmit or the receive paths of any bridge port or group of bridge ports.

The filter executes a series of test operations on the packet's contents and, if the result is zero, it stops (filters) the packet. If the end result is non-zero, the filter lets the packet pass.



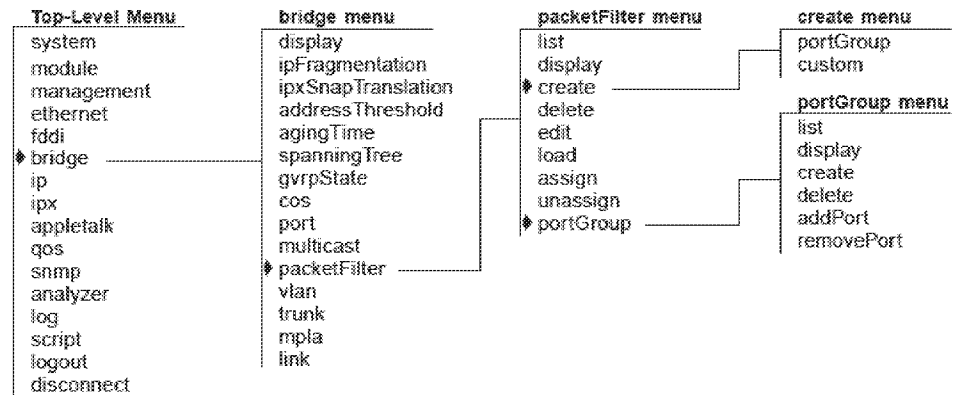
For more information about implementing packet filters on your network, see the Implementation Guide for your system.



For the CoreBuilder® 9000 platform, the commands in this chapter apply to Layer 3 switching modules only.

Menu Structure

The commands that you can use depend on the system that you have, your level of access, and the types of modules and other hardware options that are configured for your system. The following diagram shows the complete list of commands for all systems. See the checklist at the beginning of each command description in this chapter for whether your system supports the command.



bridge packetFilter list *For CoreBuilder 9000: Applies to Layer 3 switching modules only.*
Lists the currently defined packet filters.

✓ 3500
✓ 9000
9400

Valid Minimum Abbreviation

b pa li

Bridge Packet Filter List Example (3500)

Select menu option (bridge/packetFilter): list

```
Packet Filter 1 - rejdifportgrp
Port 11, txA, rxA
```

In the example, the system has one packet filter, with a filter id of 1 and a defined name of rejdifportgrp. This filter is loaded onto port 11. The filter is assigned to both the transmit all (txA) path and the receive all (rxA) path.

**bridge packetFilter
display**

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Displays the contents of the specified packet filter.

✓ 3500
✓ 9000
9400

Valid Minimum Abbreviation

b pa di

Important Considerations

- Possible values for filters (n) depend on the number of created or loaded filters on the system.
- The packet filter id and name are displayed, followed by a list of the packet filter instructions.

Options

Prompt	Description	Possible Values	[Default]
Select filter	Identifier (id number) of the filter that you want to display	<ul style="list-style-type: none"> ■ 1 – n ■ ? (for a list of all filters) 	Current filter id

Sample Bridge Packet Filter Display (3500)

Select menu option (bridge/packetFilter): **display**
Select filter {1|?} [1]:

```

Packet Filter 1 - rejdiffportgrp
  name                "rejdiffportgrp"
  pushDPGM
  pushSPGM
  and
  pushLiteral.1      0x00000000
  ne

```


**bridge packetFilter
create portGroup**

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Creates the portGroup (rejdifportgroup) standard hardware filter.

✓ 3500
✓ 9000
9400

3900
9300

Valid Minimum Abbreviation

b pa c p

Important Considerations

- The portGroup (rejdifportgroup) packet filter rejects a frame if the destination and source ports are not in the same group.
- “Creating” a hardware filter means that the code for the filter is copied from firmware into non-volatile memory.
- To verify that the filter has been created, use the `bridge packetFilter list` command. To see the contents of the portGroup filter, use the `bridge PacketFilter display` command.
- The system only creates the packet filter definition. You must still assign ports and masks to port groups, as described for “bridge packetFilter portGroup create” later in this chapter, and assign the standard filter to ports and filtering paths, as described for “bridge packetFilter assign” later in this chapter.
- At present, portGroup is the only filter supported in hardware.

Bridge Packet Filter Create Port Group Example

This example shows the user creating the portGroup filter.

```
Select menu option (bridge/packetFilter): create portgroup
Packet filter 1 stored.
```

**bridge packetFilter
create custom**

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Creates a custom packet filter using the built-in editor.

✓ 3500
✓ 9000
9400

Valid Minimum Abbreviation

`b p a c c`

Important Considerations

- You can create custom filters to add filtering logic based on the content of the packet.
- The built-in editor is a simple one-line-at-a-time editor that supports a short list of EMACS-style editing commands.
- Save your work periodically with Ctrl+w. When you press Esc to exit the built-in editor, the system examines the filter's syntax. If the syntax is correct, the filter is loaded into the switch's non-volatile memory. Incorrect syntax filters are not loaded into non-volatile memory and are not saved across editor sessions.
- After you create the filter, edit it using "bridge packetFilter edit" as described later in this chapter.
- The alternative to creating a custom packet filter using the built-in editor is to create the packet filter on an external system and transfer it across the network into the switch. See "bridge packetFilter load" later in this chapter.
- You can also use the Filter Builder component of the Web Management application to create custom filters.
 - On CoreBuilder 3500 systems, you can load the filter on to the switch directly from Filter Builder.
 - On CoreBuilder 9000 system, you must save the filter to an ASCII file and then download the file to the switch manually using TFTP and the "bridge packetFilter load" command described later in this chapter.
- The system only creates the packet filter definitions. You must still assign the standard filter to ports and filtering paths, as described for "bridge packetFilter assign" later in this chapter.

Create Custom Bridge Packet Filter Example (3500)

After you enter the custom filter editor, the system displays the editor commands, as shown here.

```
Select menu option (bridge/packetFilter): create custom
```

Editor Commands

```
Buffer: list = Ctrl-l  
Line:  next = Ctrl-n, previous = Ctrl-p  
Cursor: start = Ctrl-a, end = Ctrl-e, left = Ctrl-b, right = Ctrl-f  
Insert: line = Enter  
Delete: previous = Ctrl-h (BSP), current = Ctrl-d (DEL), line = Ctrl-k  
Mode:  insert/overstrike toggle = Ctrl-o  
Save:  Ctrl-w  
Exit:  Esc
```

You now enter packet filter language statements that define the packet filter algorithm. See the *Implementation Guide* for your system for information about developing the packet filters.

**bridge packetFilter
delete****For CoreBuilder 9000: Applies to Layer 3 switching modules only.**

Deletes the selected packet filter.

✓ 3500
✓ 9000
94003900
9300**Valid Minimum Abbreviation**

b pa de

Important Considerations

- You cannot delete a filter if it is assigned. Before you can delete the filter, you must unassign the filter from the assigned ports.
- Possible values for filters (*n*) depend on the number of created or loaded filters on the system.
- To find the id of the filter, list the filters using the `bridge packetFilter list` command.

Options

Prompt	Description	Possible Values	[Default]
Select filter	Identifier (id number) of the filter that you want to delete	<ul style="list-style-type: none"> ■ 1 – <i>n</i> ■ ? (for a list of all identifiers) 	Current filter number
Delete packet filter?	Whether you want to delete the selected packet filter	<ul style="list-style-type: none"> ■ n (no) ■ y (yes) 	y

Bridge Packet Filter Delete Examples (3500)

```
Select menu option (bridge/packetFilter): delete
Select filter {1|?} [1]: 1
Delete packet filter (n,y) [y]: y
Packet filter 1 has been deleted.
```

If the filter is assigned, it cannot be deleted. The system responds as follows to the delete command:

```
Select menu option (bridge/packetFilter): delete
Select filter {1|?} [1]: 1
The selected filter is assigned
This problem prevents the deletion of this filter.
```

bridge packetFilter
edit

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Modifies an existing packet filter using the built-in editor.

- ✓ 3500
- ✓ 9000
- 9400

Valid Minimum Abbreviation

b pa e

- 3900
- 9300

Important Considerations

- The built-in editor is a simple one-line-at-a-time editor that supports a short list of EMACS-style editing commands.
- The system displays the editor commands that you use to edit the packet filters. You can edit packet filter language statements that define the packet filter algorithm. See the *Implementation Guide* for your system for information about developing the packet filters.
- Save your work periodically with Ctrl+w. To complete the editing process, press Esc. The system replaces the filter or creates a new filter, depending on your response to the prompts.
- When you exit, the system examines the filter's syntax. If the syntax is correct, the filter is loaded into the switch's non-volatile memory.
- Possible values for filters (*n*) depend on the number of created or loaded filters on the system.

Options

Prompt	Description	Possible Values	[Default]
Select filter	Identifier (id) number of the filter that you want to edit	<ul style="list-style-type: none"> ■ 1 – <i>n</i> ■ ? (for a list of all identifiers) 	Most recent filter edited
Replace existing filter?	Whether to replace the selected filter	<ul style="list-style-type: none"> ■ n (no) ■ y (yes) 	y
Store as new filter?	Whether to create a new filter	<ul style="list-style-type: none"> ■ n (no) ■ y (yes) 	y

Replace Existing Filter Example (3500)

```
Select menu option (bridge/packetFilter): edit
Select filter {1|?} [1]:
Editing packet filter 1.
```

Editor Commands

```
Buffer: list = Ctrl-l
Line: next = Ctrl-n, previous = Ctrl-p
Cursor: start = Ctrl-a, end = Ctrl-e, left = Ctrl-b, right = Ctrl-f
Insert: line = Enter
Delete: previous = Ctrl-h (BSP), current = Ctrl-d (DEL), line = Ctrl-k
Mode: insert/overstrike toggle = Ctrl-o
Save: Ctrl-w
Exit: Esc
```

Edit buffer has been saved

```
name "rejdifportgrp"
Replace existing filter (n,y) [y]: y
Packet filter 1 has been replaced.
```

Store as New Filter Example (3500)

```
Select menu option (bridge/packetFilter): edit
Select filter {1-2|?} [1]: 1
Editing packet filter 1.
```

Editor Commands

```
Buffer: list = Ctrl-l
Line: next = Ctrl-n, previous = Ctrl-p
Cursor: start = Ctrl-a, end = Ctrl-e, left = Ctrl-b, right = Ctrl-f
Insert: line = Enter
Delete: previous = Ctrl-h (BSP), current = Ctrl-d (DEL), line = Ctrl-k
Mode: insert/overstrike toggle = Ctrl-o
Save: Ctrl-w
Exit: Esc
```

Edit buffer has been saved

```
name "BlockGeoB"
Replace existing filter (n,y) [y]: n
Store as new filter (n,y) [y]: y
Packet filter 3 stored.
```

**bridge packetFilter
load**

✓ 3500
 ✓ 9000
 9400

3900
 9300

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Transfers a packet filter file from another host machine to the switch to which you are currently connected.

Valid Minimum Abbreviation

b pa lo

Important Considerations

- On the CoreBuilder 3500, before you use the `packetFilter load` command, select the required file transfer protocol (TFTP or FTP) using the `system fileTransfer` command.
- On the CoreBuilder 3500, this single command transfers a file from another host and loads it in a one-step process.
- On the CoreBuilder 9000, loading a filter from another host is a two-step process. You must first `download` the packet filter source file to the Enterprise Management Engine (EME) using TFTP, then `connect` to the Layer 3 module, then enter this `bridge packetFilter load` command.

The syntax of the EME download command is:

```
download module <slot.subslot> filter <IP address> <filename>
```

You must use TFTP to download on the CoreBuilder 9000. FTP does not work.

When you enter `bridge packetFilter load`, the CoreBuilder 9000 does not prompt you for any options. Instead, the module simply looks for the downloaded filter on the EME. If it finds it, it loads it. If it does not find it, it prints the message `Filter not found`.

- TFTP or FTP hosts may place restrictions on which files and pathnames are valid. See your host administrator or host documentation for TFTP and FTP information.
- `bridge packetFilter load` verifies the syntax of the filter. If the syntax is correct, it stores the filter into non-volatile memory. If the syntax is incorrect, you are prompted to enter the built-in editor so that you can fix the filter.

Options (3500)

Prompt	Description	Possible Values	[Default]
Host IP address	IP address of the machine from which you want to transfer the filter	Any valid IP address	current IP address
File pathname	Path and file name of the filter to transfer	<ul style="list-style-type: none"> ■ ? (for a list of criteria for entering the pathname) ■ Up to 128 characters 	path and file name last loaded

Bridge Packet Filter Load Example (3500)

The system transfers the specified filter and displays a confirmation message:

```
Select menu option (bridge/packetFilter): load
Host IP address: 158.101.112.191
File pathname {?}: /tftpboot/srackley/joe.fil
Packet filter 2 stored.
```

Bridge Packet Filter Load Example (9000)

The user has copied the source text for the “reject multicast traffic” filter, `rejmulticast.fil`, from the Filter Builder application to the TFTP application’s root directory on host 159.101.8.112. (You must use TFTP; FTP does not work.)

The user then logs on to the CoreBuilder 9000 EME and issues the download command to transfer the filter file to the EME. Note that the user specifies the type of download (filter) and for which module (6.01) the filter is destined.

```
CB9000> download module 6.01 filter 159.101.8.112 rejmulticast.fil

File transfer request pending.
Downloading file from external file server to eme - 000000289
Downloading file from eme to module 6.1 - 000000289
File transfer completed successfully.
```


The user next connects to the module and loads the filter.

```
CB9000> connect 6.01
```

```
Menu options (Corebuilder 9000-94DC8): -----
list          - List all packet filters
display       - Display a packet filter
create        - Create a packet filter
delete        - Delete a packet filter
edit          - Edit a packet filter
load          - Load a packet filter
assign        - Assign a packet filter
unassign      - Unassign a packet filter
portGroup    - Administer port groups
```

Type "q" to return to the previous menu or ? for help.

```
-----
CB9000@slot6.1 [12-E/FEN-TX-L3] (): bridge packetFilter load
Packet filter 1 stored.
```

Lastly, the user lists the loaded filters with `bridge packetfilter list` and confirms the contents of the filter with `bridge packetfilter display`.

```
CB9000@slot6.1 [12-E/FEN-TX-L3] (bridge/packetFilter): list
```

```
Packet Filter 1 - rejMulticast
No port assignments
```

```
Menu options (Corebuilder 9000-94DC8): -----
-----
list          - List all packet filters
display       - Display a packet filter
create        - Create a packet filter
delete        - Delete a packet filter
edit          - Edit a packet filter
load          - Load a packet filter
assign        - Assign a packet filter
unassign      - Unassign a packet filter
portGroup    - Administer port groups
```

Type "q" to return to the previous menu or ? for help.

```
-----
CB9000@slot6.1 [12-E/FEN-TX-L3] (bridge/packetFilter): display 1
```

```
Packet Filter 1 - rejMulticast
name          "rejMulticast"
pushField.b   0
pushLiteral.b 0x01
and
not
```

**bridge packetFilter
assign****For CoreBuilder 9000: Applies to Layer 3 switching modules only.**

Assigns a selected packet filter to a port or set of ports (port group).

✓ 3500
✓ 9000
94003900
9300**Valid Minimum Abbreviation**

b pa a

Important Considerations

- When you assign a packet filter to one or more ports, you must assign a processing path. The path (transmit all, transmit multicast, receive all, receive multicast, or receive internal) of a port can have only one packet filter assigned to it; however, you can assign a single packet filter to multiple paths and ports.
- If you try to assign a filter to a port that already has a filter assigned, the system displays a warning message and the assignment fails.
- After you assign the filter, ports and paths are removed from the list of possible values (which are listed in the Options table).
- Possible values for filters (n) depend on the number of created or loaded filters on the system.
- Possible values for bridge ports (n) depend on the number of existing bridge ports on the system.

Options

Prompt	Description	Possible Values	[Default]
Select filter	Identifier (id number) of the filter that you want to assign	<ul style="list-style-type: none"> ■ 1 – n ■ ? (for a list of valid filter identifiers) 	Current valid selected filter
Select bridge ports	Number of the bridge port to which you want to assign the selected filter	<ul style="list-style-type: none"> ■ 1 – n ■ all ■ ? (for a list of valid ports) 	Current valid selected bridge port

Prompt	Description	Possible Values	[Default]
Select path(s)	Identifier of the path to which you want to assign the selected filter	<ul style="list-style-type: none"> ■ txA ■ txM ■ rxA ■ rxM ■ rxI ■ all ■ ? (for a list of valid paths) 	Current valid selected path

Bridge Packet Filter Assign Examples (3500)

```
Select menu option (bridge/packetFilter): assign
Select filter {1|?} [1]:
Select bridge port(s) (1-12|all|?) [4-6]: all
Select path(s) (txA,txM,rxA,rxM,rxI|all|?): txA
```

To specify multiple ports, use the hyphen (-) to indicate ranges, and commas to indicate individual, non-contiguous ports. To specify multiple paths, separate the paths with commas.

```
Select menu option (bridge/packetFilter): assign
Select filter {1|?} [1]:
Select bridge port(s) (1-6|all|?): 1-3,6
Select path(s) (txA,txM,rxA,rxM,rxI|all|?): txA,rxA,rxI
```

bridge packetFilter unassign

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Unassigns selected packet filter from one or more ports.

✓ 3500
✓ 9000
9400

3900
9300

Valid Minimum Abbreviation

b pa u

Important Considerations

- The packet filter that you want to unassign must have been assigned to at least one port.
- Possible values for filters (n) depend on the number of created or loaded filters on the system.
- Possible values for bridge ports (n) depend on the number of existing bridge ports on the system.
- After you unassign the filter, ports and paths are added to the list of possible values (which are listed in the Options table).

Options

Prompt	Description	Possible Values	[Default]
Select filter	Identifier (id number) of the filter that you want to unassign	<ul style="list-style-type: none"> ■ 1 – n ■ ? (for a list of valid filter identifiers) 	Current valid selected filter
Select bridge ports	Numbers of one or more bridge ports from which you want to unassign the selected filter	<ul style="list-style-type: none"> ■ 1 – n ■ all ■ ? (for a list of valid ports) 	Current valid selected bridge port
Select path(s)	Identifiers of one or more paths from which you want to unassign the selected filter	<ul style="list-style-type: none"> ■ txA ■ txM ■ rxA ■ rxM ■ rxI ■ all ■ ? (for a list of valid paths) 	Current valid selected path

Bridge Packet Filter Unassign Examples (3500)

The unassignment is from the transmit all (txA) paths on port 1.

```
Select menu option (bridge/packetFilter): unassign
Select filter {1|?} [1]: 1
Select bridge port [1]: 1
Select path(s) (txA,rxA|all|?) [txA,rxA]: txA
```

**bridge packetFilter
portGroup list**

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Displays a list of currently defined port groups.

✓ 3500
✓ 9000
9400

Valid Minimum Abbreviation

b p a p l

Bridge Packet Filter Port Group List Example

Select menu option (bridge/packetFilter/portGroup): list

```
Port Group 1 - Marketing
  Port group mask - bit 15
Port Group 2 - Sales
  Port group mask - bit 32
```

In the example, the system has two port groups defined: Marketing and Sales. The display shows the group id, group name (if any), and group mask.

3900
9300

**bridge packetFilter
portGroup display**

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Displays a port group.

- ✓ 3500
- ✓ 9000
- 9400

Valid Minimum Abbreviation

b pa p di

Important Consideration

- Possible values for port groups (*n*) depend on the number of user-defined port groups on the system.

- 3900
- 9300

Options

Prompt	Description	Possible Values	[Default]
Select port group	Number of the port group to display	<ul style="list-style-type: none"> ■ 1 – <i>n</i> ■ ? (for a list of valid port groups) 	Current port group

Sample Bridge Packet Filter Port Group Display (3500)

```
Select menu option (bridge/packetFilter/portGroup): display
Select port group {1-2|?} [2]: 2

Port Group 2 - Sales
Port 5                               Port 6
```

**bridge packetFilter
portGroup create**

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Creates a port group.

✓ 3500
✓ 9000
9400

Valid Minimum Abbreviation

b p a p c

Important Considerations

- You can create up to 32 port groups, one for each bit in the 32-bit port group mask.
- The `portGroup create` command only creates port group associations. You must create and assign a filter to a port group to affect filtering. See “bridge packetFilter create portGroup” and “bridge packetFilter assign” earlier in this chapter.
- Possible values for bridge ports (n) depend on the number of bridge ports on the system.

Options

Prompt	Description	Possible Values	[Default]
Select port group mask	Mask that you want to assign to the port group	<ul style="list-style-type: none"> ■ 1 – 32 ■ ? (for a list of masks) 	–
Select port group name	Name of the port group that you want to create Use quotation marks around any string with embedded spaces. Use "" to enter an empty string	<ul style="list-style-type: none"> ■ Up to 32 alphanumeric characters ■ ? (for name criteria) 	–
Select bridge port	Number of the bridge port that you want to add to the new group	<ul style="list-style-type: none"> ■ 1 – n ■ all ■ ? (for a list of valid ports) 	–

Bridge Packet Filter Port Group Create Example (3500)

```
Select menu option (bridge/packetFilter/portGroup): create
Select port group mask {1-32|?}: 15
Select port group name {?} []: Marketing
Port Group 1 - Marketing - has been created
Select bridge port(s) (1-6|all|?): 1,3,4
```

```
Select menu option (bridge/packetFilter/portGroup): create
Select port group mask {1-14,16-32|?}: 32
Select port group name {?} []: Sales
Port Group 2 - Sales - has been created
```

bridge packetFilter portGroup delete

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Deletes a selected port group.

✓ 3500
✓ 9000
9400

Valid Minimum Abbreviation

b pa p de

Important Considerations

- When you delete port groups from the system, those groups are no longer available for use in packet filters.
- When you delete a port group, the remaining port group IDs are automatically renumbered to maintain consecutive numbering.
- Possible values for port groups (n) depend on the number of user-defined port groups on the system.

Options

Prompt	Description	Possible Values	[Default]
Select port group	Number of the port group to delete	<ul style="list-style-type: none"> ■ 1 – n ■ ? (for a list of groups) 	Current port group
Delete port group?	Whether to delete the selected port group	<ul style="list-style-type: none"> ■ n (no) ■ y (yes) 	y

Bridge Packet Filter Port Group Delete Example

```
Select menu option (bridge/packetFilter/portGroup): delete
Select port group {1-2|?} [2]: 1
Delete port group (n,y) [y]: y
Port Group 1 - Marketing - has been deleted.
```

**bridge packetFilter
portGroup addPort**

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Adds ports to an existing port group.

- ✓ 3500
- ✓ 9000
- 9400

- 3900
- 9300

Valid Minimum Abbreviation

b pa p a

Important Considerations

- You add ports to an existing group by entering port identifiers at the prompts. At least one port group must exist before you can add ports.
- The maximum number of ports that a port group can contain is 32, which is the maximum number of ports on a switching system.
- Possible values for port groups (*m*) depend on the number of user-defined port groups on the system.
- Possible values for bridge ports (*n*) depend on the number of existing bridge ports on the system.

Options

Prompt	Description	Possible Values	[Default]
Select port group	Number of the port group to which you want to add a bridge port	<ul style="list-style-type: none"> ■ 1 – <i>m</i> ■ ? (for a list of groups) 	Current port group
Select bridge port	Number of the bridge port that you want to add to the selected port group	<ul style="list-style-type: none"> ■ 1 – <i>n</i> ■ all ■ ? (for a list of groups) 	–

Bridge Packet Filter Port Group Add Port Examples

```
Select menu option (bridge/packetFilter/portGroup): add
Select port group {1-2|?} [2]: 2
Select bridge port(s) (1-6|all|?): 2
```

When you display port group 2, the display shows that port 2 is added:

```
Select menu option (bridge/packetFilter/portGroup): display
Select port group (1-2|all|?) [2]:

Port Group 2 - Sales
Port 2
Port 6

Port 5
```

**bridge packetFilter
portGroup
removePort**

For CoreBuilder 9000: Applies to Layer 3 switching modules only.

Removes ports from a port group.

Valid Minimum Abbreviation

b p a p r

Important Considerations

- At least one group must exist before you can remove a port from a port group.
- Possible values for port groups (m) depend on the number of user-defined port groups on the system.
- Possible values for bridge ports (n) depend on the number of existing bridge ports on the system.

Options

Prompt	Description	Possible Values	[Default]
Select port group	Number of the port group from which you want to remove a bridge port	<ul style="list-style-type: none"> ■ 1 – m ■ ? (for a list of groups) 	Current port group
Select bridge port	Number of the bridge port that you want to remove from the selected port group	<ul style="list-style-type: none"> ■ 1 – n ■ all ■ ? (for a list of ports) 	–

Bridge Packet Filter Port Group Remove Port Examples

```
Select menu option (bridge/packetFilter/portGroup): remove
Select port group {1-2|?} [2]: 2
Select bridge port(s) (1-6|all|?): 6
```

Displaying port group 2 shows that port 6 is removed:

```
Select menu option (bridge/packetFilter/portGroup): display
Select port group (1-2|all|?) [2]:
```

```
Port Group 2 - Sales
Port 2                               Port 5
```

✓ 3500

✓ 9000

9400

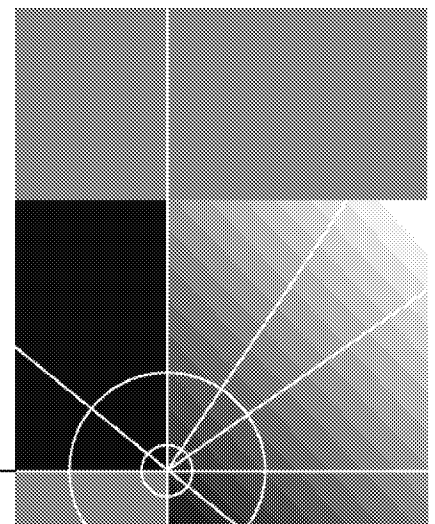
3900

9300



ROUTING PROTOCOLS

- Chapter 16 Internet Protocol (IP)
- Chapter 17 Virtual Router Redundancy Protocol (VRRP)
- Chapter 18 IP Multicast
- Chapter 19 Open Shortest Path First (OSPF)
- Chapter 20 IPX
- Chapter 21 AppleTalk



16

INTERNET PROTOCOL (IP)

To route packets using the Internet Protocol (IP), you:

- Establish an IP routing interface
- Decide which IP options and routing protocols you want to use
- Enable IP routing

An IP routing interface defines the relationship between an IP virtual LAN (VLAN) and the subnetworks in the IP network. Each routing IP VLAN interface is associated with one VLAN that supports IP. The system has one interface defined for each subnet that is directly connected to it.

You can also choose between two different routing models when you establish an IP routing interface:

- VLAN-based routing
Because bridging is faster in normal circumstances, the system first tries to determine if it can bridge the frame before routing it.
- Router port-based routing
The system first tries to route packets that belong to recognized protocols, and then bridges all other packets. If the network or a portion of the network is devoted to routing IP frames, this model makes network traffic more efficient.

This chapter provides guidelines and other key information about how to configure IP in your system. This chapter addresses the commands in the `ip` menu except for `multicast` and `ospf`, which other chapters in this *Command Reference Guide* explain.

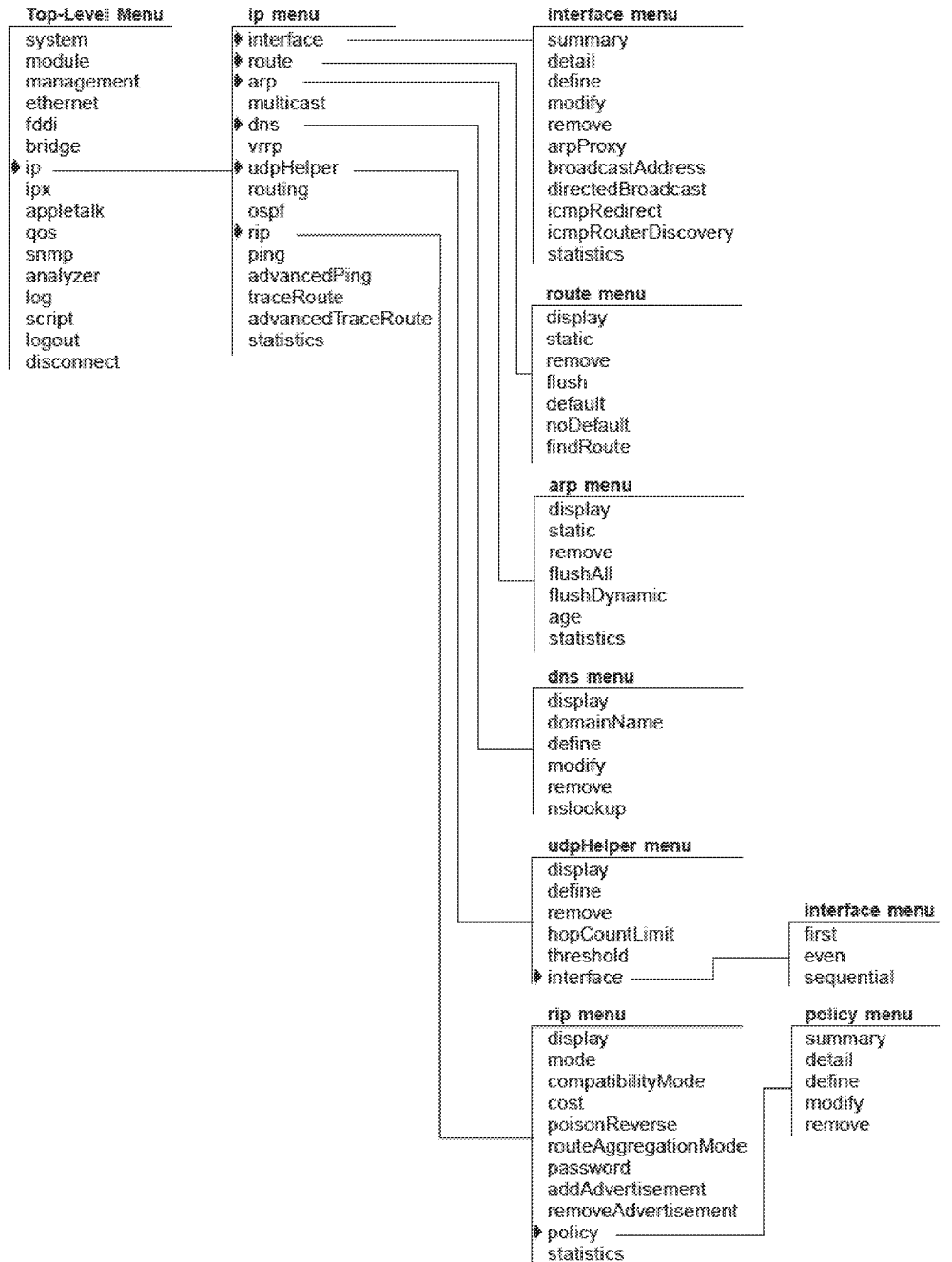
For information about IP multicast, see Chapter 18. For information about Open Shortest Path First (OSPF) routing using IP, see Chapter 19.



For more information about IP routing, see the Implementation Guide for your system.

Menu Structure

The commands that you can use depend on the system that you have, your level of access, and the types of modules and other hardware options that are configured for your system. The following diagram shows the complete list of commands for all systems. See the checklist at the beginning of each command description in this chapter for whether your system supports the command.



ip interface summary *For CoreBuilder 9000: Applies to Layer 3 switching modules only.*

✓ 3500

✓ 9000

✓ 9400

✓ 3900

✓ 9300

Displays summary information about the IP interfaces that are configured on the system.

Valid Minimum Abbreviation

```
ip i su
```

Important Considerations

- When you enter the command, you are prompted for an interface index number even if you have only one interface defined.
- The first line in the output (the status line) indicates whether IP routing is enabled:
 - For CoreBuilder 9000 Layer 3 modules, it also indicates whether ICMP router discovery is enabled on the system.
 - For the CoreBuilder 3500, IP interface options (such as ICMP router discovery) appear under “ip interface detail” and are set on a per-interface basis.
- The Type field differs according to platform:
 - In the CoreBuilder 3500, which provides port-based routing and VLAN-based routing, the Type field displays whether the IP interface is VLAN-based or router port-based.
 - In all other platforms, which provide VLAN-based routing, the Type field displays whether the IP interface is used for VLAN traffic or for system management.
- The last (rightmost) field in the display differs according to platform:
 - In the CoreBuilder 3500, the ID field displays either the logical port number that is associated with a router port-based IP interface, or the VLAN interface index number that is associated with the IP interface.
 - In all other platforms, the VLAN index field displays the VLAN interface index number that is associated with the IP interface.

Options

Prompt	Description	Possible Values	[Default]
Interface index	Index number of the IP interface whose summary information you want to display	<ul style="list-style-type: none"> ■ One or more selectable interface indexes ■ all ■ ? (for a list of selectable interface indexes) 	–

Fields in the IP Interface Summary Display

Field	Description
Index	Index number of the IP interface whose summary information you want to display
IP address	IP address of the interface, chosen from the range of addresses that the central agency assigned to your organization. This address is specific to your network and system.
Subnet mask	32-bit number that uses the same format and representation as an IP address. The subnet mask determines which bits in the IP address are interpreted as the network number, the subnetwork number, and the host number. Each IP address bit that corresponds to a 1 in the subnet mask is in the network/subnetwork part of the address. Each IP address bit that corresponds to a 0 is in the host part of the IP address.
State	State of the IP interface. It indicates whether the interface is available for communications (<code>up</code>) or unavailable (<code>down</code>).
Type	<ul style="list-style-type: none"> ■ Type of interface: VLAN-based or router port-based (3500) ■ Type of interface: VLAN or system (all other platforms)
ID (3500)	<ul style="list-style-type: none"> ■ Logical port number of the router port-based IP interface or the VLAN index that is associated with the IP interface
VLAN index (3900, 9000, 9300, 9400)	<ul style="list-style-type: none"> ■ VLAN index number that is associated with the IP interface